Microsoft Research

U-Prove

NIST Privacy Enhancing Cryptography Workshop - December 8-9, 2011

Christian Paquin (cpaquin@microsoft.com)

Senior Program Manager
Security & Cryptography, Extreme Computing Group
Microsoft Research

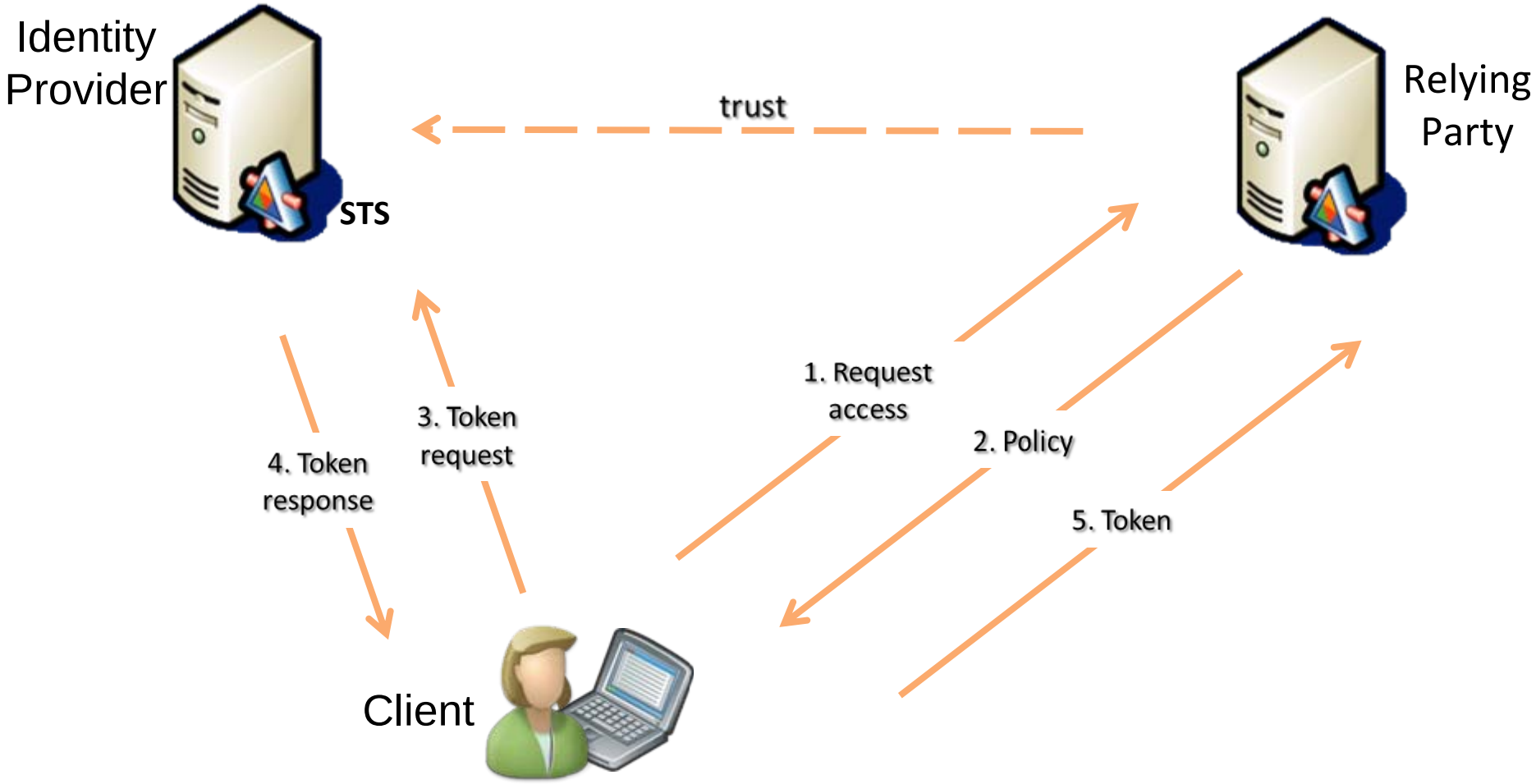
Identity landscape

- More and more services are migrated online
  - Improves convenience
  - Reduces costs
- High-value transactions require high-level of identity assurance
  - Usernames/passwords are ubiquitous, but provide low-security
  - Conventional “enterprise” solutions (e.g., Kerberos, PKI) don’t scale or are not flexible enough for an internet-wide system
  - How can you show some ID online, just like in real life?

Identity federation

- Most popular proposed architecture
  - Very flexible
  - Easy to deploy
- Many existing frameworks: WS-Federation/Trust, SAML, Information Cards, OpenID, OAuth, Facebook Connect, …
- But many challenges
  - Security
  - Privacy
  - Scalability

Federated architecture



Challenge #1: Security

- Compromise IdP credential, access all RPs
  - Phishing problem
- Strong authentication to IdP is possible, but authentication to RP is weaker
  - Issued tokens are software only (token hijacking attacks, transferability)
- IdP is all powerful
  - IdP (insider, malicious code) can surreptitiously act on the user's behalf
  - Selectively deny access

Challenge #2: Privacy

- IdP can profile user's activities

- Even if IdP doesn't learn the visited RP, profiling is possible by colluding parties (or insiders)
  - Timing correlation
  - Unique correlation handles (e.g., digital signatures, serial numbers, etc.)

Challenge #3: Scalability

- All tokens are retrieved on-demand
  - IdP must be available 24/7
- IdP is a central point of failure
  - Nice target for denial of service attack
- IdP is a bottleneck for every user access

User-centric approach

- Federated approach where the user is put at the ***center*** of the architecture, and in ***control*** of her information

- Minimal disclosure technologies complement such an approach to improve security, privacy, and scalability

What's U-Prove?

- Efficient privacy enhancing technology developed in the early 90s
  - Think "PKI with privacy-by-design"
  - Provides unlinkability between issuance and presentation
  - Provides minimal disclosure of attributes, e.g.,
    - Disclose a subset of the attributes
    - Prove that name is not on blacklist
    - Prove that age is greater than 18
- To create the equivalent of real-life credentials

lustrated

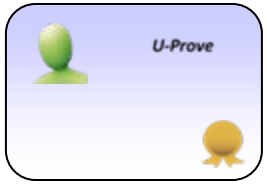
U-Prove

Name: Alice Smith

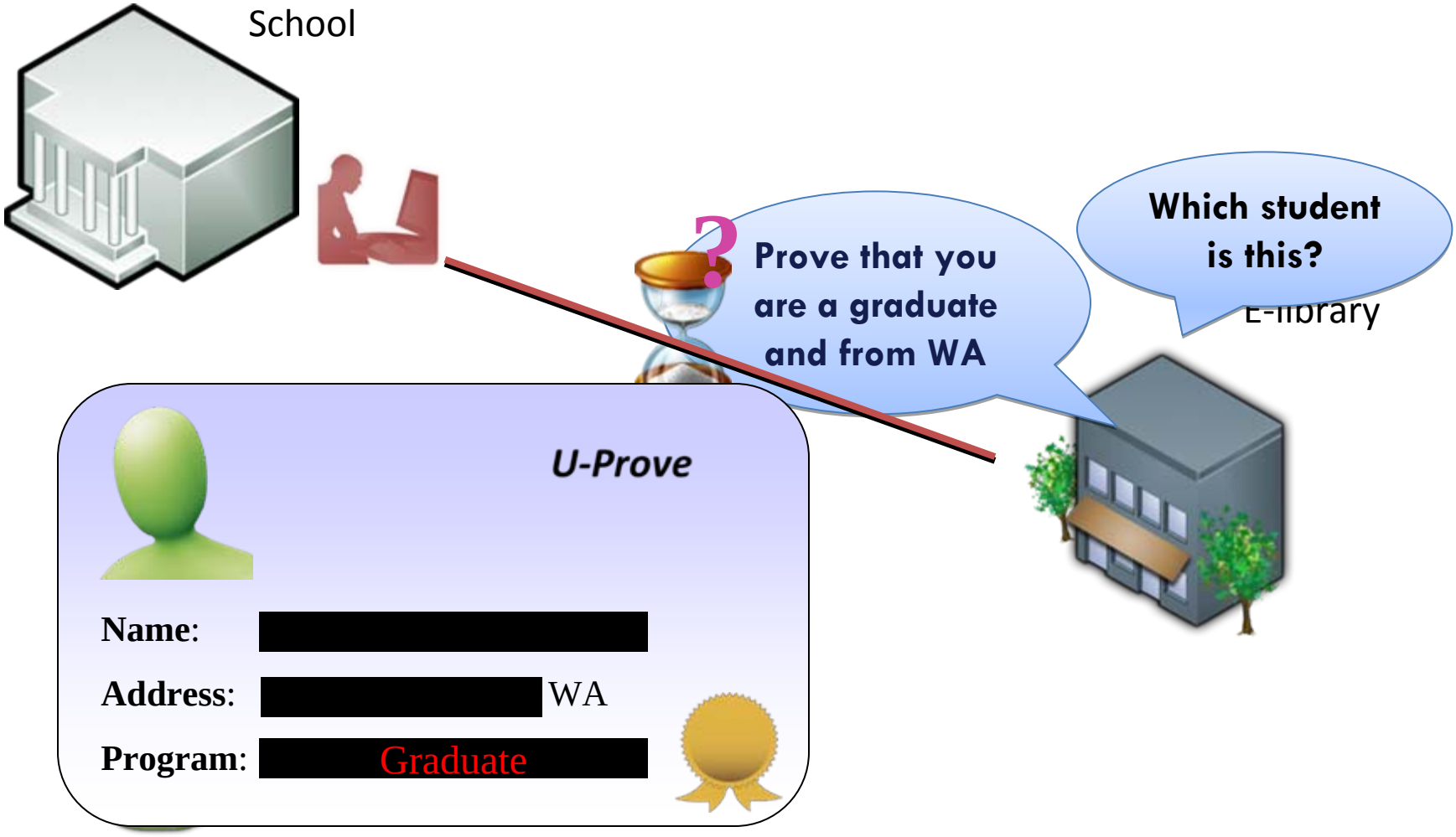
Address: 1234 Pine, Seattle, WA

Program: Computer Science, M. Sc.

E-library



Minimal disclosure illustrated



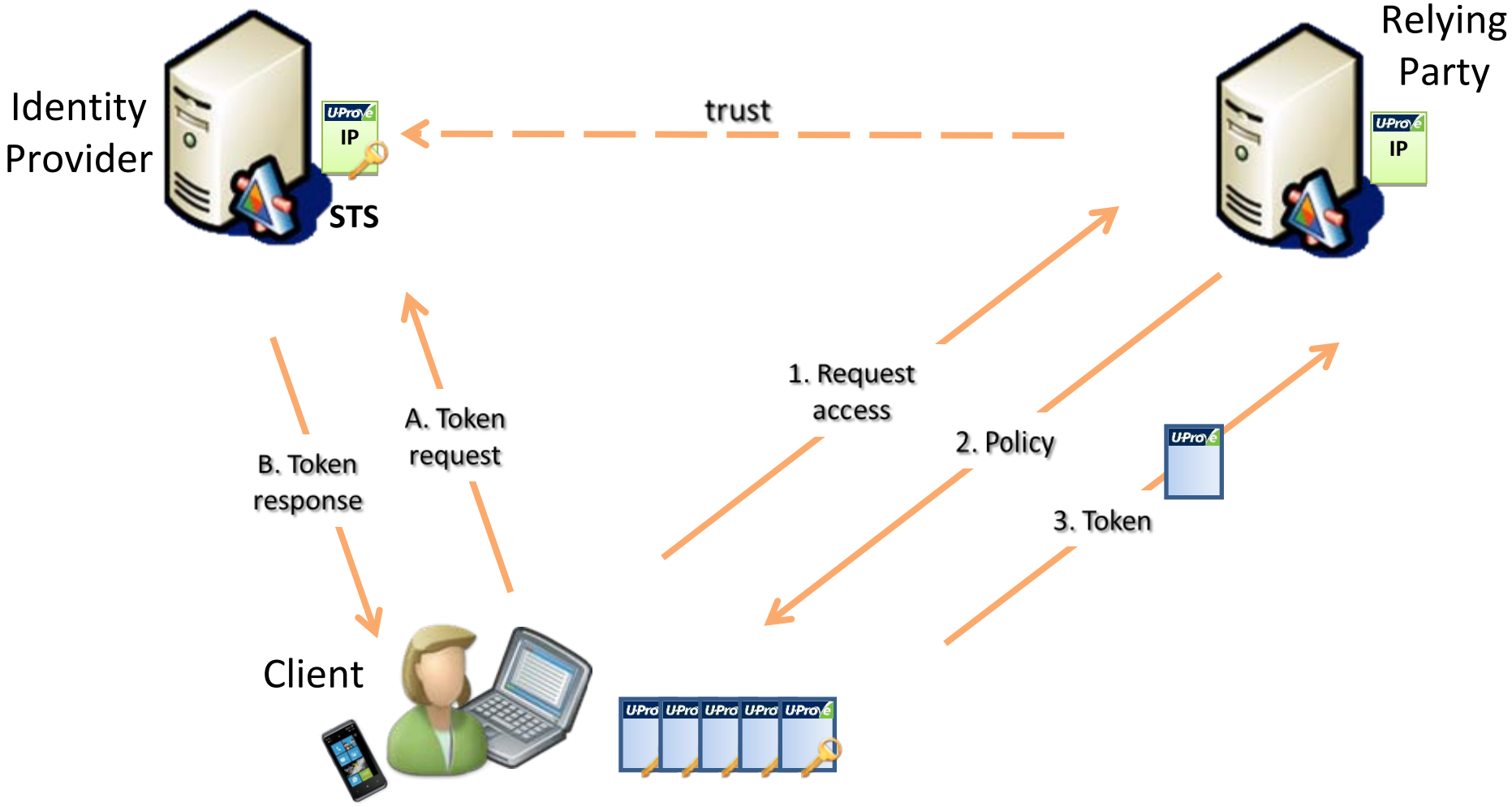
Microsoft's past efforts

- Microsoft Passport
  - "Classic" federation system, first designed to authenticate to Microsoft web properties, but extended to become web SSO system
  - Privacy concerns, which lead to the design of…
- Identity Metasystem and Information Cards
  - CardSpace was Microsoft's implementation
  - Great user control, but still needed to address some privacy concerns

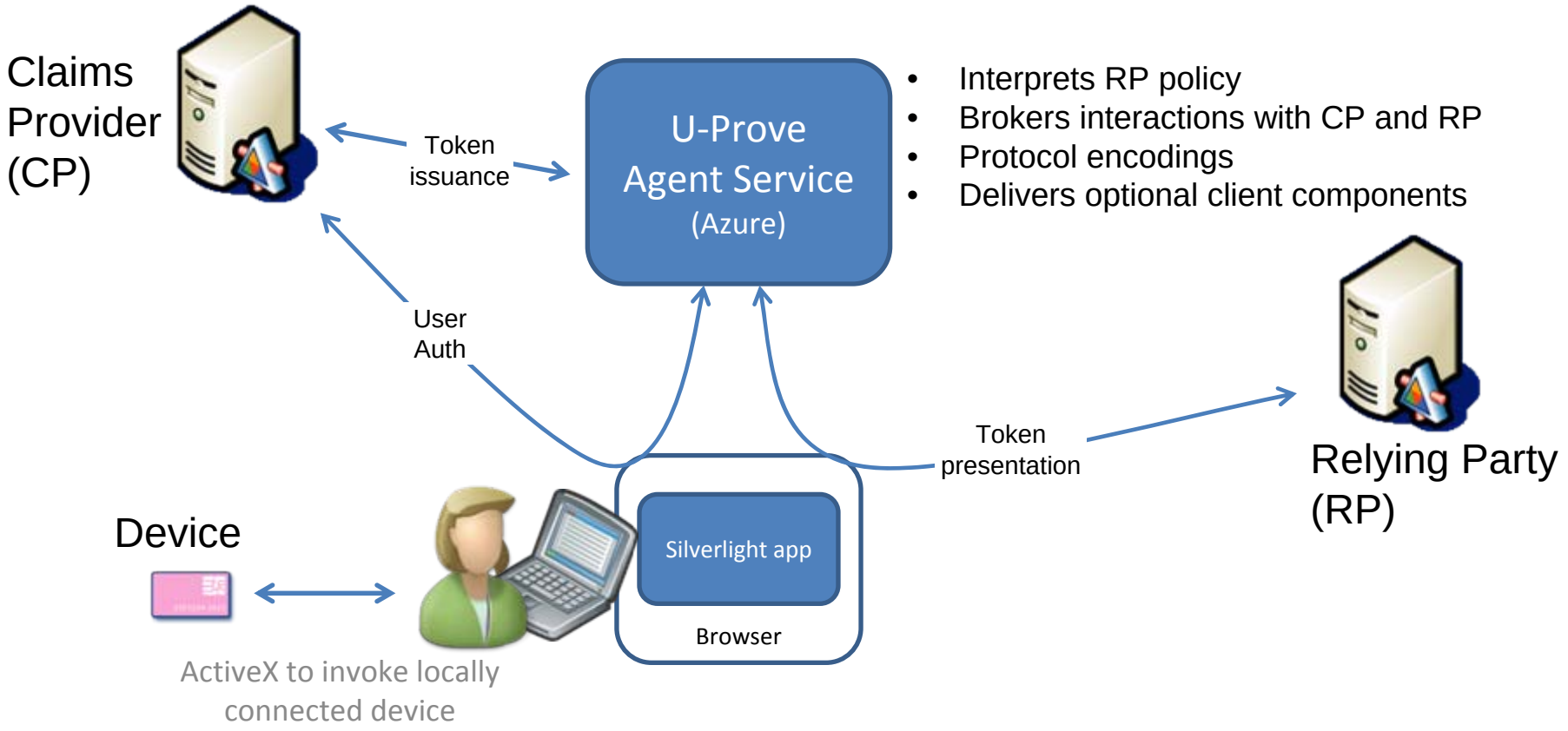
U-Prove releases

- U-Prove Community Technology Previews (CTP)
  - 1st CTP demonstrated integration with CardSpace (March 2010)
  - 2nd CTP demonstrated a cloud user agent service (February 2011)
  - Specifications released under the Open Specification Promise
  - Crypto libraries available under an open-source license
  - http://www.microsoft.com/u-prove

Federation + U-Prove



U-Prove agent architecture (CTP2)

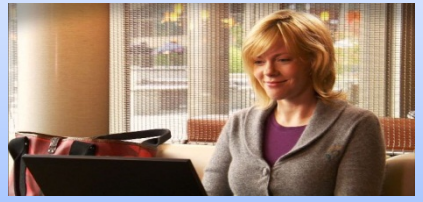


U-Prove demos/PoCs

Erika Trilogy

University feedback + e-library access

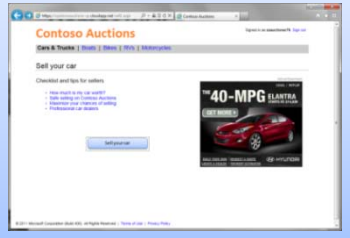
eParticipation



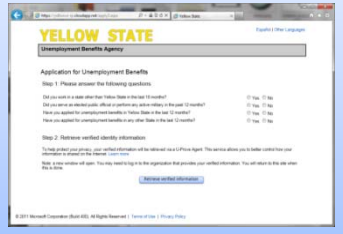
HealthVault registration

U-Prove Agent demos

Car auction



Unemployment benefits



MediaRoom

*A*ttribute-*B*ased *C*redentials *4* (for) *Trust*

- 4-year, EC-funded FP7 project, kicked-off in November 2010
- Goal: survey, compare, abstract, implement, and pilot various minimal disclosure technologies
  - Focuses on U-Prove and Idemix
  - Supports many features: revocation, inspection, complex proofs
  - School social network and polling pilots
- Consortium partners
- https://abc4trust.eu/

*L*ightweight privac*Y*-enhancing c*R*yptography for mob*I*le *C*ontactless *S*ervices

- 3-year, French-funded (ANR) project, to start early 2012
- Goal: architect and implement an efficient minimal disclosure system for NFC-enabled mobile phones and contactless services
- Consortium partners

Work in progress

- Privacy-preserving business models for identity providers
  - Subscription vs. per-transaction models
  - Attributes paid for by user, relying parties, or devices
- Technical work
  - New features (e.g, predicates, revocation, inspection, etc.)
  - New schemes (e.g, delegatable credentials)
- New deployment models
  - Mobile, cloud-based
- Outreach and education

Questions?

cpaquin@microsoft.com