

Microsoft and the Identity Metasystem

Dr. Stefan Brands

Principal Architect

Identity & Security Division

January 27, 2009

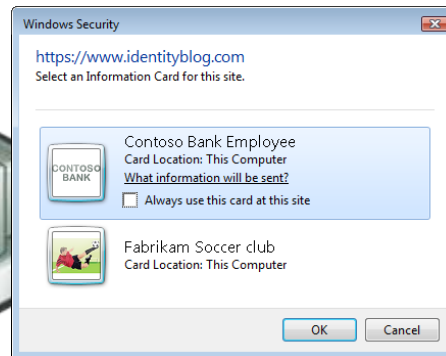
Claims-based identity



Name: Alice Smith



Who are you?



Microsoft's Geneva platform

- "Geneva" Server
 - Security Token Service (STS) for AD DS
 - Issues SAML 1.1 and 2.0 tokens
- "Geneva" Framework
 - Build claims-aware applications and STSes
 - SAML 2.0 protocol, WS-Federation Web SSO, ...
- Windows CardSpace "Geneva"
 - Identity selector (interoperability profile)
 - Information Card Foundation

Why an identity/claim selector ?

- Home realm discovery
- Improved protection against phishing
- User-generated key pairs
 - Can prevent impersonation by IdP
- Improved availability, security, and privacy
 - Long-lived claims
 - Minimum disclosure
 - No unwanted linkages
 - Observer-protected tokens
 - And more ...



U-Prove tokens



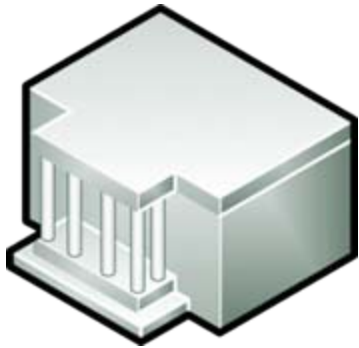
Name: Alice Smith

Address: 1234 Pine, Seattle, WA

D.O.B.: 23-11-1955



U-Prove tokens





???

Which person from WA is this?

In what state do you live?



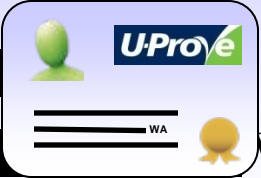





Name: [REDACTED]

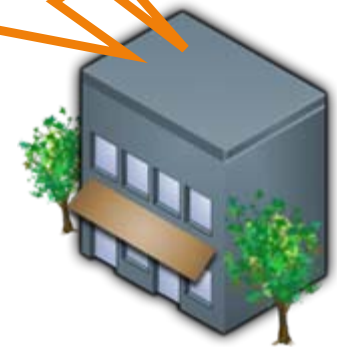
Address: [REDACTED]

D.O.B: [REDACTED]

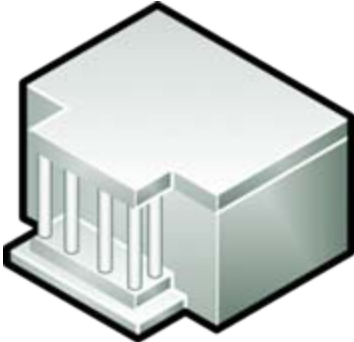





WA



Derived claims





Are you over 21?

 **U-Prove**

Name: [Redacted]

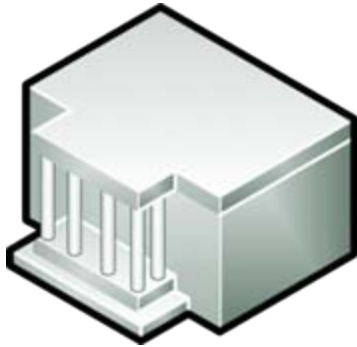
Address: [Redacted]

D.O.B: [Redacted] **Over-21 proof**



Issuer-driven revocation



Blacklist

Name 1
Name 2
...

Prove that
you are from
WA and over
21



U-Prove

Name: **Not-on-blacklist proof**

Address: [redacted] WA




Status: **Over-21 proof**



User-signed audit





A customer
from Seattle
visits



Name: [Redacted]

Address: [Redacted] Seattle, WA

Status: [Redacted]



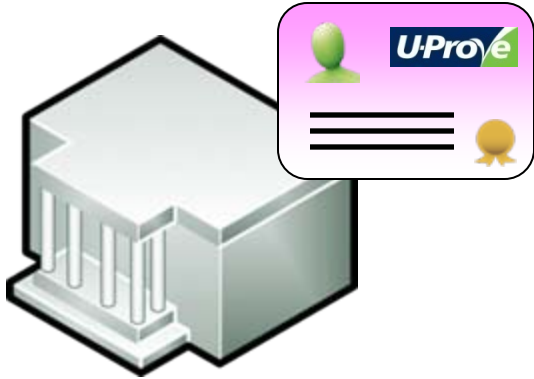
Name: Alice Smith

Address: 1234 Pine, Seattle, WA

Status: [Redacted]



Device-protected tokens



Integration into Windows

Geneva (CardSpace,
Framework, and Server)



**Windows
Communication
Foundation**

Microsoft
.net Framework

Learn more

Audio & video:

- http://www.credentica.com/intro_video.html
- http://www.chyp.com/podcasts/DIF_020_Stefan_Brands.mp3
- <http://www.credentica.com/files/MIX06-IdentityPanel.wmv>
- http://www.credentica.com/files/privacy_by_design_U-Prove.wmv

Non-technical reading:

- <http://www.idcorner.org>
- http://www.credentica.com/target_markets.html
- <http://www.credentica.com/faq.html>

U-Prove crypto:

- http://www.credentica.com/the_mit_pressbook.html



Additional U-Prove features

- Lending disincentive
- Limited-use tokens
- Recertification and updating of tokens
 - Issuer does not learn contents
- Verifier-driven revocation
- Tokens with identity escrow
- User-encoded (hidden) attributes
- Digital signatures with all U-Prove features