

Trust Frameworks

Hannes Tschofenig

Nokia Siemens Networks

Passwords are Broken

- On average people maintain 25 accounts
- Username/Password reuse across sites is very common
- Even strong passwords are vulnerable (e.g. phishing, spyware)
- Rising cost of identity theft:
 - Over 10 million Americans are also victims of identity theft each year. – “The Department of Justice’s Efforts to Combat Identity Theft.” U.S. Department of Justice. Office of the Inspector General. Mar. 2010. Web. 2 Jun. 2010.
<http://www.justice.gov/oig/reports/plus/a1021.pdf>
 - A Federal Trade Commission survey found that some victims of identity theft can spend more than 130 hours reconstructing their identities (e.g., credit rating, bank accounts, reputation, etc.) following an identity crime. – “2006 Identity Theft Survey Report.” Federal Trade Commission. Nov. 2007 p. 6. Web. 2 Jun. 2010.
<http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
- Deployment of services demanding higher level of assurance not progressing due to high barrier of entry.

End User Security & Privacy Concerns

What are your biggest concerns regarding misuse of your personal data? What would be a worst case scenario?



End User Privacy View

80%

of respondents see privacy as a very important topic*

63%

of respondents are concerned about privacy violations*

65%

of subscribers feel they lack control over their personal data*



“A revolution doesn’t happen when a society adopts new tools. It happens when it adopts new behaviors.”

Clay Shirky, Professor at NYU

Improving Security on the Web: Trust Frameworks – One Possibility

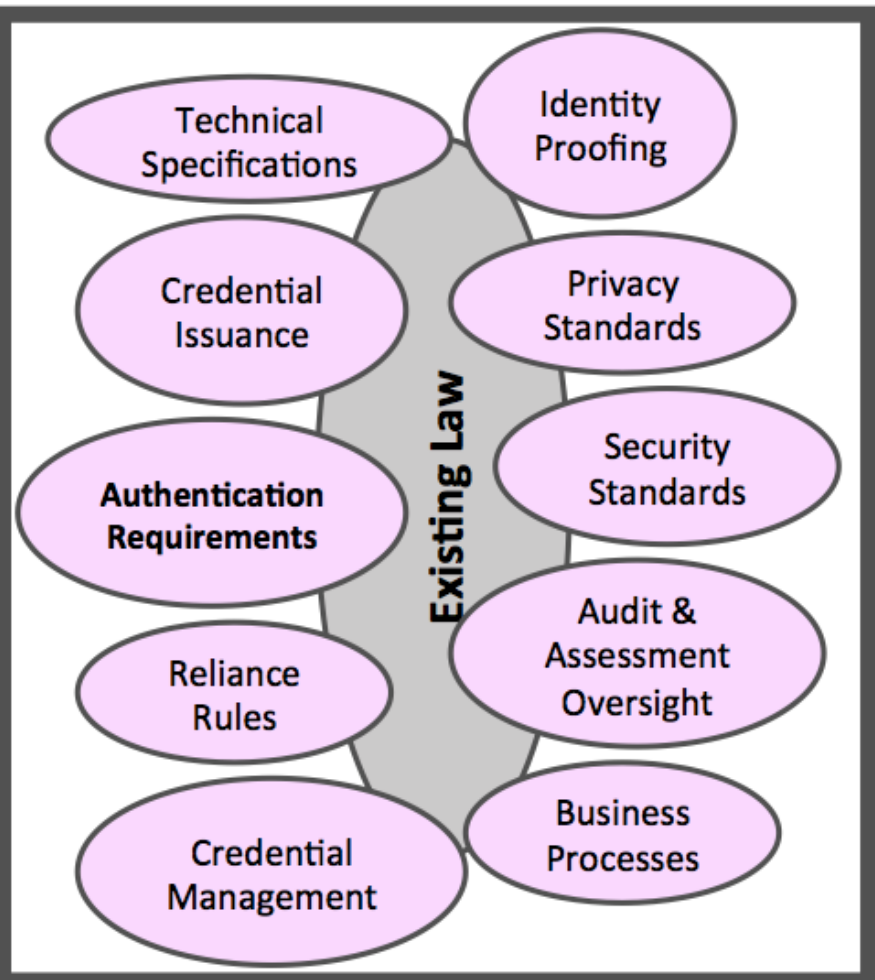
Operational Specifications

- Content
 - Technical specifications, process standards, policies, procedures, performance requirements, assessment criteria, etc.
- Goals
 - Make it work
 - Accomplish interoperability

Legal Rules

- Content
 - Existing law
 - Contractual obligations
- Goals
 - Regulate Operational Specifications
 - Make Operational Specifications legally binding on the participants
 - Define and govern the legal rights and responsibilities of the participants

Operational Specifications



Contract:
"I Agree" to ...

Legal Rules

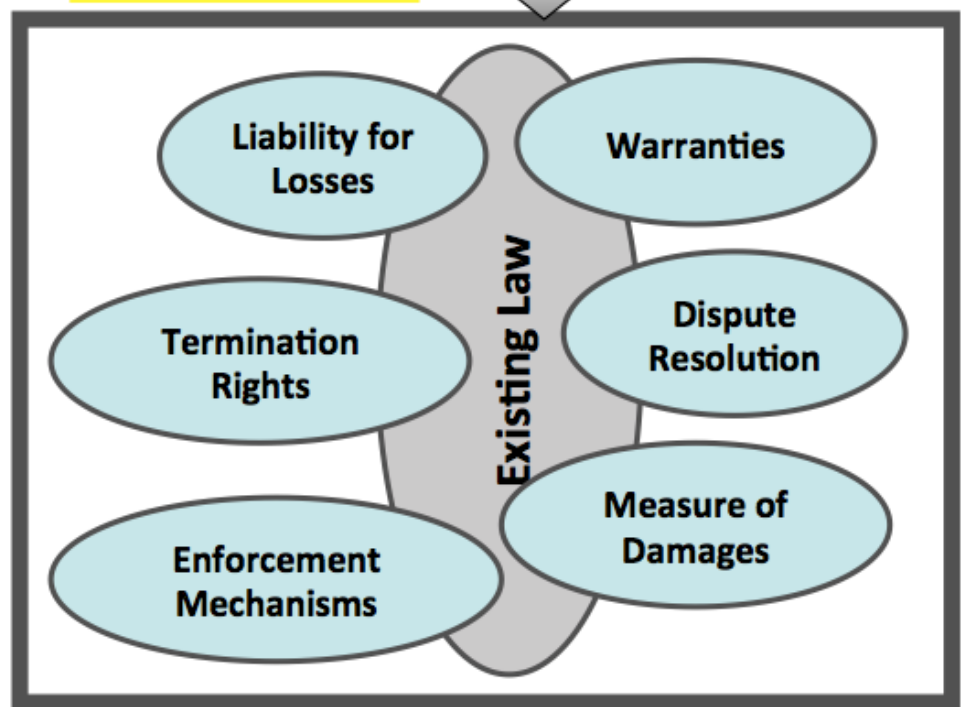
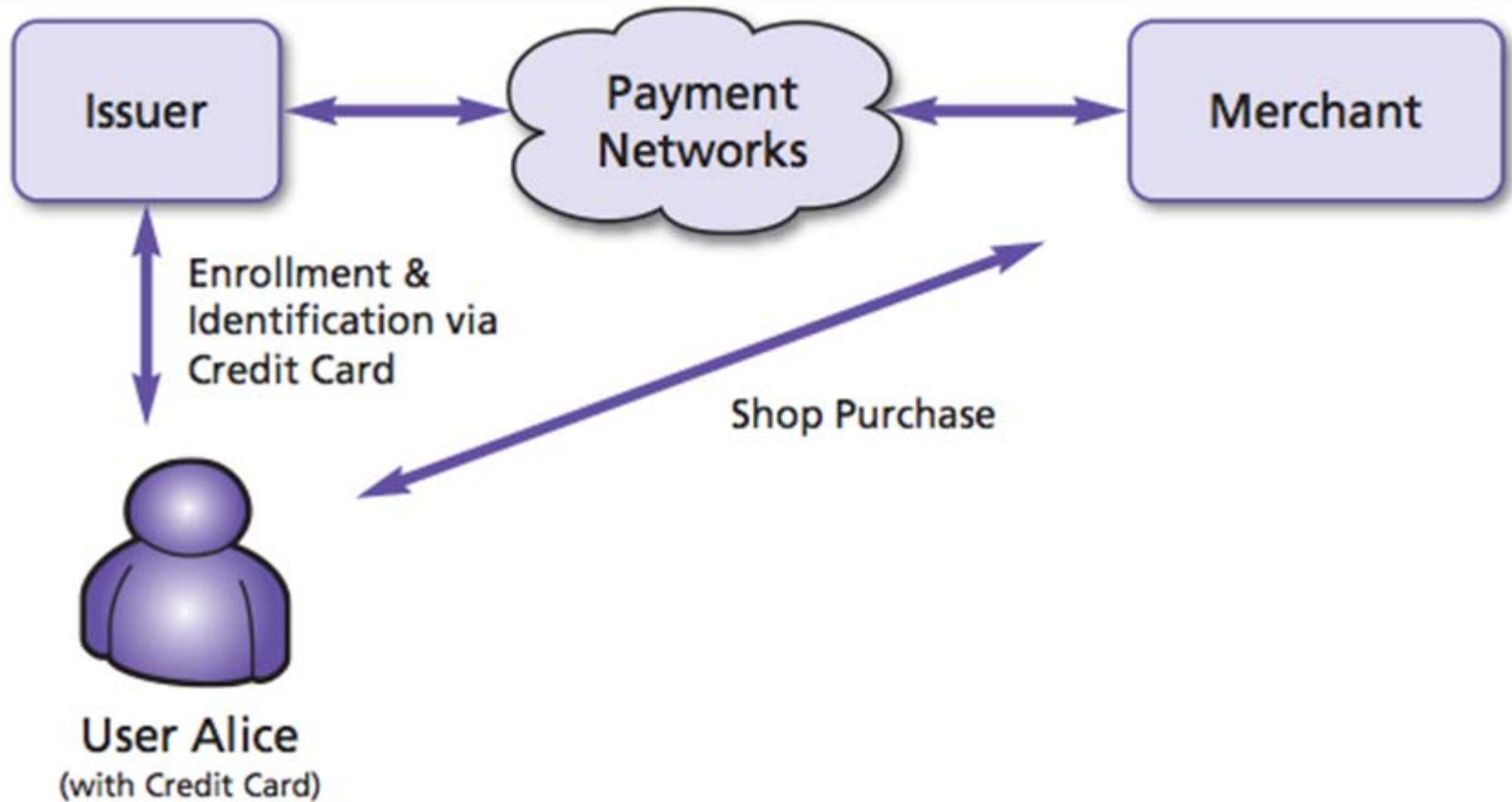


Figure from Thomas Smedinghoff's W3C Identity in the Browser workshop presentation.

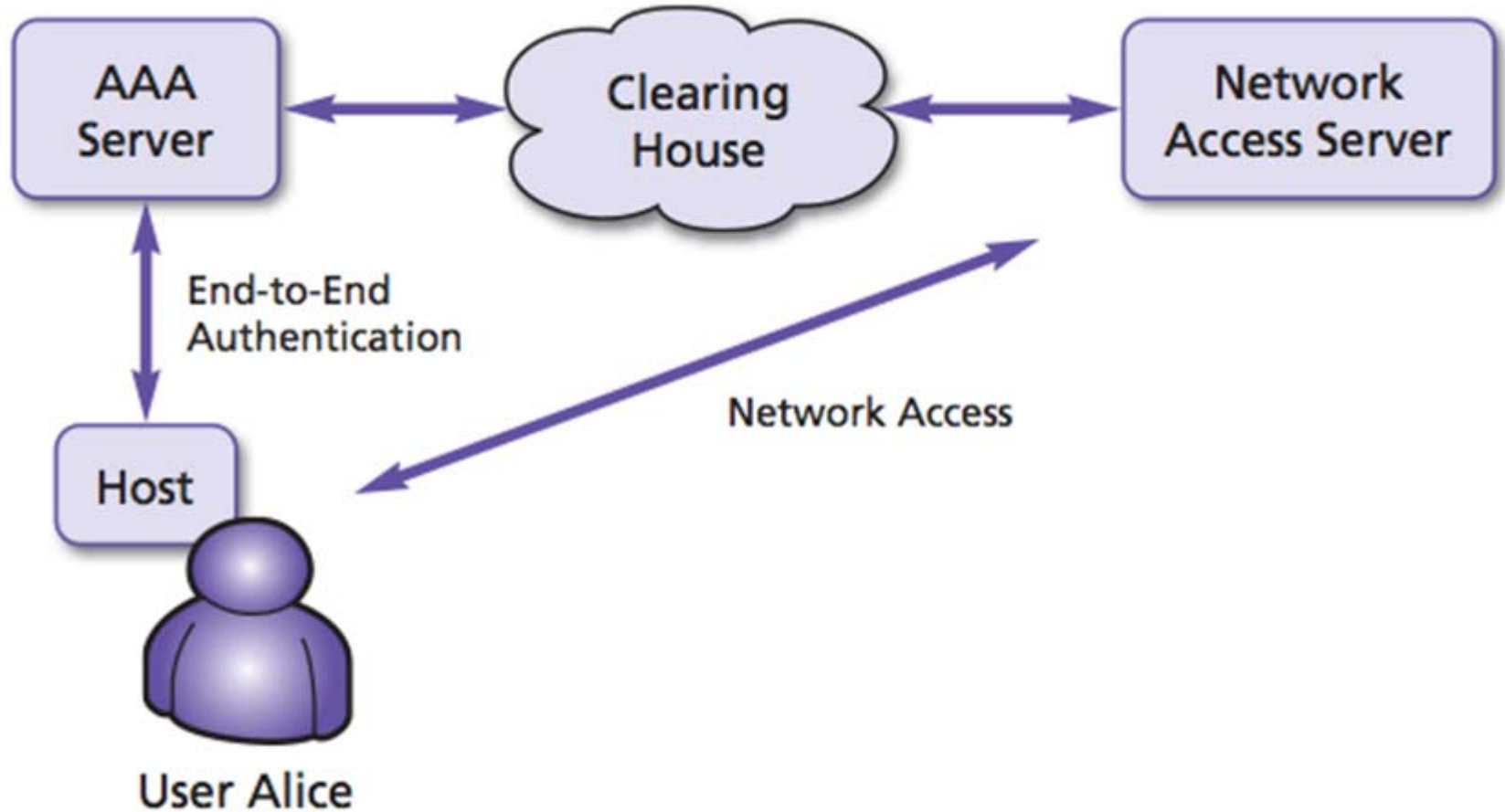
Example of Existing Trust Frameworks

- Credit Card System
- AAA infrastructure for network access
- Education federation
- Voice over IP infrastructure
- Instant Messaging infrastructure
- Email Infrastructure
- Web SSO federations (including OpenID, Facebook Connect, etc.)

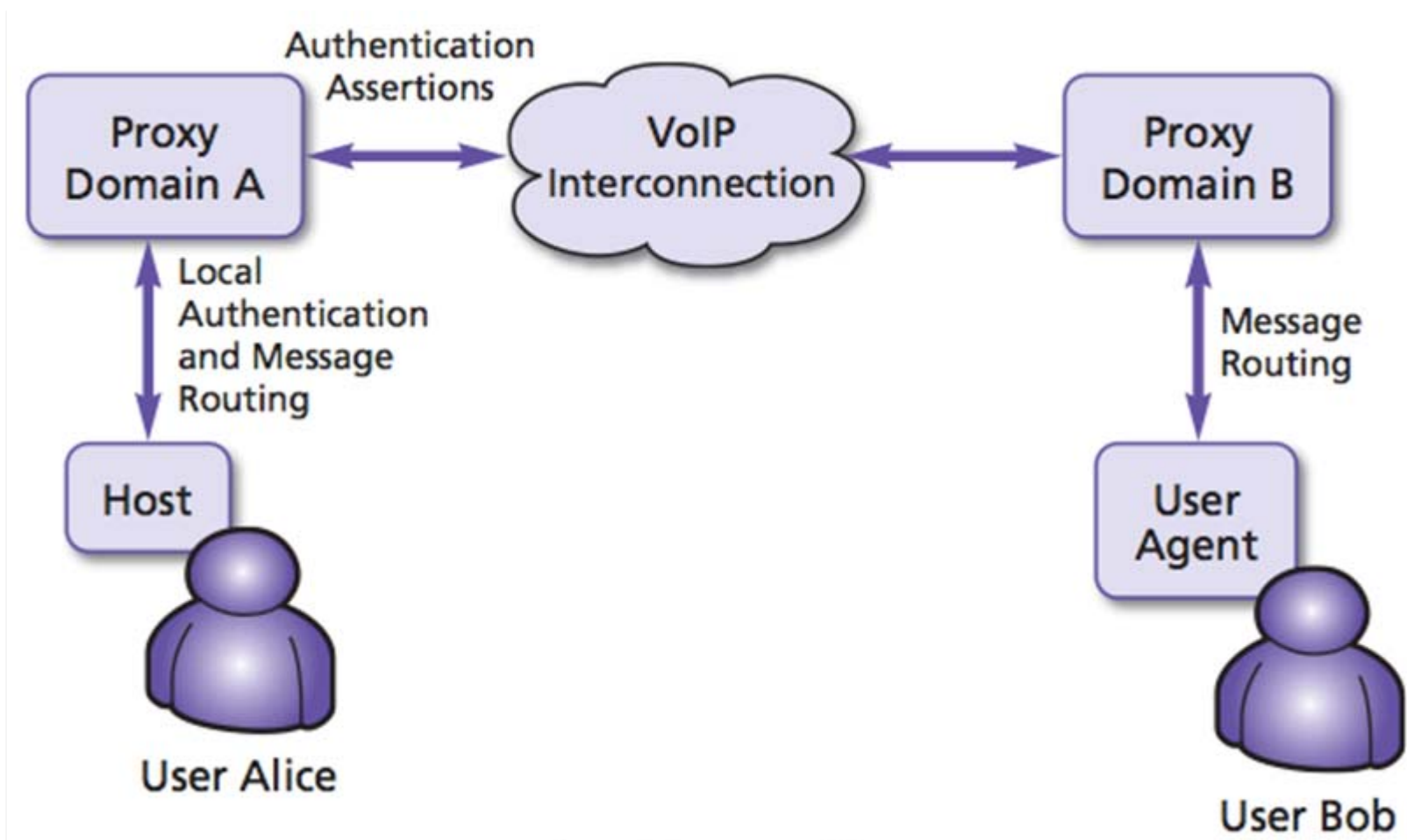
Credit Card System



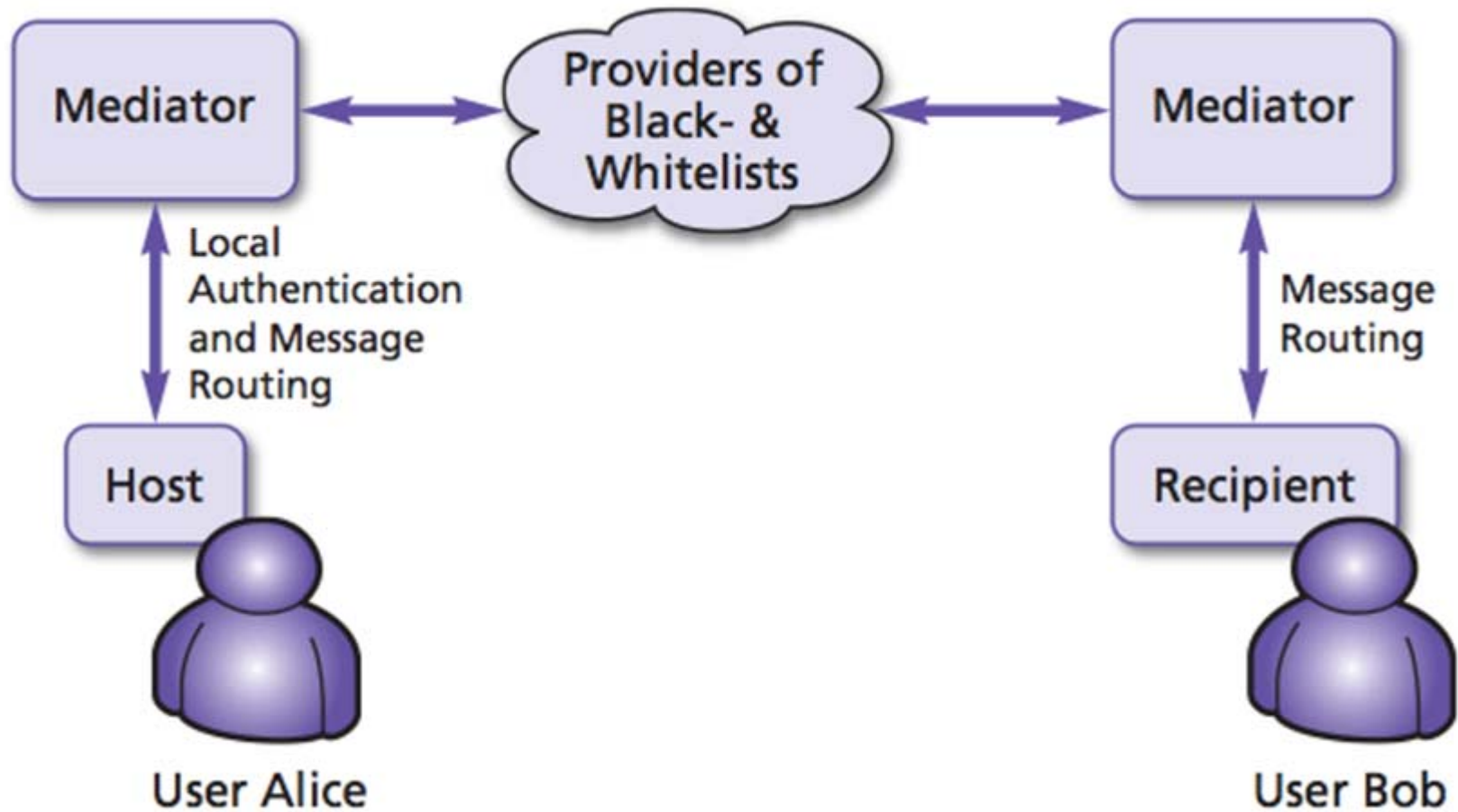
Network Access Authentication



Voice over IP



Email



Summary

- Technology (and also terminology) varies for each trust framework.
- Not only technical aspects matter.
- Legal and business constructs vary heavily as well
 - Different incentive systems
 - Regulatory rules depend on type of data
 - Different level of contractual requirements.
- Balance between “operational specifications” and “legal rules” varies in the different trust frameworks.
- Today’s trust frameworks are purpose built and changed incrementally over time
 - Not designed on a clean slate.
- Different views about the desirable properties of a trust framework

Recent Developments

- After the publication of the ENISA report pointing to the need to further research trust frameworks US government has launched a new initiative.
- Subsequent slides illustrate example of an ongoing efforts in the area of trust frameworks:
 - OMB M04-04
 - NIST SP 800-63
 - GSA ICAM
 - NSTIC

Office of Management and Budget (OMB) M04-04

- E-Authentication Guidance for Federal Agencies, Dec. 16, 2003
 - <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- First initiative focusing on C2G and B2G authentication
- Established four levels of assurance (based largely on a UK policy memo)
 - Level 1: Little or no confidence in the asserted identity's validity.
 - Level 2: Some confidence in the asserted identity's validity.
 - Level 3: High confidence in the asserted identity's validity.
 - Level 4: Very high confidence in the asserted identity's validity.
- Required NIST to publish technical guidance

NIST SP 800-63

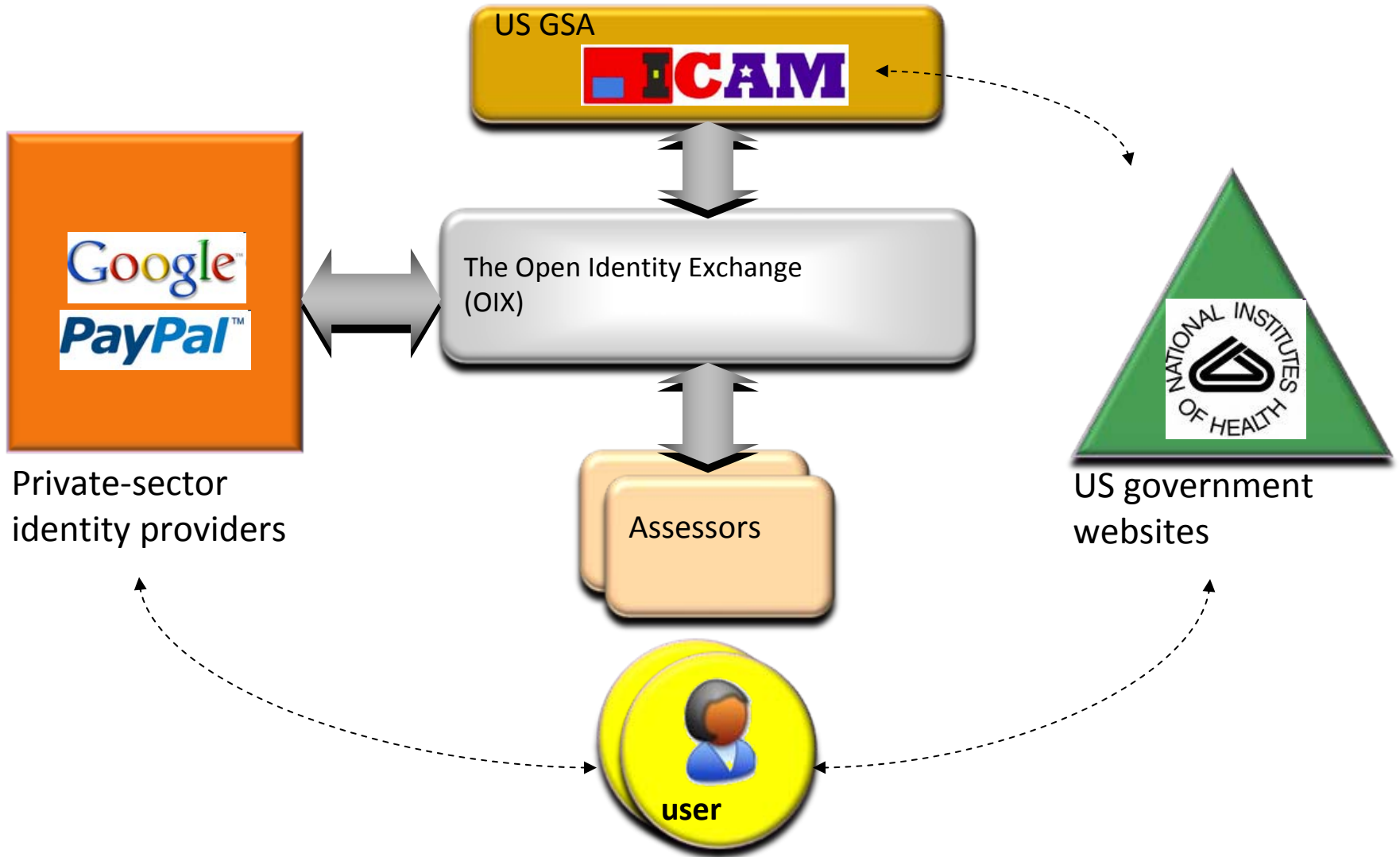
- In response to OMB 04-04, NIST developed SP 800-63 (released 2006; updated 2008) to provide a single framework for remote authentication over the Internet.
- http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf
- Included identity proofing, broad range of credentials (passwords, OTP, soft and hard PKI), and a variety of protocol requirements for the four levels of assurance
- Identity proofing has been the most difficult aspect for agencies
- Cost is also a factor at Levels 3 and 4.
 - Level 3 requires multifactor authentication.
 - Level 4 requires a hardware token (e.g., a smart card).

Identity, Credential and Access Management (ICAM) Policy Initiatives

- To support E-Government activities ICAM aims to leverage industry based credentials that citizens already have for other purposes.
 - Requirements aligned with NIST SP 800-63
- "Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3" document explains what government Relying Parties expect from Trust Framework Providers:
<http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf>
 - Describes what an assessment package from a TFP applicant has to provide.
 - Describes the process of reviewing the application
 - This has lead to the formation of the Open Identity Exchange (OIX) and the Kantara trust framework activities.
- ICAM has recognized OpenID providers, an InfoCard provider, and the InCommon Federation.



GSA ICAM Trust Framework



GSA ICAM, cont.

- A TFP is an organization that defines or adopts an on-line identity trust model and then certifies identity providers compliant with that model. Adoption means that any identity provider certified by that TFP is qualified to provide identity assertions to Federal agencies.
- There are five categories:
 - 1. **Registration and Issuance** – how well does the credential service provider (Identity Provider) register and proof the identity of the credential applicant, and issue the credential to the approved applicant?
 - 2. **Tokens** – What is the Identity Provider's token technology and how well does the technology intrinsically resist fraud, tampering, hacking, and other such attacks?
 - 3. **Token and Credential Management** – how well does the Identity Provider manage and protect tokens and credentials over their full life cycle?
 - 4. **Authentication Process** – how well does the Identity Provider secure its authentication protocol?
 - 5. **Assertions** – how well does the Identity Provider secure Assertions, if used, and how much information is provided in the Assertion?

Assessment Package

- Technical and policy based on different assurance levels
- Privacy Policy
 - Opt In: Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted.
 - Minimalism: Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile (based on E-Government Act of 2002).
 - Activity Tracking: Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication.
 - Adequate Notice: Identity Provider must provide End Users with adequate notice regarding federated authentication.
 - Non Compulsory: Agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.
 - Termination: In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.
- Determination of whether the Applicant sufficiently reviews member identity provider *bona fides* to ensure member identity provider organizational maturity, legitimacy, stability, and reputation.
- Audit Criteria Assessment

- OIX is a registry.
 - Identity providers fulfilling requirements of ICAM trust framework were the first listed entries in the registry.
- Per the Identity Scheme Adoption Process (ISAP) <http://www.idmanagement.gov/documents/IdentitySchemeAdoptionProcess.pdf> , ICAM determined that OpenID 2.0 was of sufficient value to adopt as an ICAM identity scheme. ICAM published version 1.0.1 of the OpenID 2.0 Profile on 18 November 2009, see
 - http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf
- ICAM published version 1.0.1 of the Identity Meta-System Interoperability 1.0 Profile on 18 November 2009, see
 - http://www.idmanagement.gov/documents/ICAM_IMI_10_Profile.pdf
- Other available profiles listed at http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

OIX US ICAM LOA 1 Trust Framework

- OIX’s application submission is called “OIX US ICAM LOA 1 Trust Framework”

<http://openidentityexchange.org/sites/default/files/oix-us-icam-loa1-tfp-assessment-package-2010-02-12.pdf>

- Explains what conditions must be fulfilled in order for a Identity Provider to be approved by OIX as US ICAM LOA 1 Version 1.
- *Application provides information* TFPAP asks for, namely
 - OIX Organizational Maturity
 - OIX Review of Member Organizational Maturity
 - OIX US ICAM Privacy Requirements for Members
 - OIX Assessor Qualifications
 - OIX Process to Certify Members
 - OIX Process to Recertify Members
 - US ICAM LOA 1 V1 Trust Criteria

US ICAM LOA 1 Certified Identity Providers

The following OIX members are certified as identity providers for the [US ICAM LOA 1 trust framework](#):

Identity Provider	ICAM Profile	Listing Date	URI
Google	OpenID 2.0	2011-03-13	http://google.com
Equifax	IMI 1.0	2010-03-03	http://equifax.com
PayPal	OpenID 2.0	2010-03-03	http://paypal.com
PayPal	IMI 1.0	2010-03-03	http://paypal.com
VeriSign	OpenID 2.0	2010-03-29	http://pip.verisignlabs.com
Wave Systems	OpenID 2.0	2010-12-09	http://wave.com

US ICAM LOA 1 Listed Assessors

The following OIX members are listed assessors for the US ICAM LOA 1 trust framework:

John Steensen, MBA, CISA

- [Spatial Dynamics Corporation](#)
- jsteensen@spatialdynamicscorp.com
- (925) 413-6379

<http://openididentityexchange.org/certified-providers> (June 2011)

National Strategy for Trusted Identity in Cyberspace (NSTIC)

- Latest effort by the US government to stimulate the identity eco-system.
- Extends GSA ICAM scope to C2B and B2B (in addition to B2G, G2G)
- Strategy document available:
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

NSTIC:

A Vision for an Identity Eco-System

- The Identity Ecosystem **goes beyond passwords** and provides people with a variety of more secure and privacy-enhancing ways to access online services.
- People can validate their identities securely when they're doing sensitive transactions (like banking) and stay **anonymous** when they're not (like blogging).
- The Identity Ecosystem enhances individuals' privacy by **minimizing the information they must disclose** to authenticate themselves.
- The Identity Ecosystem is a vibrant marketplace that provides people with **choices among multiple identity providers** - both private and public - and **choices among multiple credentials**.
- Participating service providers will agree to **consistent standards** for identification, authentication, security, and privacy, giving people and institutions more trust online.
- *[liberally paraphrased from <http://www.nist.gov/nstic/>]*

Soliciting Feedback from Stakeholders

- Workshops:
 - First workshop in June 2011 (Washington DC) on governance, see <http://www.nist.gov/itl/nstic-workshop-june2011.cfm>
 - Second workshop late June 2011 (Boston) on privacy, see <http://www.nist.gov/itl/nstic-privacy-workshop.cfm>
 - Third workshop September 2011 (Bay area) on technology & standards
- Notice of Inquiry:
 - <http://www.nist.gov/nstic/nstic-frn-noi.pdf> (on governance)
- Plan is to establish a steering group with multi-stakeholder involvement.
- Pilot projects will be conducted.

Challenges

- Observations:
 - Identity proofing is the greatest impediment to issuing strong authentication credentials
 - In-person is expensive, online is weak without OOB confirmation
 - Organizations hate to issue strong credentials to customers, but don't mind managing passwords.
 - Pure authentication information is often insufficient for any practical purpose
- Incentive questions:
 - How to incentivize private sector to issue strong credentials?
 - How to encouraging private sector to accept strong credentials?
 - How to make sure that privacy is considered in designs (e.g. data minimalization)?

Summary

- Move away from passwords to stronger credentials has been difficult but is needed for improved Web security.
- Commercial sector has been slow in accepting credentials issued by other parties.
- Interaction between IdP and RP leads to privacy concerns
- Your help is needed. Participate in the technical area in the IETF on
 - WOES: <https://www.ietf.org/mailman/listinfo/woes>
 - OAuth: <http://datatracker.ietf.org/wg/oauth/>
 - WebSec: <http://datatracker.ietf.org/wg/websec/charter/>
 - HTTP-Auth: <https://www.ietf.org/mailman/listinfo/http-auth>
 - ABFAB: <http://datatracker.ietf.org/wg/abfab/>
 - KITTEN: <http://datatracker.ietf.org/wg/kitten>
- To the audience: What properties would be important for you?