OPEN IDENTITY EXCHANGE

A Market Solution to Online Identity Trust

OPEN IDENTITY EXCHANGE

Background

- OIX is an Internet-scale solution to the problem of how identity credentials can be trusted online.

"On the Internet, nobody knows you're a dog."

OPEN IDENTITY EXCHANGE

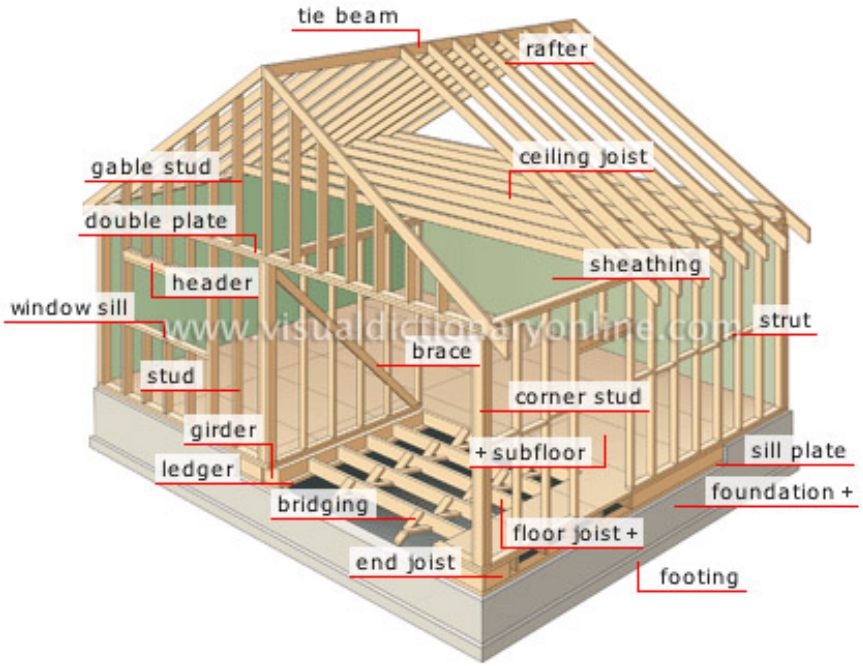
Background

"OIX is the organization where different parties across verticals such as federal, Telco, and healthcare, can come together to address policy challenges through the creation of vertical **trust frameworks**."

- Nico Popp, VP Identity and Authentication Services, Symantec
OIX Founding Board Member

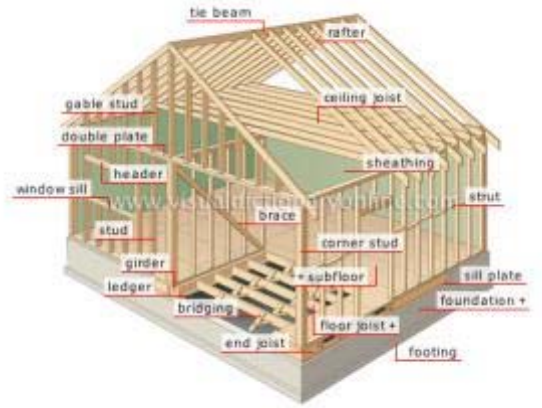
Thinking "Frameworks"

A house is made up of a number of framework components



Components of a Trust Framework

- Means and Protocol for Communication
  - the data necessary to initiate the communication (the "**question**")
  - the information returned (the "**answer**")
- Documentation of
  - "**Levels of Protection**" a given service must afford the identity provider
  - "**Levels of Assurance**" a given service provides the entity relying upon the service
  - "**Levels of Control**" afforded the party or entity about whom the communication references.



Trust Framework components include: Descriptions, Definitions & Documentation

OPEN IDENTITY EXCHANGE

Components of Trust Frameworks

Consists of:

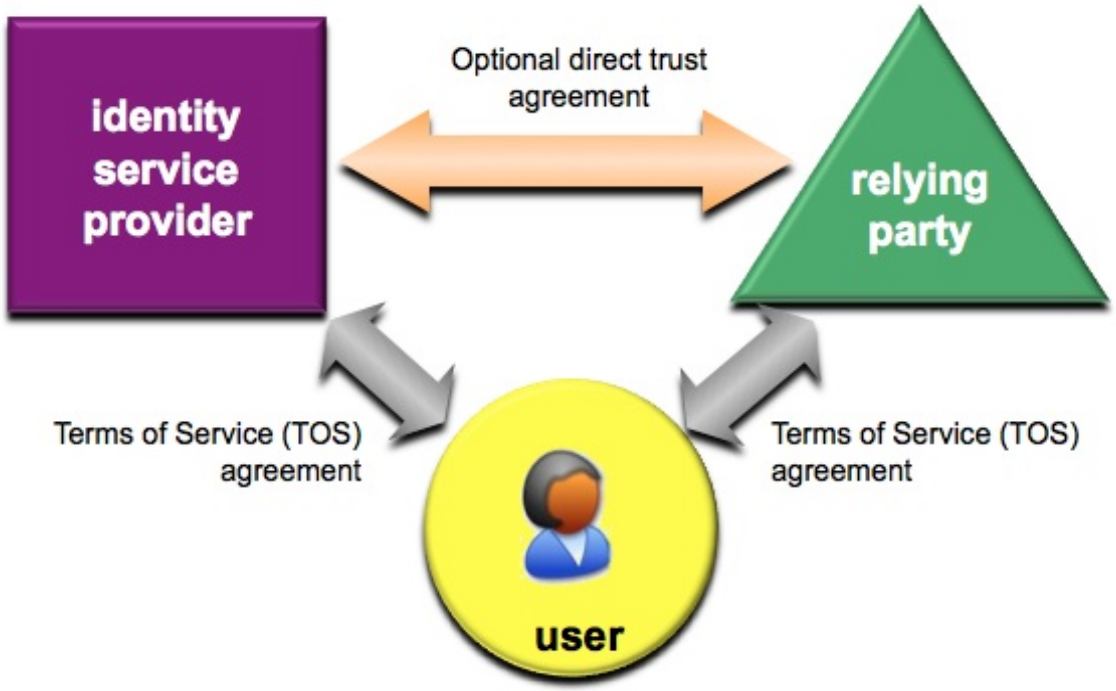
Policy “Rules” are specific legal duties like privacy protection.

Assurance includes assessment & certification procedures

Technology “Tools” are specific protocols like the OpenID 2.O standard.

A Basic "Trust Triangle"

Looking at it in context:

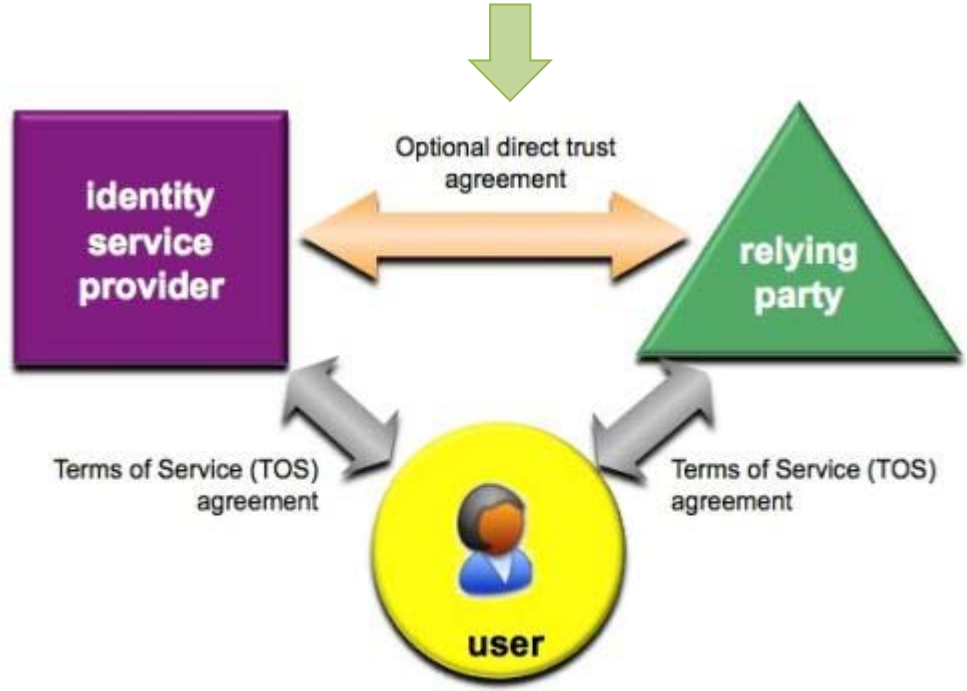


The user has a direct trust relationship with both the **identity service provider** and the **relying party**.

A Basic "Trust Triangle"

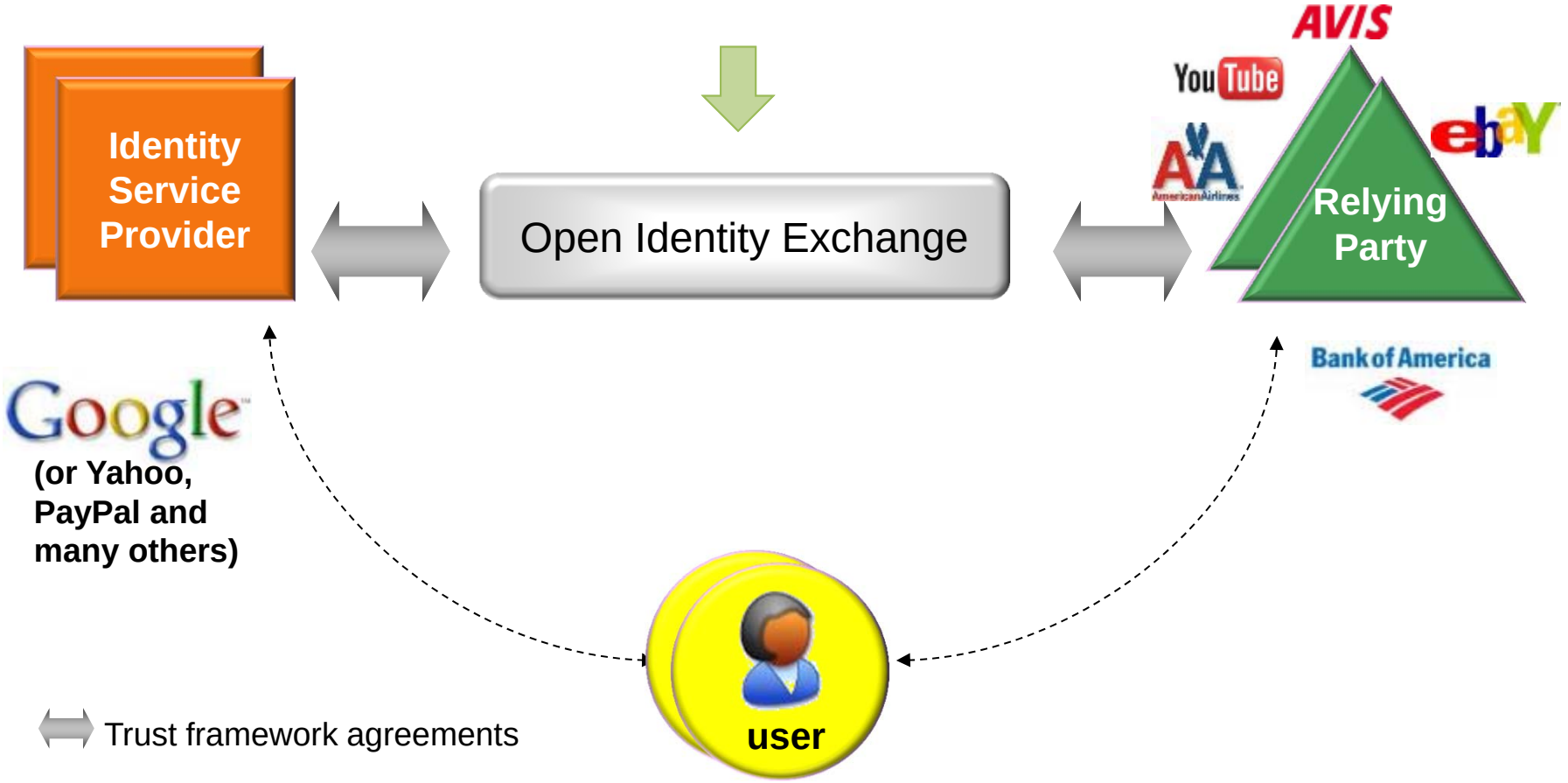
Looking at it in context:

How can the identity service provider and relying party trust each other?



The OIX Identity Trust Framework Model

Here's how:

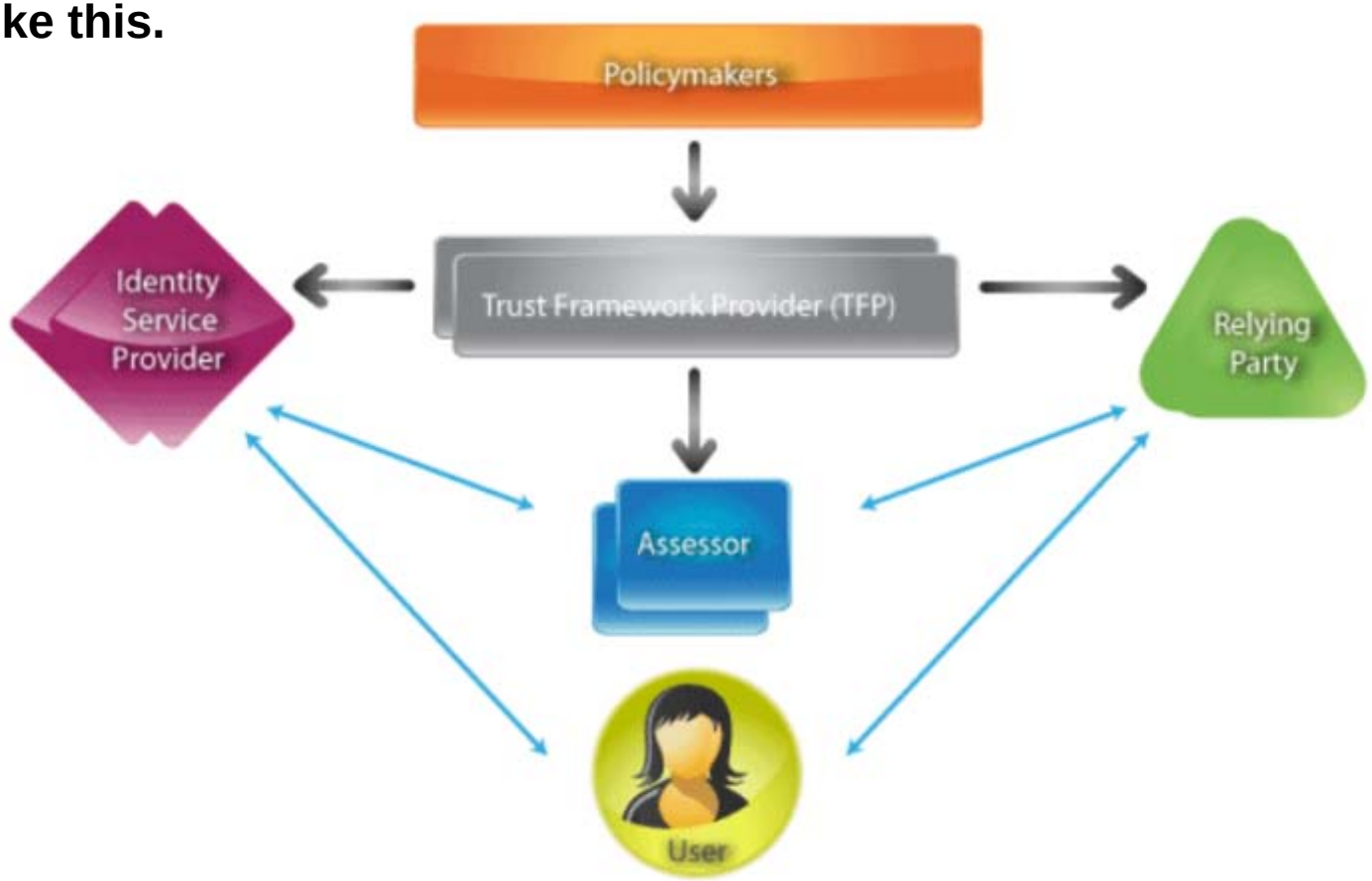


Interoperability is Key

- OIX Trust Frameworks reduce friction of using the web through **interoperability of digital identities**
  - Convenience/ease-of-use leads to increases e-commerce opportunities
  - Strengthens **Consumer confidence** in privacy and protection of personal data.

Open Identity Trust Framework

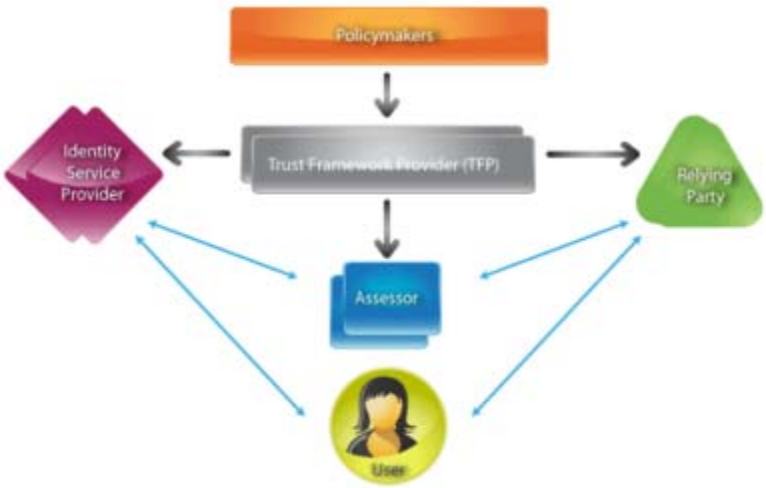
Looks like this.



Open Identity Trust Framework

Defined:

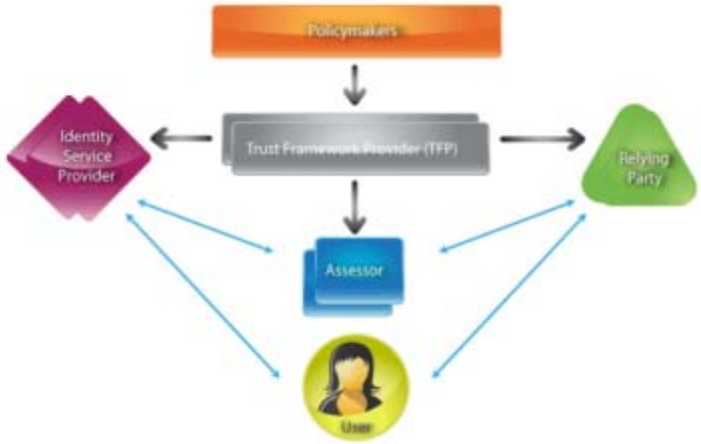
- **Open:** participation is opt-in, market driven, and transparent
- **Identity:** authentication is a critical requirement for market growth and new web services
- **Trust:** results from reliable and repeatable transactions
- **Frameworks:** are systems for technical and policy interoperability



Open Identity Trust Framework

Defined:

- **User/Consumer** - person or entity who is identifying themselves as a valid user of the system.
- **Identity Provider** - The entity that provides a representation of a user of some system.
  - i.e. Google, PayPal, Facebook
- **Relying Party:** An entity that depends on the assertions of an identity provider when making decisions about users.
  - i.e. Banks, Airlines, YouTube, eBay, Amazon



Note: The roles are not necessarily constant and entities may change roles or assume multiple roles depending on the nature of transaction.

Open Identity Trust Framework

What they want:

- **Consumers** want:
  - Privacy & Protection of their personal data
  - Control of and benefit from the use of their personal data
  - Comfort level with Relying Party based on previous experiences

Open Identity Trust Framework

What they want:

- **Identity Service Providers** want:
  - To assure **Relying Parties** and **Users** that they are accurately representing identities AND that **privacy** is appropriately protected.
  - Access to **Best Practices.**
  - Their approach recognized/noted as **appropriate.**

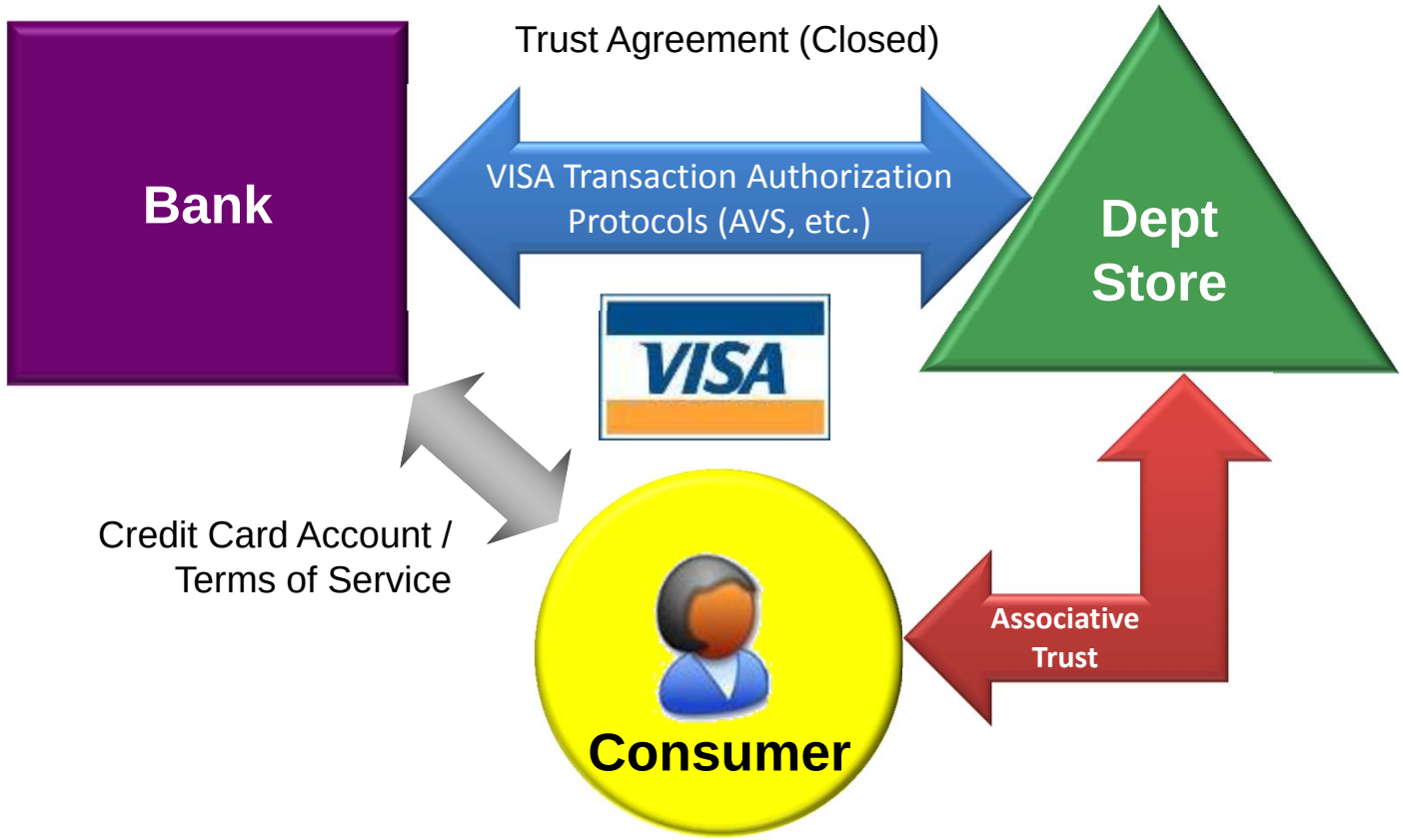
Google PayPal facebook

Open Identity Trust Framework

What they want:

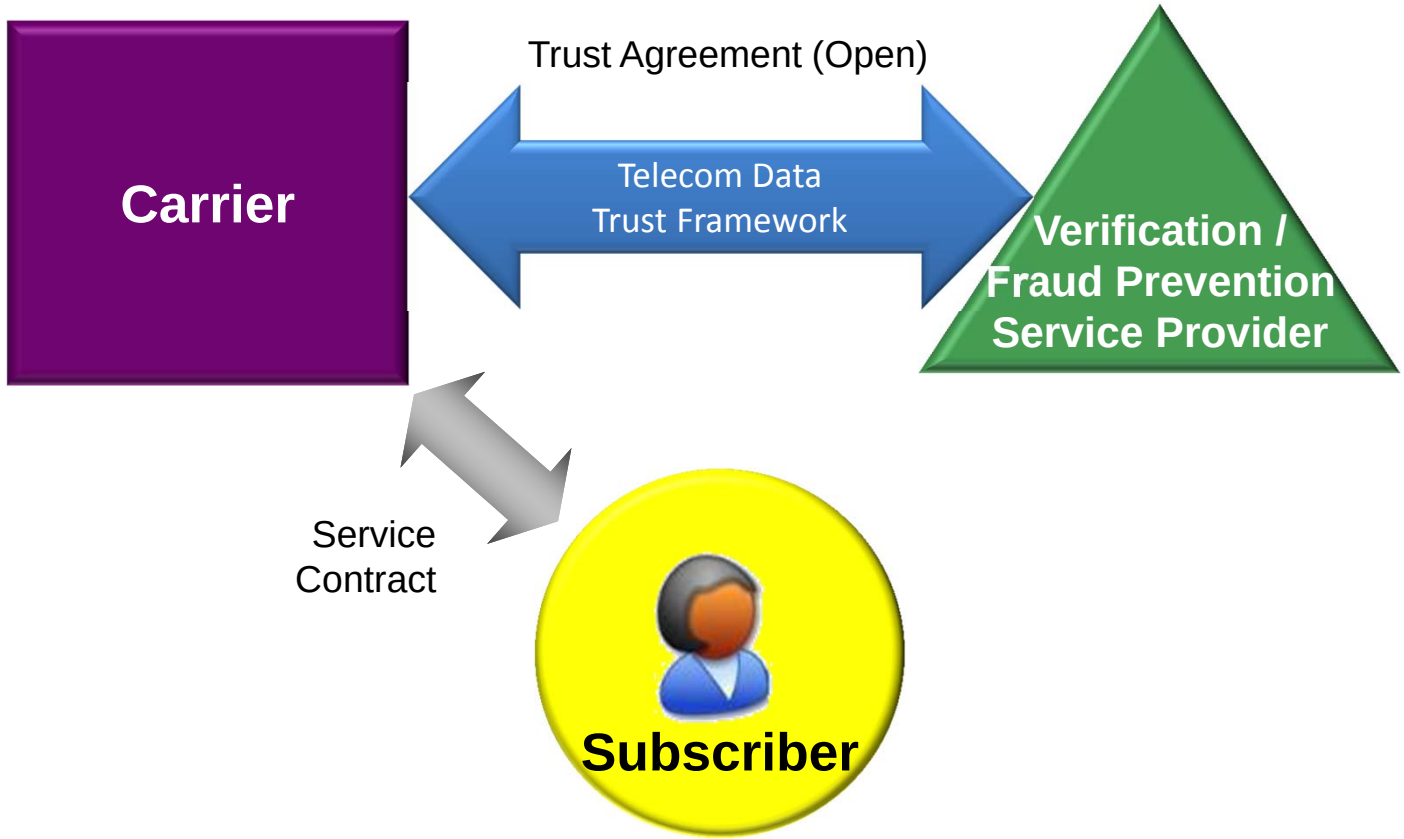
- **Relying Parties** want:
  - Assurances that the identity presented is valid and data associated is accurate.
  - To drive **Rules & Tools**.
  - Access to **Best Practices.**
    - Including **Trust Frameworks**

A Familiar Trust Framework - VISA



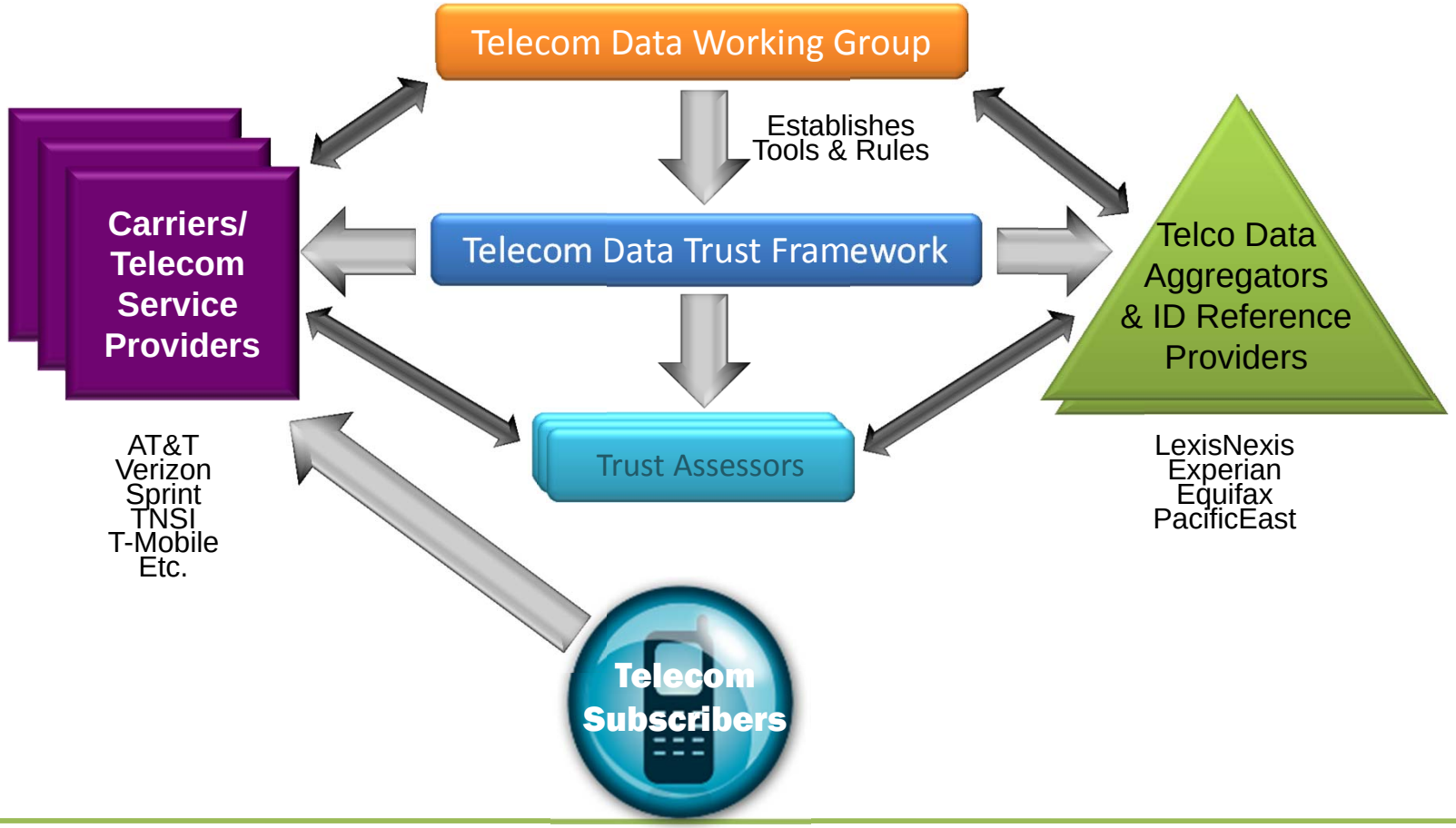
A Possible Trust Framework

Telecommunications – Top Level:



A Possible Trust Framework

Telecommunications – Built out:



Online/eCommerce Requires Trust

"The Internet will not reach its full potential until users and consumers feel more secure and confident than they do today when they go online. A coordinated national strategy to significantly improve online trust will put e-commerce on stronger footing."

– Commerce Secretary Gary Locke (Jan 2011)

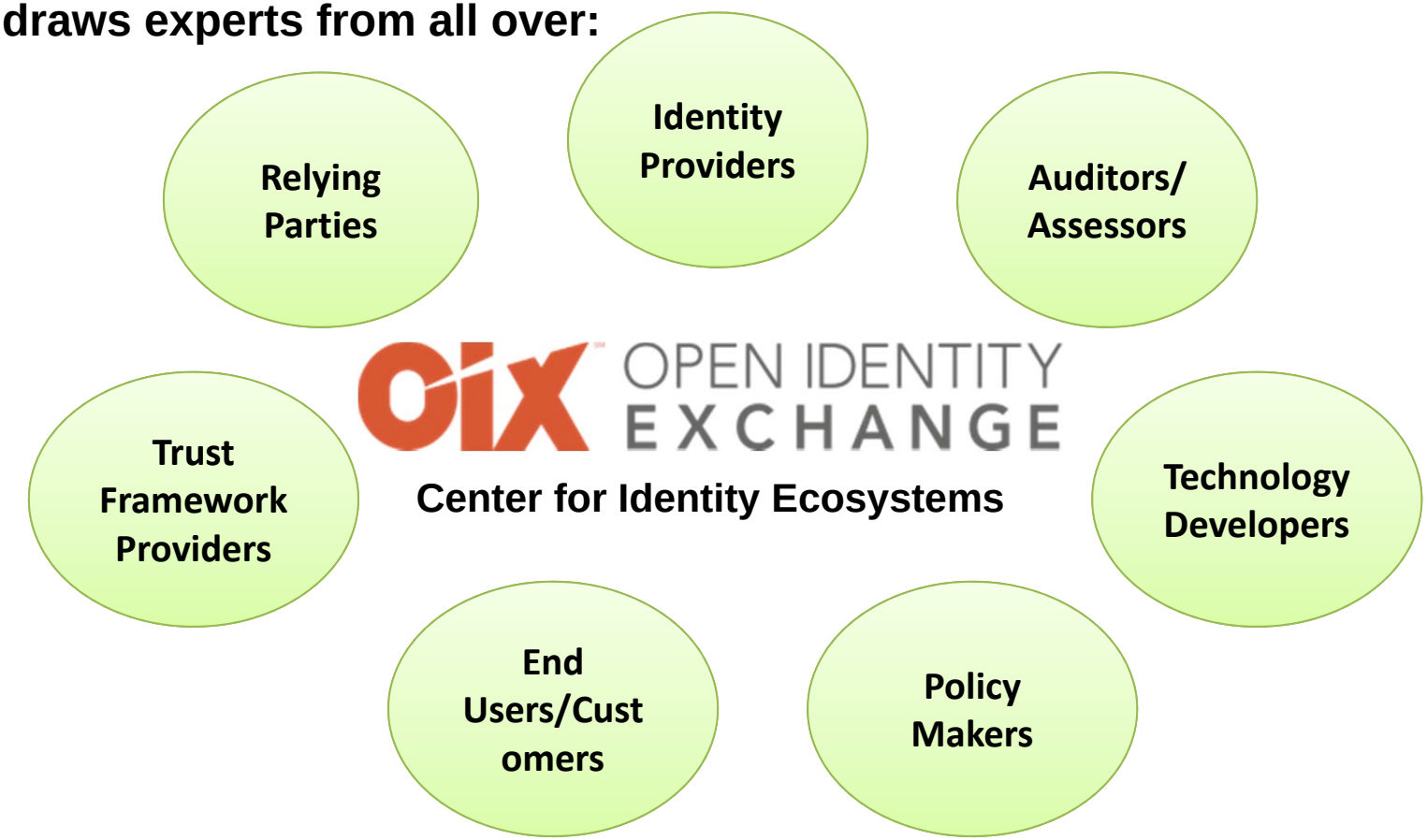
OIX OPEN IDENTITY EXCHANGE

Leading the Charge

- **Helps Build Trust Frameworks**
  - "Telecom Data Working Group"
  - "Email Attribute Working Group"
- **Offers Valuable Resources**
  - OIX Knowledge Center for best practices learning and discussion
  - OIX Technology Center for technical interoperability
  - Thought Leadership
- **Certifies Compliance**
  - Directly for "US Government ICAM Framework"
  - And with others like Kantara, and iScheme

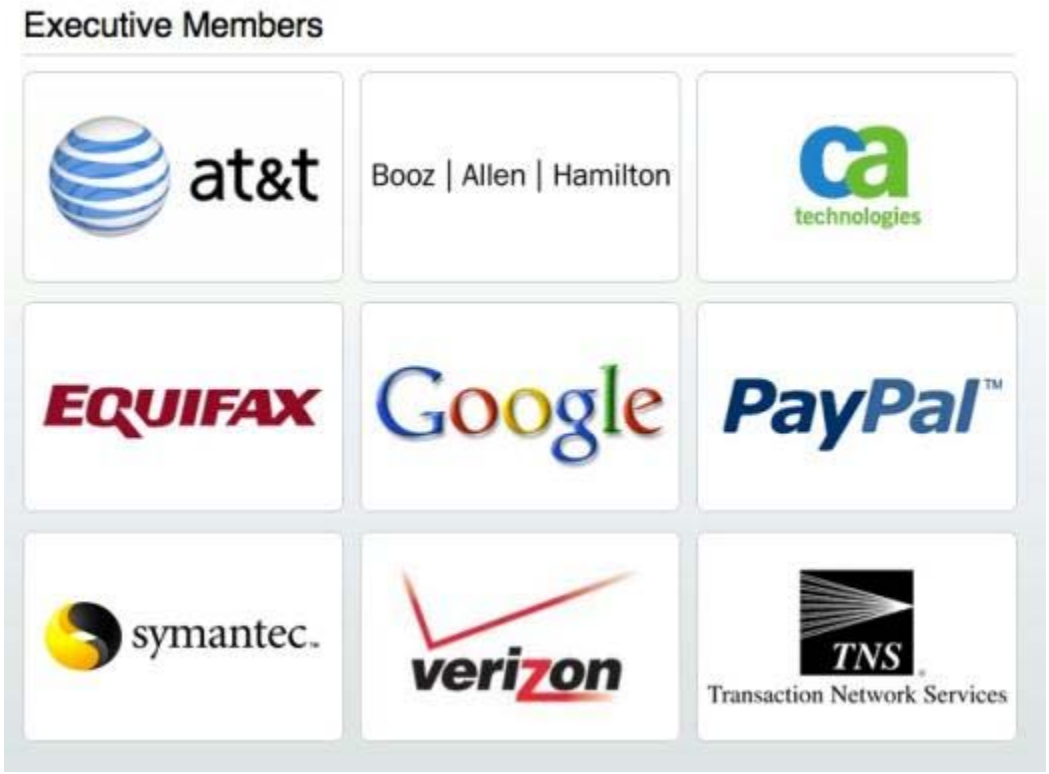
Leading the Charge

OIX draws experts from all over:



Leading the Charge

OPEN IDENTITY EXCHANGE



Driving Adoption

OPEN IDENTITY EXCHANGE

Ready to get involved?

Are you interested in getting involved in the OIX community to help shape the future of digital identity?

To learn more about Trust Frameworks and OIX, go to:

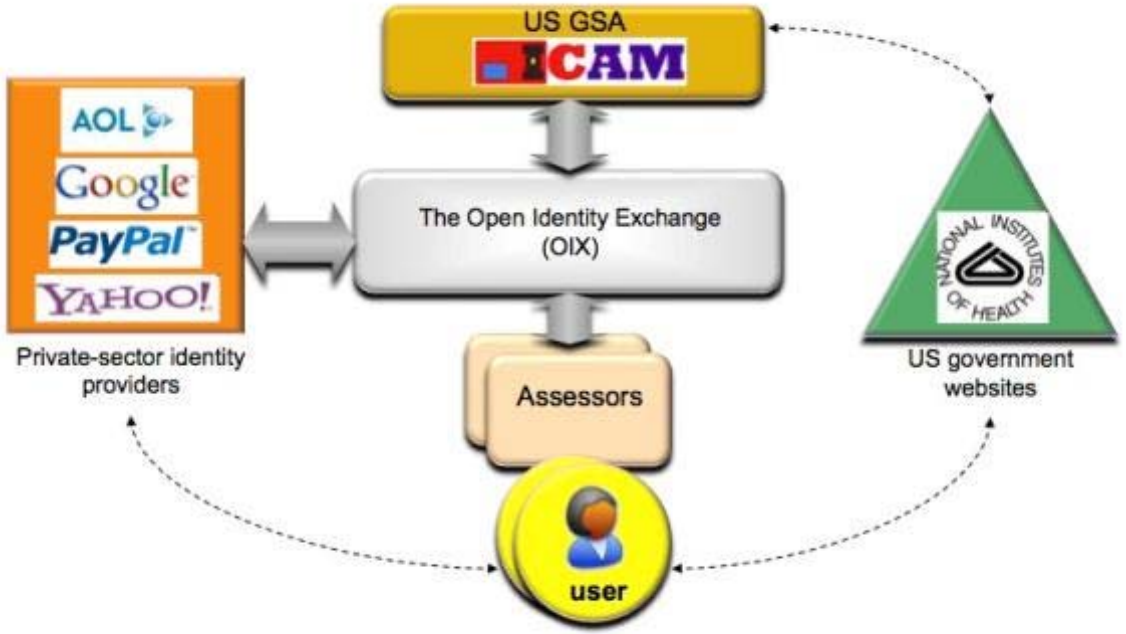
http://openidentityexchange.org

OPEN IDENTITY EXCHANGE

A Market Solution to Online Identity Trust

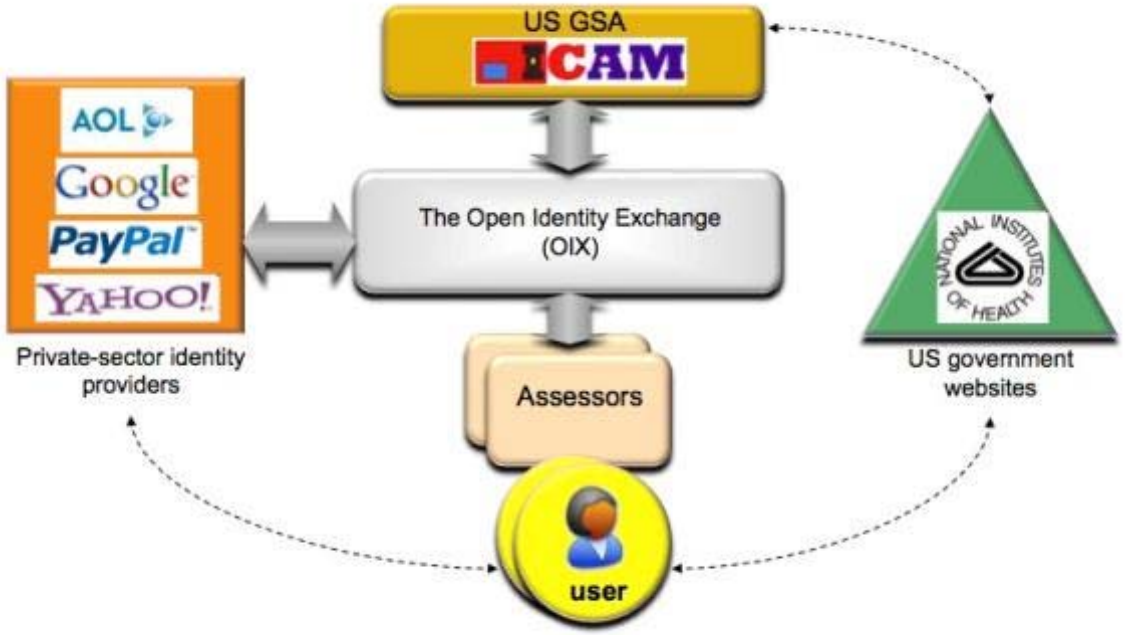
Bonus Slides…

The US ICAM Trust Framework



- First example of OIX Trust Frameworks developed in conjunction with the U.S. GSA on behalf of the Identity Credential, and Access Management (ICAM) subcommittee of the U.S. CIO Council.

The US ICAM Trust Framework



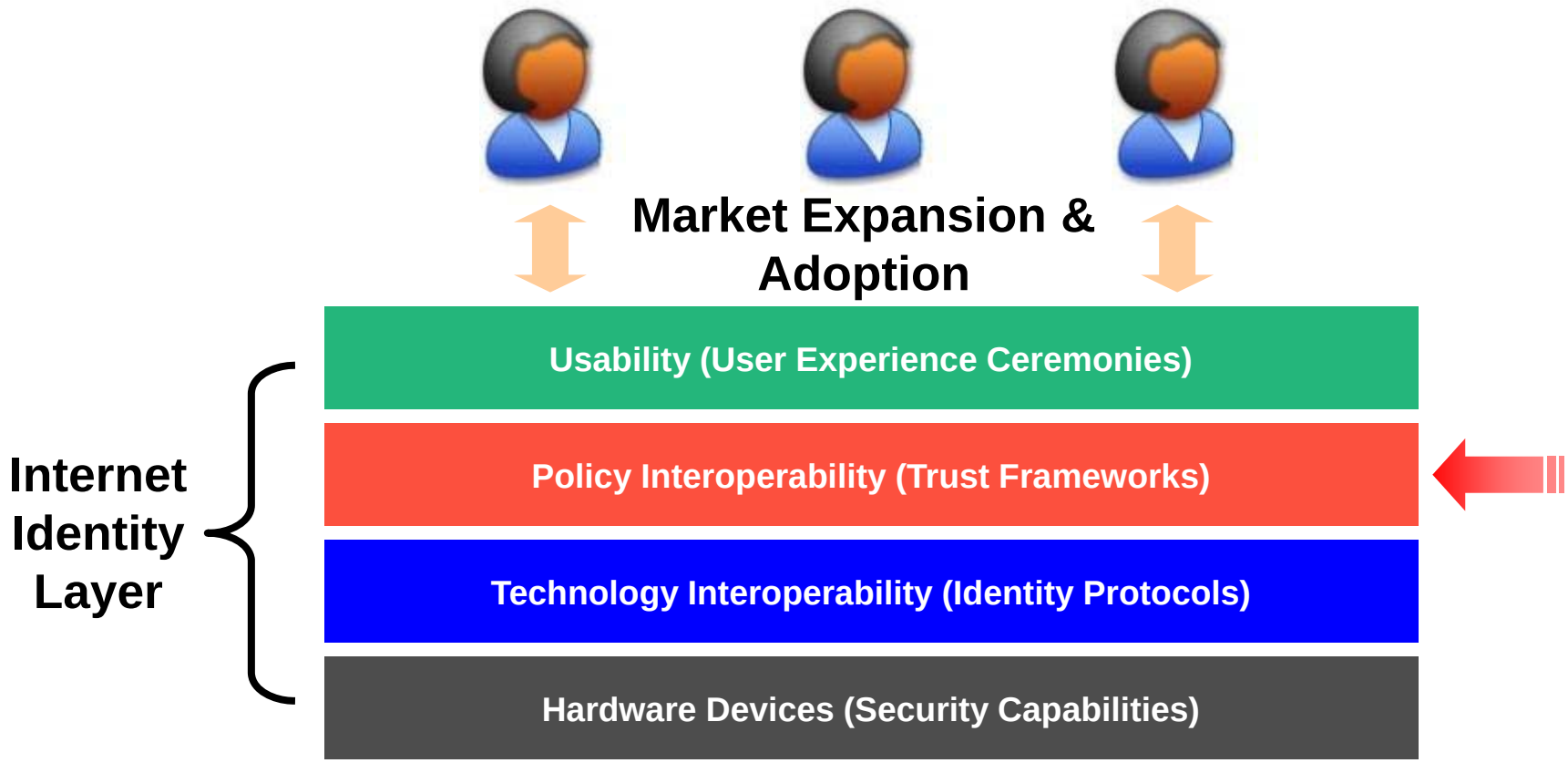
- Designed to meet the first of the four LOAs defined by the ICAM Trust Framework Provider Adoption Process (TFPAP), the OIX US ICAM LOA 1 trust framework was approved by ICAM on 15 February 2010 and went operational on 3 March 2010.

The US ICAM Trust Framework

- The US ICAM LOA 1 trust framework enables U.S. federal agency websites, such as the National Institute of Health (NIH), the National Library of Medicine (NLM), and the Library of Congress (LOC), to begin accepting OpenID and Information Card credentials from OIX certified private-industry providers.

- **Milestone of note:** July 27, 2010, OIX announced formation of the ***US ICAM Trust Framework Working Group*** to extend the OIX US ICAM Trust Framework specification to LOA 2 and Non-PKI 3.

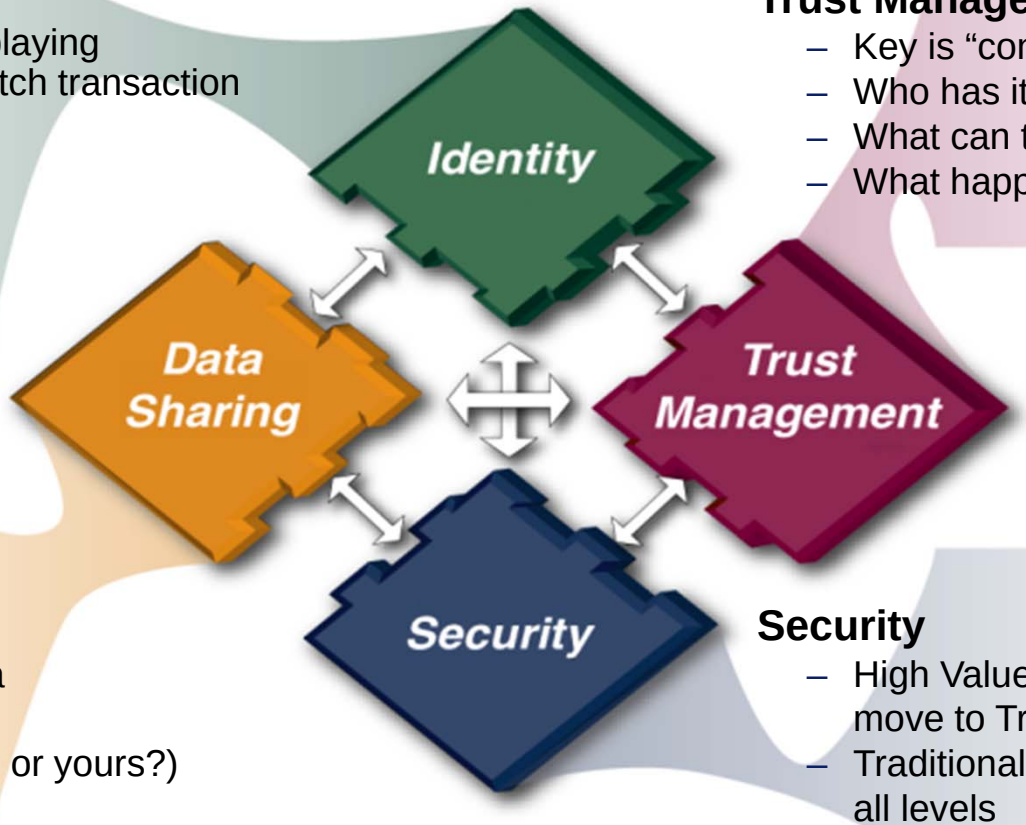
Where trust frameworks fit



Four critical components when enabling a Trust Network

Identity
- Must know “who” is playing
- Identity attributes match transaction
- Multiple layers
- Multiple technologies

Trust Management
- Key is “control”
- Who has it
- What can they do
- What happens in breach



Data Sharing
- Who contributes data
- Who can use it
- Where is it (my cloud or yours?)
- Who can take it
- What happens in the future

Security
- High Value transactions move to Trust Network
- Traditional security applies at all levels