Identity
Agenda

• Goals

• Terminology

• What can decentralized networks contribute?
  – Better Identity Provider
  – Public attestation
Goals
What are we trying to solve?

• **Authentication**
  How can users securely authorize transactions?

• **Attestation**
  How can we enable users to prove their trustworthiness?
Our role
W3C Web Payments Community Group

- We’re not *identity* experts. We’re *payments* experts.
- What are our *unique challenges* around identity?
- How does the emergence of *distributed networks* affect identity?
### Terminology

<table>
<thead>
<tr>
<th>Entity</th>
<th>Identity</th>
<th>Identity Provider (IdP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="mailto:mark@gmail.com">mark@gmail.com</a></td>
<td>Google</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mark@safeway.com">mark@safeway.com</a></td>
<td>Safeway</td>
</tr>
<tr>
<td></td>
<td>TheMark72</td>
<td>Xbox Live</td>
</tr>
</tbody>
</table>

Reference: ISO 29115; OpenID Connect 1.0 Core
## Terminology

<table>
<thead>
<tr>
<th>Identity</th>
<th>Claim</th>
<th>Claim Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mark@gmail.com">mark@gmail.com</a></td>
<td>name: “Mark Dinkel”</td>
<td>Jumio</td>
</tr>
<tr>
<td><a href="mailto:mark@safeway.com">mark@safeway.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TheMark72</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reference: draft-ietf-oauth-json-web-token-19; OpenID Connect 1.0 Core
Advantages
The good news first

OpenID Connect is pretty good!

- Authentication mechanism agnostic
- Cryptographically secure
- Granular sharing of information and permissions
- Supports discovery
Reliance on IdPs

Why care?

- They are a target
- Difficult to switch
- Right to own your identity
Self-issued IdP

The other option

- OpenID Connect 1.0 Core - Section 7
- https://self-issued.me
- Suggested use case: Mobile phone
- Open issues: backup, security
Peer-assisted Key Derivation (PAKDF)

Trustless login using blind signatures

Reference: justmoon.github.io/pakdf
Peer-assisted Key Derivation (PAKDF)

Trustless login using blind signatures

- Full benefits of identity provider (multi-factor authentication, rate-limiting, fingerprinting)
- If using multiple peers provides strong protections against bad IdPs
Switching providers

Global distributed namespace

~alice
acmebank.com
\text{rNb721TdNHN37yoURrMYDiQ}

alice@acmebank.com

Stefan Thomas, CTO
Switching providers

Global distributed namespace

~alice

foobank.com

rNb721TdNHN37yoURrMYDiQ

alice@foobank.com
Service Discovery

How to pay alice?

Reference: RFC 7033 WebFinger

[{
    "uri": "ripple:12345-004-12341234567@eft.rippleunion.com",
    "currency": "CAD"
}, {
    "uri": "ripple:rNb721TdNHn37yoURrMYDiQF?dt=1234",
    "currency": "BTC"
}, ...]
## Reputation

<table>
<thead>
<tr>
<th>Identity</th>
<th>Claim</th>
<th>Claim Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mark@gmail.com">mark@gmail.com</a></td>
<td>name: “Mark Dinkel”</td>
<td>Jumio®</td>
</tr>
</tbody>
</table>

Reference: draft-ietf-oauth-json-web-token-19; OpenID Connect 1.0 Core
Mark@gmail.com

Claim:

{
  reviewer: "bob@live.com",
  score: 9.5,
  comment: "Great guy!"
}
Reputation

Identity

Claim

Score Provider

mark@gmail.com

804
low risk