Identity Assurance and your Real World Identity

Andrew Nash
Senior Director of Identity Services
THE BIG BANG THEORY

1. The cosmos goes through a superfast "inflation," expanding from the size of an atom to that of a grapefruit in a tiny fraction of a second.

2. Post-inflation, the universe is a seething, hot soup of electrons, quarks and other particles.

3. A rapidly cooling cosmos permits quarks to clump into protons and neutrons.

4. Still too hot to form into atoms, charged electrons and protons prevent light from shining; the universe is a superhot fog.

5. Electrons combine with protons and neutrons to form atoms, mostly hydrogen and helium. Light can finally shine.

6. Gravity makes hydrogen and helium gas coalesce to form the giant clouds that will become galaxies; smaller clumps of gas collapse to form the first stars.

7. As galaxies cluster together under gravity, the first stars die and spew heavy elements into space; these will eventually form into new stars and planets.

NOTE: The numbers in cosmology are so great and the numbers in subatomic physics are so small that it is often necessary to express them in exponential form. Ten multiplied by itself, or 100, is written as 10². One thousand is written as 10³. Similarly, one-tenth is 10⁻¹, and one-hundredth is 10⁻².
Internet Consumer Identity ... Yesterday?

Consumer Internet interactions are repetitive, frustrating and littered with outdated info.
Consumer Trust and Safety

Yes, I'm calling from your local utility to confirm some information... could I have your date of birth, social security number and any credit cards or bank accounts please?
Identity Evolution
Finally Addressing the Consumer

Enterprise Centric

1

Federated Partners

2

User Centric

3

Social Networks

Mashups

Tagging

e-commerce

Finance

Web 2.0

PayPal
Transactional Opportunity

cookies
historical
data

Fraud/Risk
Reduction

Reduced
Friction

Targeted
Marketing

Increased
Checkout
Completion

Consumer
Claims

checkout-time
identity

PayPal
identity service
The Identity Trust Gradient

- Low Value
- High Value
- None
- Extreme

Transaction “value”

Regulatory / Compliance / Risk

Blogs
Social Networks
Shopping
Financial
Health
Intelligence Agency

PayPal
Identity Assurance Frameworks

• Kantara (and others)
  – Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations

• It consists of 4 parts:
  – Assurance Levels
  – Service Assessment Criteria
  – Accreditation and Certification Model
  – Business Rules
US Federal Govt Assurance Levels

<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>Example</th>
<th>Assessment Criteria – Organization</th>
<th>Assessment Criteria – Identity Proofing</th>
<th>Assessment Criteria – Face-to-Face or Multiple Forms of Govt Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL 1</td>
<td>Registration to a news website</td>
<td>Minimal Organizational criteria</td>
<td>Minimal criteria - Self assertion</td>
<td></td>
</tr>
<tr>
<td>AL 2</td>
<td>Change of address of record by beneficiary</td>
<td>Moderate organizational criteria</td>
<td>Moderate criteria - Attestation of Govt. ID</td>
<td></td>
</tr>
<tr>
<td>AL 3</td>
<td>Access to an online brokerage account</td>
<td>Stringent organizational criteria</td>
<td>Stringent criteria – stronger attestation and verification of records</td>
<td>Multi-factor auth; Cryptographic protocol; “soft”, “hard”, or “OTP” tokens</td>
</tr>
<tr>
<td>AL 4</td>
<td>Dispensation of a controlled drug or $1mm bank wire</td>
<td>Stringent organizational criteria</td>
<td>More stringent criteria – stronger attestation and verification</td>
<td>Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process</td>
</tr>
</tbody>
</table>
So how is it, that…

- Anonymity with user attributes is acceptable?
  - One time credit card #
    + shipping address
    = product shipment
So how is it, that...

- You can perform a transaction with a high level of assured identity but low authentication
  - E-commerce
  - Library borrowing
So how is it…

• A digital representation of me is sufficient in many (most?) cases as opposed to my real world identity

• Additional conversation at:
  
  http://www.xmlgrrl.com/blog/2009/12/31/how-to-rest-assured/

  http://connectid.blogspot.com/2010/01/taxonomy-of-federated-applications.html
Well for a start …

- There should be a lot more levels between AL1 and AL2
- Pseudo-anonymity should have much broader acceptance (maybe at all levels)
- In broad e-commerce transactional domains a level 1.x may be the 80% case
- Even government e-commerce transactions probably don’t have to know who you are
But maybe mostly because …

- The model fails to account for risk based processing
- Financial institutions and most commerce sites apply a set of risk based evaluation rules
But maybe mostly because …

- Unlike NIST, risk based systems are not a one time identity proofing exercise

- Continual verification of identity “goodness”
  - Context, transaction history, behavior, …

- Enhancement to authentication
  - Triggers for step-up authentication
US Federal Privacy Policy

• Informed Consent
  – Define default information to be released to RPs
  – Should provide ability to deny release of certain attributes

• Abstract Identifier
  – Where PII not required

• Minimal Transmission
  – No more attrib than required shared

• Activity Tracking
  – Not disclosed to other parties
User Managed Access

http://kantarainitiative.org/confluence/display/uma/UMA+Explained
UMA Dashboard

http://kantarainitiative.org/confluence/display/uma/User+Experience
Role of IDP?

Consumer Agreements

- "All information should be free"
- "Help keep me safe"
- "I am very privacy conscious"

Relying Party Contracts

- "Anonymous is ok"
- "Moderate levels of private information"
- "Assurance Level 3"

Information Classification

Attribute Providers

"PayPal"
Credit Card Analog

- Credit cards evolved a similar if more complex ecosystem
- Consumer and Merchant agreements with penalties
- Caveat Emptor
  - Credit card system is in a steady state
  - VERY different world during startup phase
  - Features now available were not economically viable during the equivalent credit card big bang
Consumer IDP as Consumer Advocate

- Consumer IDP must be focused on:
  - The success of their users
  - Privacy and Control
  - Usability

- Anonymity – the cut case

- Consumer Control / Permission
  - Tools and protocols necessary but not sufficient condition
  - Consumer information classification
    - What does the consumer think is sensitive?
    - What are the trigger conditions?

- Notification
  - Exception reporting in human terms

- Auditing
  - “Just where did I go last week…?”
The Three Laws of Consumer IDP’s???

1. An IDP may not injure a consumer, or through inaction, allow a consumer to come to harm.

2. An IDP must obey orders given by consumers, except where such orders would conflict with the First Law.

3. An IDP must protect its own existence as long as such protection does not conflict with the First or Second Law.
Unpaid Plug