U-Prove Technology Overview

November 2010

TOC

- Introduction
- Community Technology Preview
- Additional Capabilities
- RSA Demo
- Conclusion

Introduction

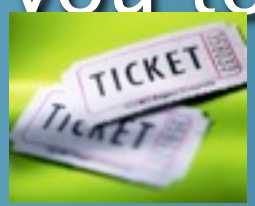
History

- U-Prove well established in academia
  - Patent portfolio (granted ‘93 – ’00)
  - 30+ scientific papers (from ‘93 onward)
  - E-cash PoC and pilots with Siemens, Gemplus, KPN, DigiCash, Zero-Knowledge, Nokia
- Credentica acquisition (Feb 2008)
  - Patents, software, people
- Microsoft incubation
  - Incubated U-Prove-enabled ID platform
  - Public CTP (March ‘10)

U-Prove Technology

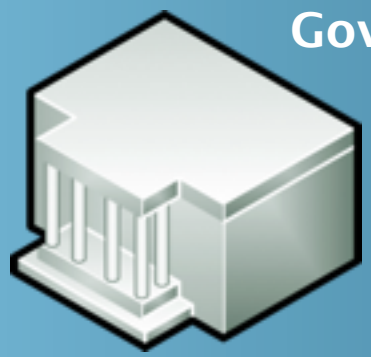
- Strong multi-party security technology for user-centric identity, data sharing, strong authentication, and digital signature

- Allows you to build "e-tokens"



- Has unique security, privacy, and efficiency benefits over "conventional"

Minimal disclosure



Minimal disclosure

Name: Alice Smith

Address: 1234 Pine, Seattle, WA

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

Minimal disclosure

U-Prove

Name: Alice Smith

Address: 1234 Pine, Seattle, WA

D.O.B: 23-11-1955

Coho Winery

Minimal disclosure

Gov

Coho Winery

Minimal disclosure

Gov

The user can prove unanticipated properties about the encoded claims in a U-Prove token issued to her in advance

Even in collusion, the issuing and relying parties cannot learn more about the user than what was disclosed

Coho Winery

Minimal disclosure

Gov

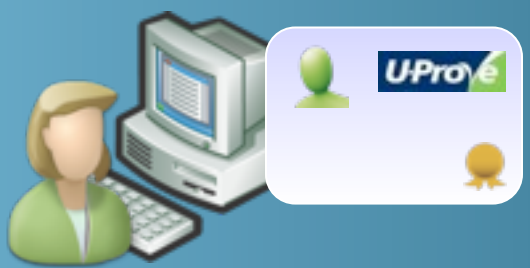
Coho Winery

Minimal disclosure

Gov

Coho Winery

Minimal disclosure



Minimal disclosure

Gov

Prove that you are over 21 and from WA

Coho Winery

U-Prove

Name: Alice Smith

Address: 1234 Pine, Seattle, WA

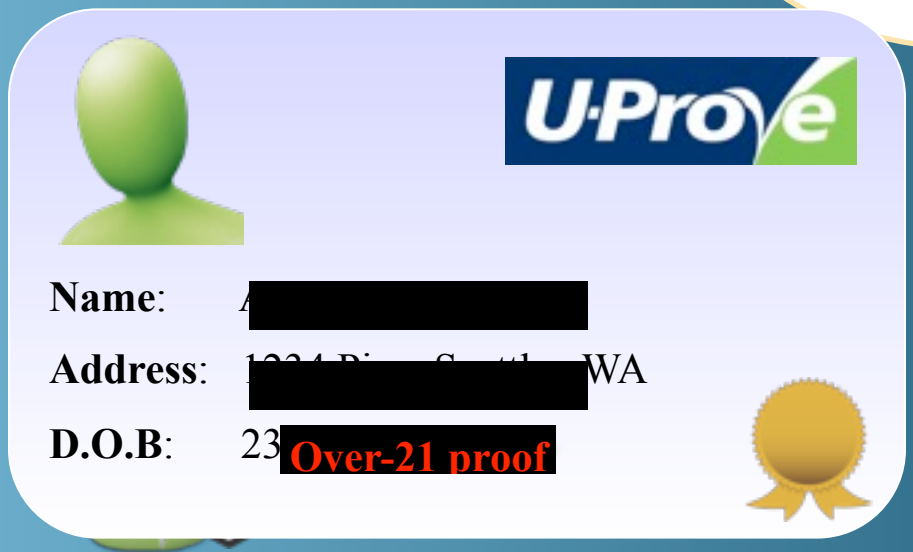
D.O.B: 23-11-1955

Minimal disclosure

Gov

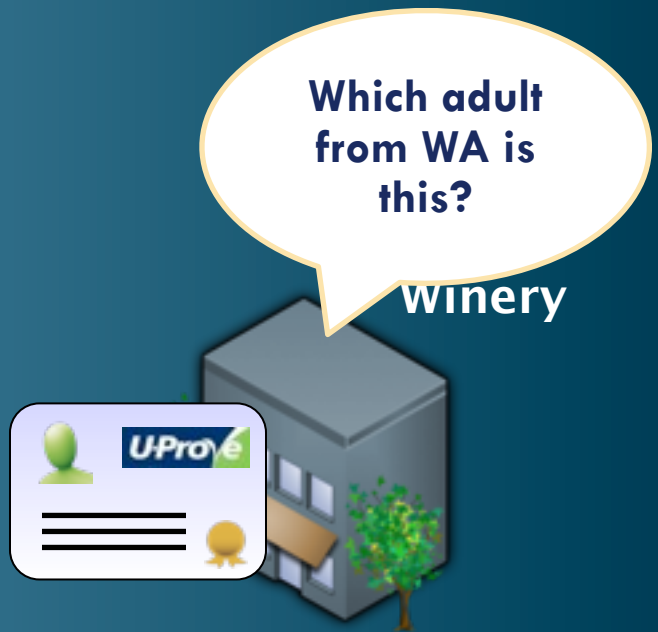
Prove that you are over 21 and from WA

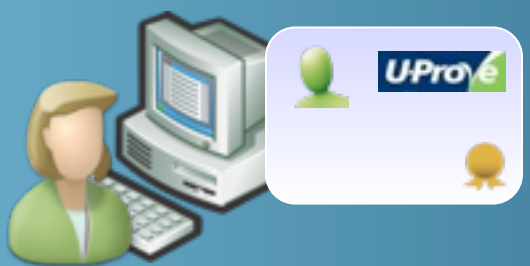
Coho Winery



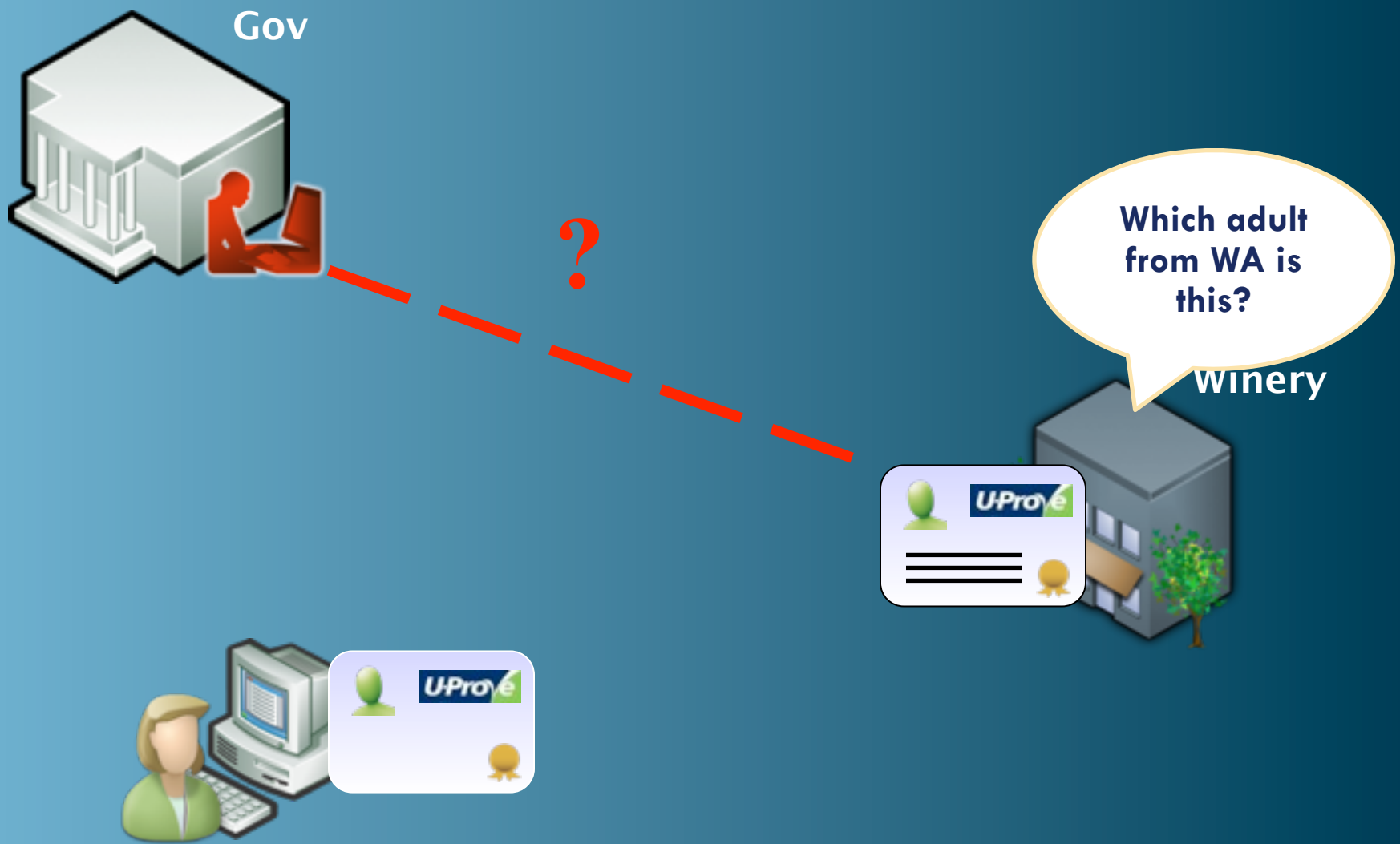
Minimal disclosure

Minimal disclosure





Minimal disclosure



Minimal disclosure

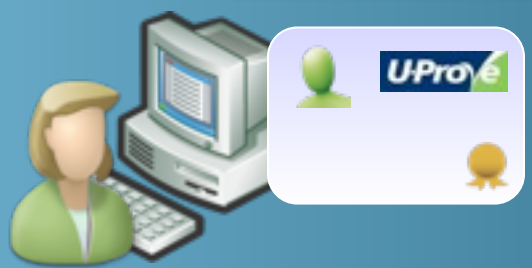
Gov

The user can prove unanticipated properties about the encoded claims in a U-Prove token issued to her in advance

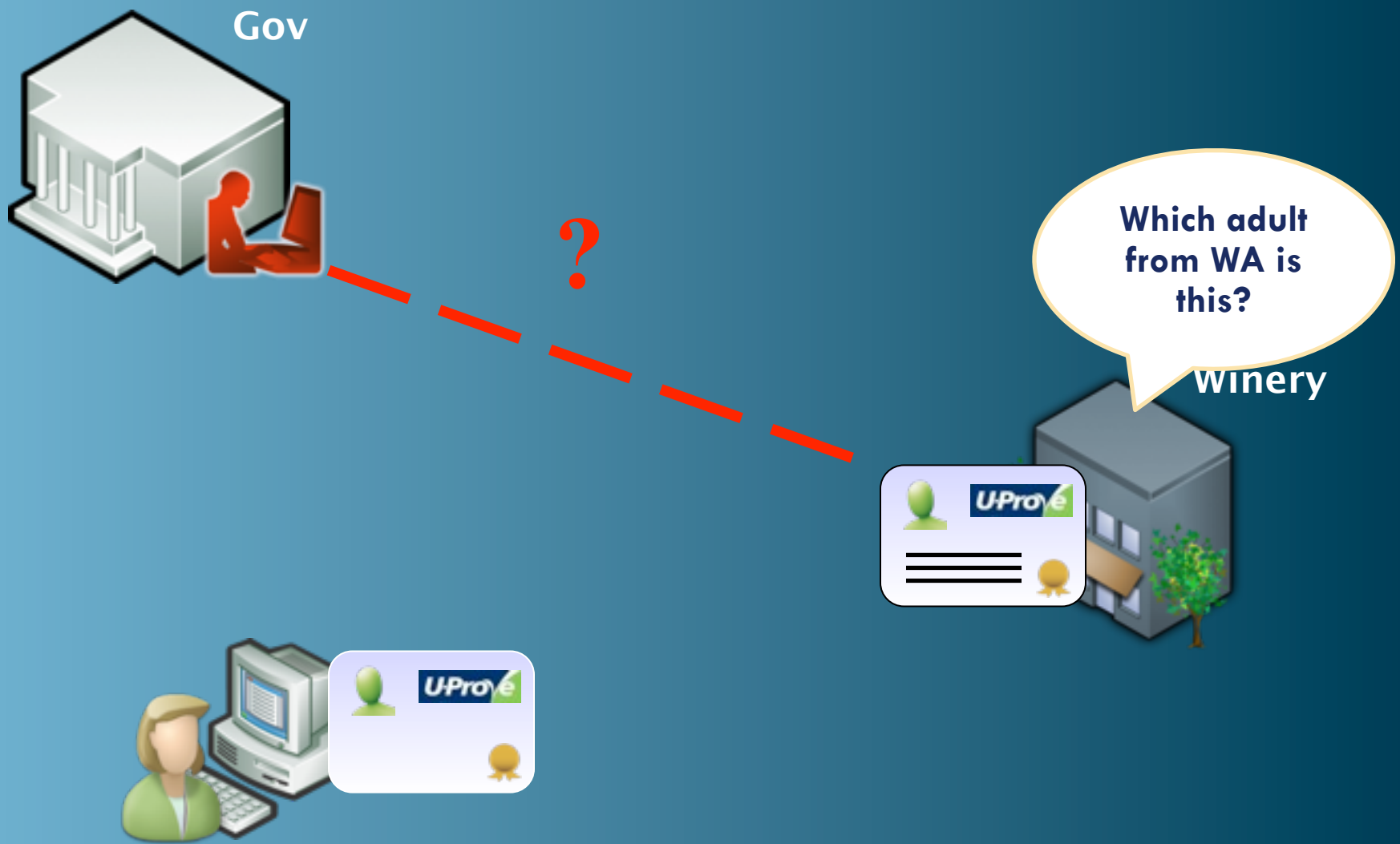
Even in collusion, the issuing and relying parties cannot learn more about the user than what was disclosed

Which adult from WA is this?

Winery



Minimal disclosure



What's new?

- Similar to conventional security tokens (X.509, SAML, Kerberos), but
  - U-Prove tokens contain no inescapable correlation handles
    - E.g., coins (unlinkable) vs. bills (w/ serial#)
  - Users can prove properties of the claims
    - Disclose a subset of the claims
    - Derived claim: "birth date" to "over-21 proof"
    - Negation: name not on the control list

U-Prove CTP

Released March 2010

U-Prove CTP

- Specifications (released under Open Specification Promise)
  - U-Prove crypto specification (addressing feature subset)
  - Integration into the ID metasystem specification
- Open-source crypto SDKs (implementing crypto spec)
  - Posted on Code Gallery, under the BSD license
  - C# and Java versions
- Identity platform integration (implementing integration spec)
  - Modified version of Windows CardSpace 2.0
  - Extension to the Windows Identity Foundation
  - Modified version of Active Directory Federation Services 2.0

http://www.microsoft.com/u-prove

Federation + U-Prove

Identity Provider

STS

Relying Party

Client

Federation + U-Prove

Identity Provider

Relying Party

Client

Federation + U-Prove

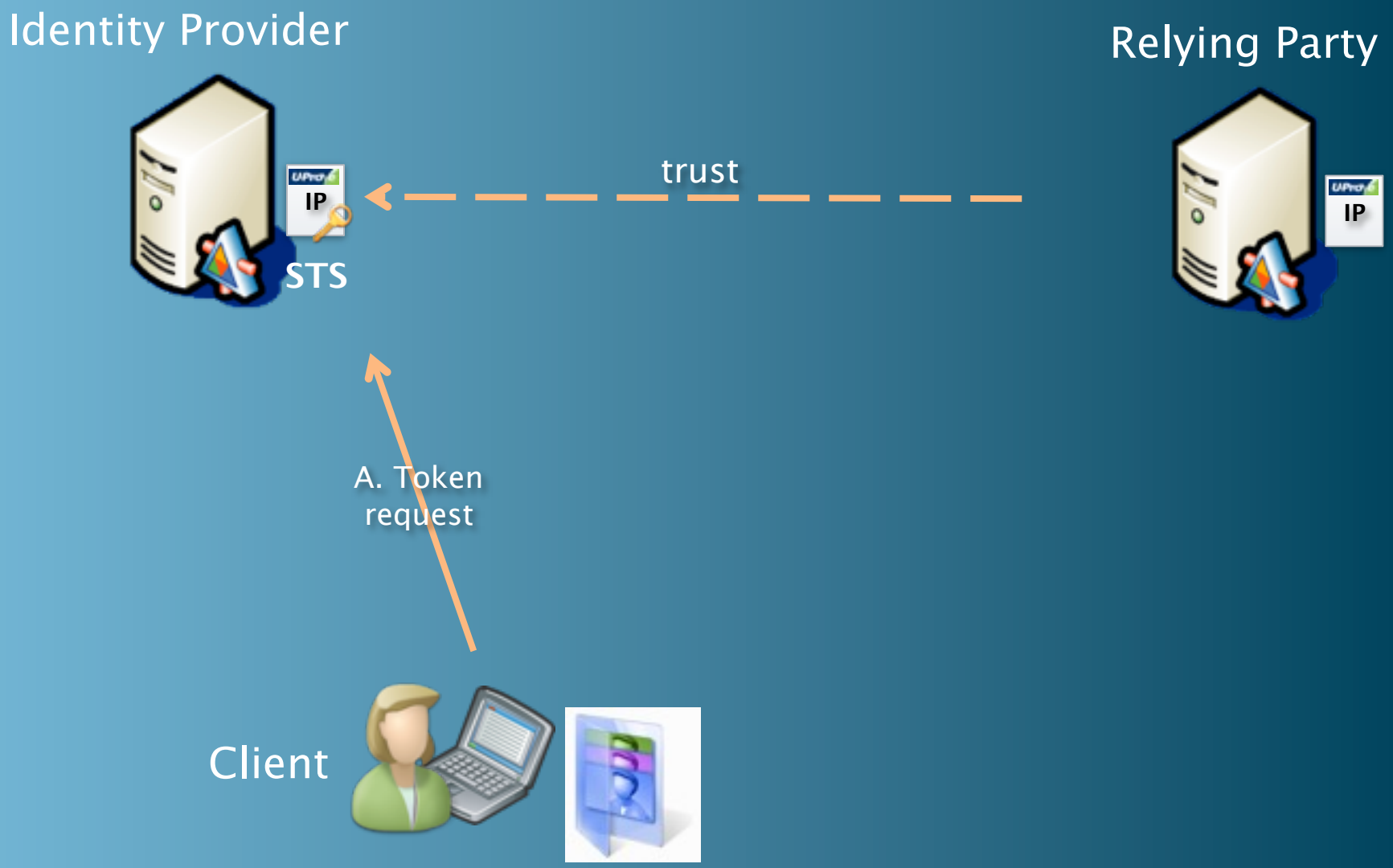
Identity Provider

trust

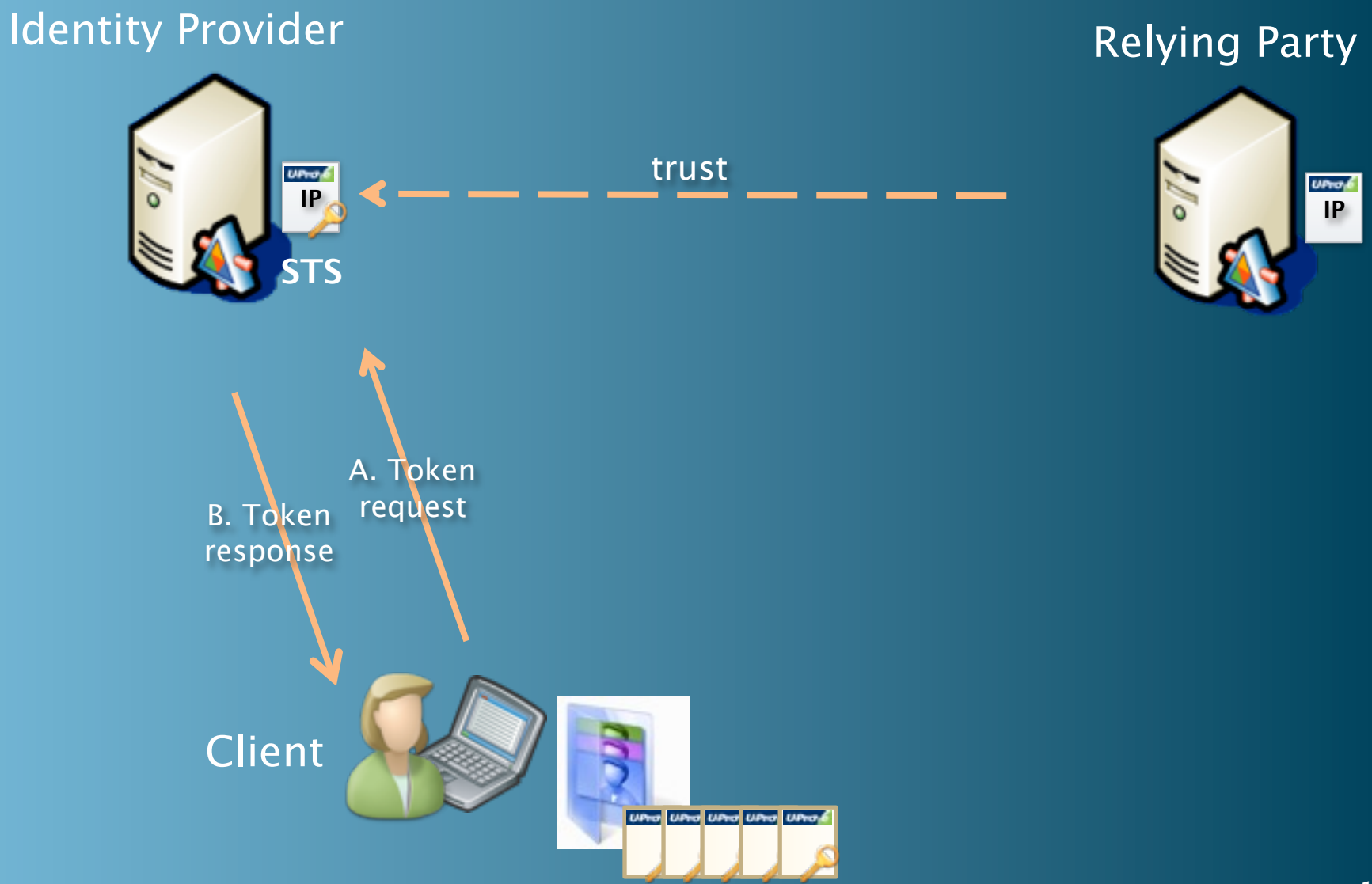
Relying Party

Client

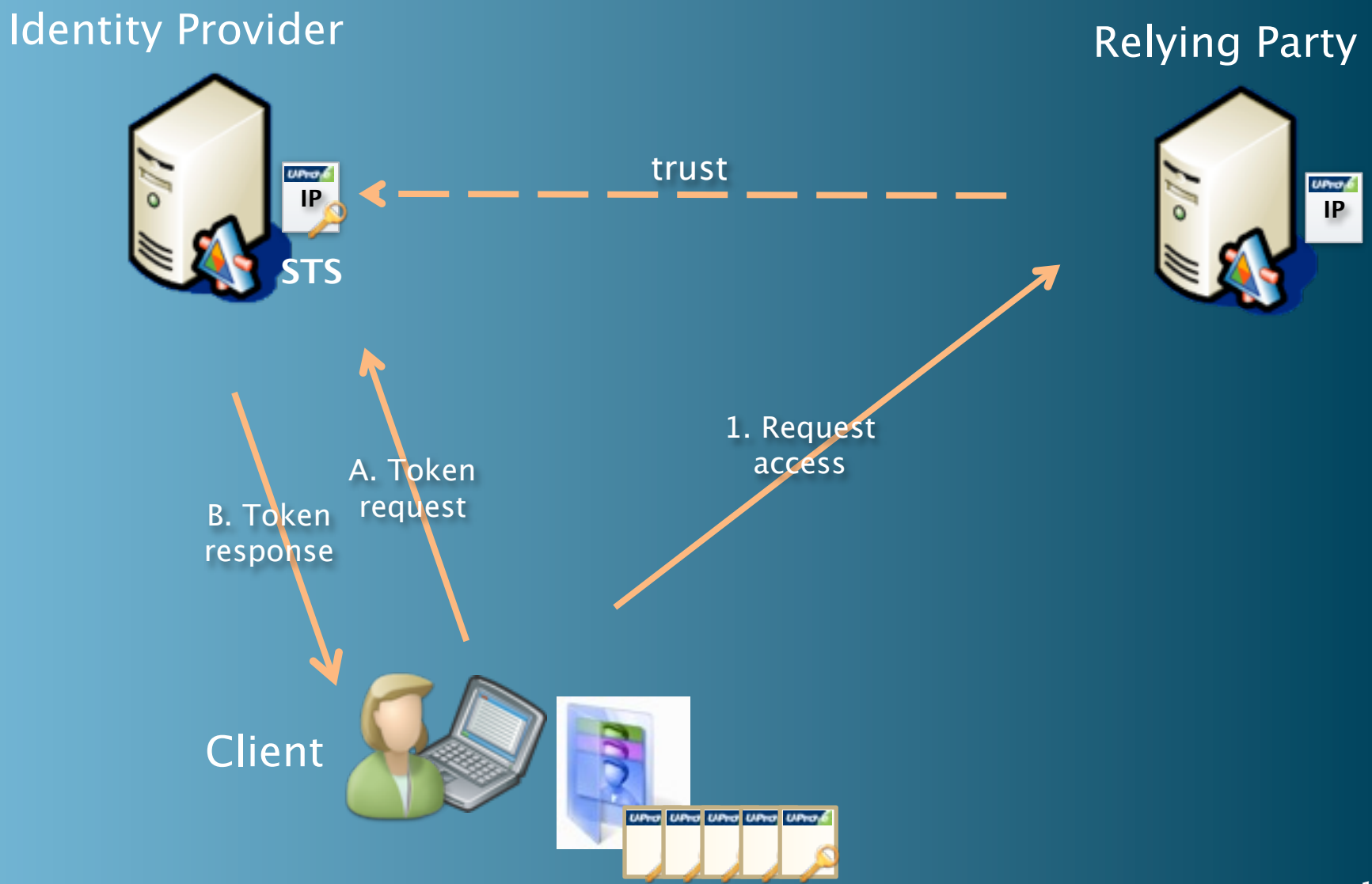
Federation + U-Prove



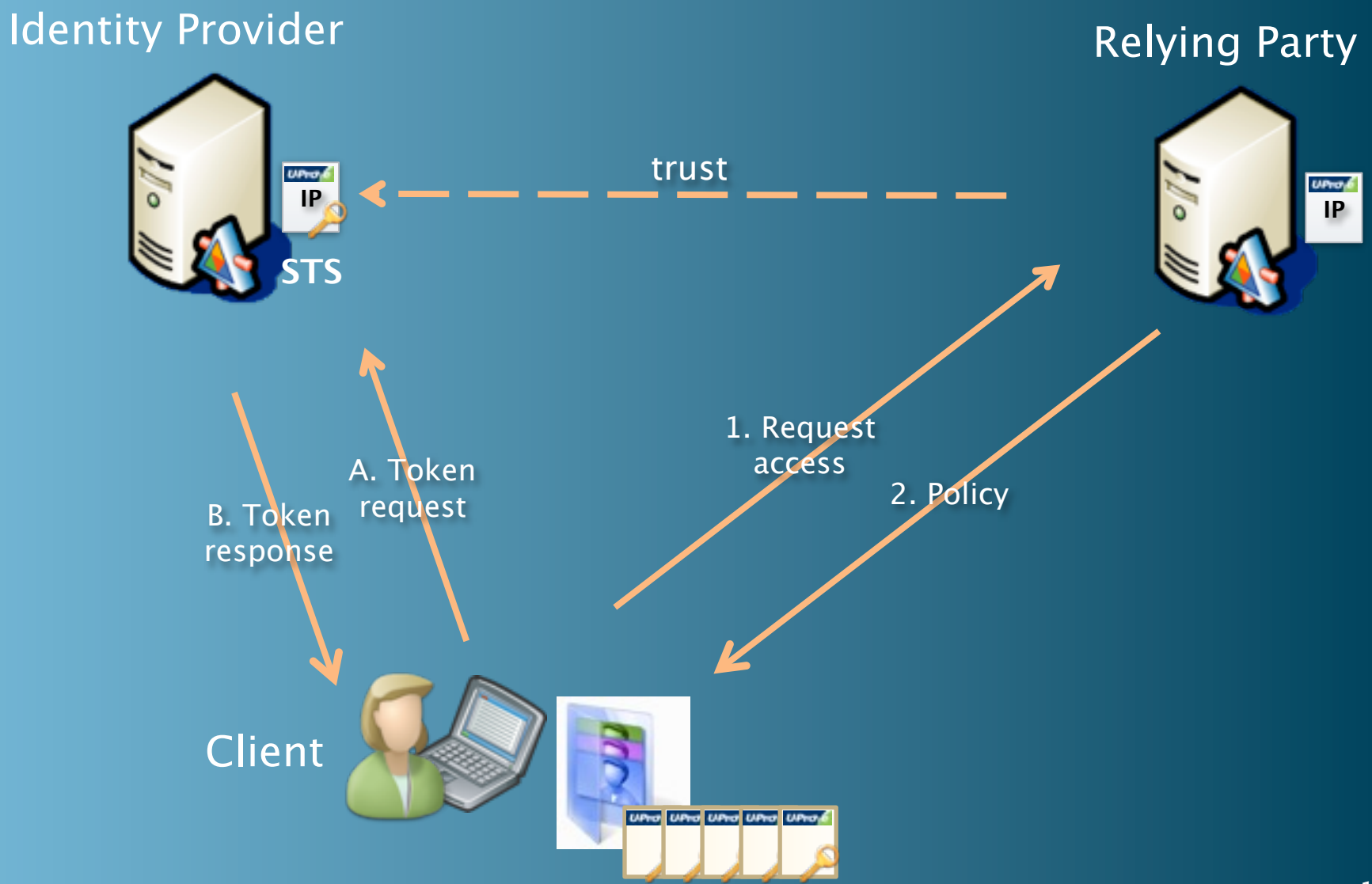
Federation + U-Prove



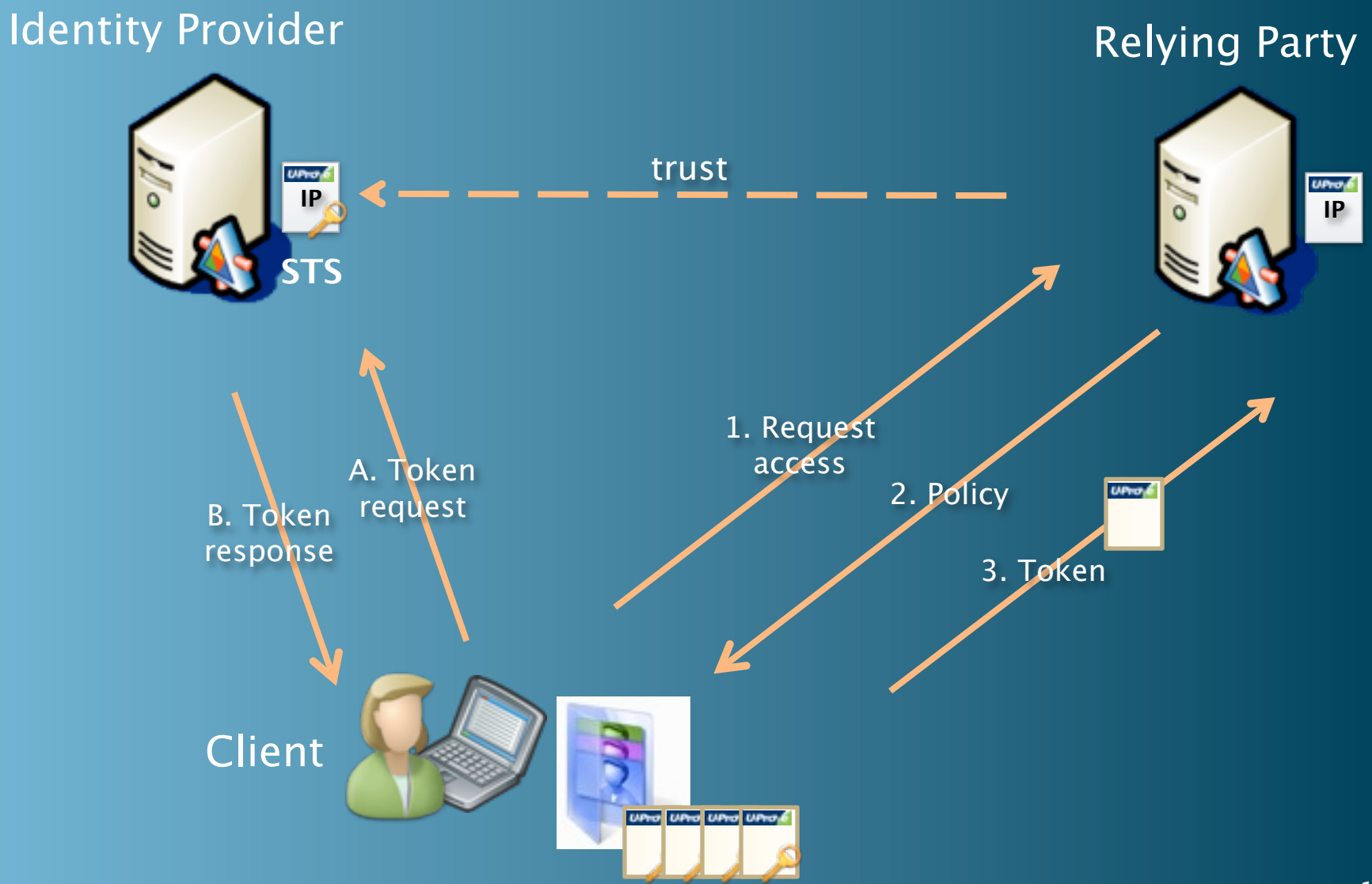
Federation + U-Prove



Federation + U-Prove



Federation + U-Prove



CTP features

- The CTP implements the foundational U-Prove features:
  - Selective disclosure (i.e., no derived claims)
  - Unlinkability of token issuance and presentation
  - Long-lived token support
  - User-signed presentation tokens
  - Data signature (in crypto SDKs only)

U-Prove technology additional capabilities

U-Prove technology addit

The following slides provide a U-Prove technology overview

(If you miss a step in the animation, press the left arrow to rewind)

U-Prove technology additional capabilities

Censorable audit logs

Censorable audit logs

Gov

Adatum Auditor

Coho Winery

Censorable audit logs

Gov

Adatum Auditor

Coho Winery

Provide name and address and get $20

Censorable audit logs

Gov

Adatum Auditor

Coho Winery

U-Prove

Name: Alice Smith

Address: 1234 Pine, Seattle, WA

D.O.B: 23-11-1955

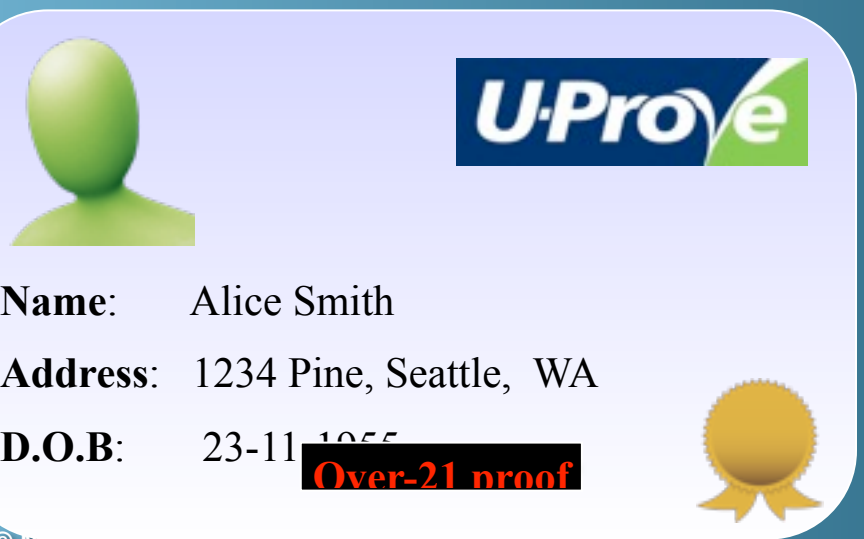
Provide name and address and get $20

Censorable audit logs

Gov

Adatum Auditor

Coho Winery



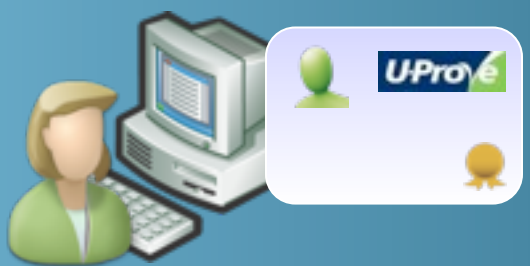
Provide name and address and get $20

Censorable audit logs

Gov

Adatum Auditor

Coho Winery



Censorable audit logs

Gov

Adatum Auditor

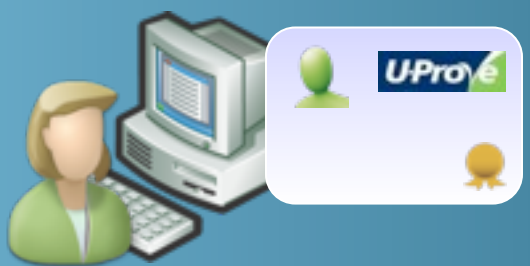
Name: Alice Smith

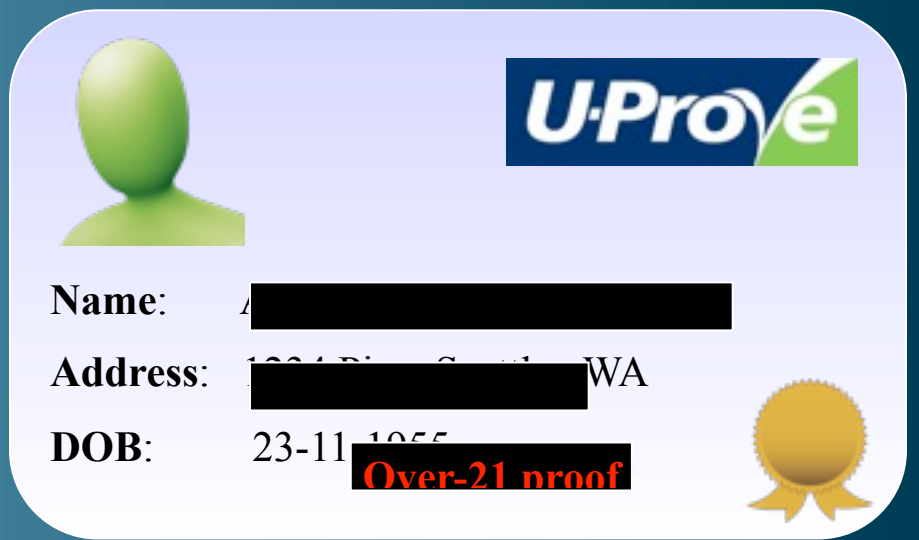
Address: 1234 Pine, Seattle, WA

DOB: 23-11-1955

Over-21 proof

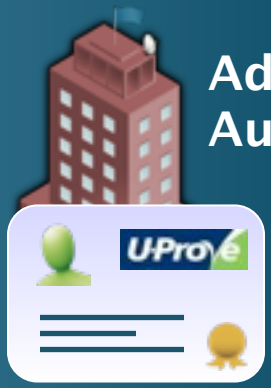
Censorable audit logs





Censorable audit logs

Gov



Adatum Auditor

Coho Winery

My customer was an adult from WA

Censorable audit logs

Gov

Adatum Auditor

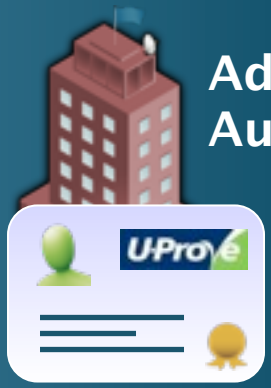
Relying parties can remove disclosed information from presentation transcripts (without invalidating the issuer's and the user's signatures), keeping only what is necessary for audit compliance

Coho Winery

My customer was an adult from WA

Censorable audit logs

Gov



Adatum Auditor

Coho Winery

My customer was an adult from WA

Broker-mediated disclosure

Broker-mediated disclosure

U-Prove

Name: Alice Smith

Address: 1234 Pine, Seattle, WA

Disorder: Anxiety

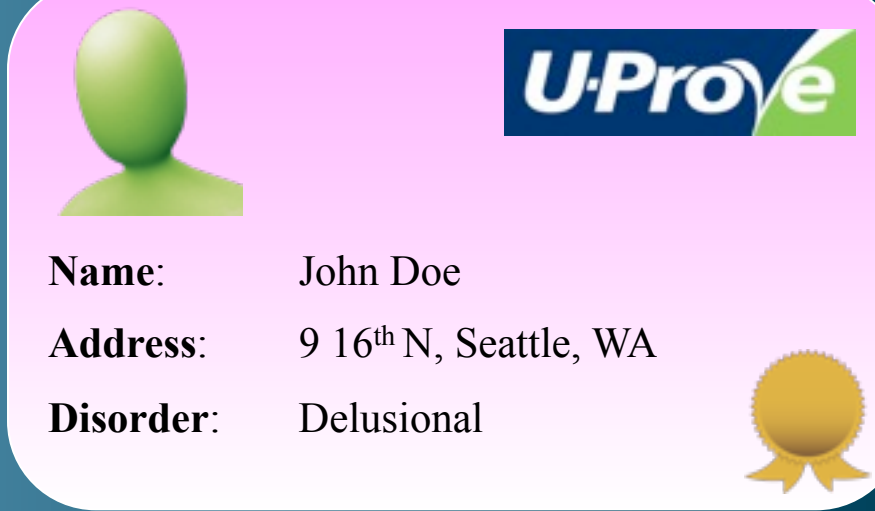
Hospital

Contoso Research

Broker

Broker-mediated disclosure

Broker-mediated disclosure



Broker-mediated disclosure

Broker-mediated disclosure

A broker can disclose anonymous data it collected to 3rd parties, while preserving the authenticity of the issuer's signature on the data

Broker-mediated disclosure

Broker-mediated disclosure

Hospital

Hospital

Contoso Research

Broker

Broker-mediated disclosure

Clients from Seattle with mental disorder?

Broker-mediated disclosure

Clients from Seattle with mental disorder?

Name: Alice smith

Address: 1234 Pine, Seattle, WA

Disorder: Anxiety

Broker-mediated disclosure

U-Pro

Clients from Seattle with mental disorder?

Name: John Doe

Address: 9 16th N, Seattle, WA

Disorder: Delusional

Name: Alice smith

Address: 1234 Pine, Seattle, WA

Disorder: Anxiety

Broker-mediated disclosure

U-Pro

Clients from Seattle with mental disorder?

Name: John Doe

Address: 9 16th N, Seattle, WA

Disorder: Delusional

Name: Alice smith

Address: 1234 Pine, Seattle, WA

Disorder: Anxiety

Names are different

Both from Seattle

Both are mental disorders

Broker-mediated disclosure

U-Pro

Clients from Seattle with mental disorder?

Name: [redacted]

Address: [redacted]

Disorder: [redacted]

Name: [redacted]

Address: [redacted]

Disorder: [redacted]

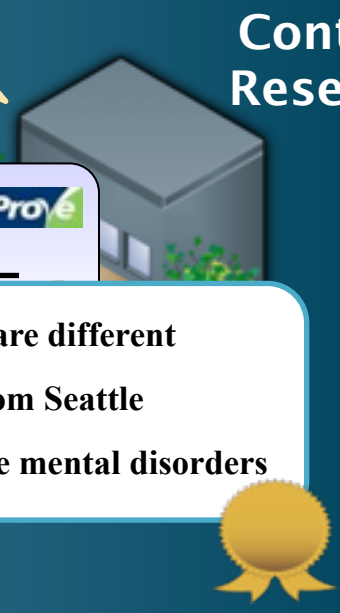
Names are different

Both from Seattle

Both are mental disorders

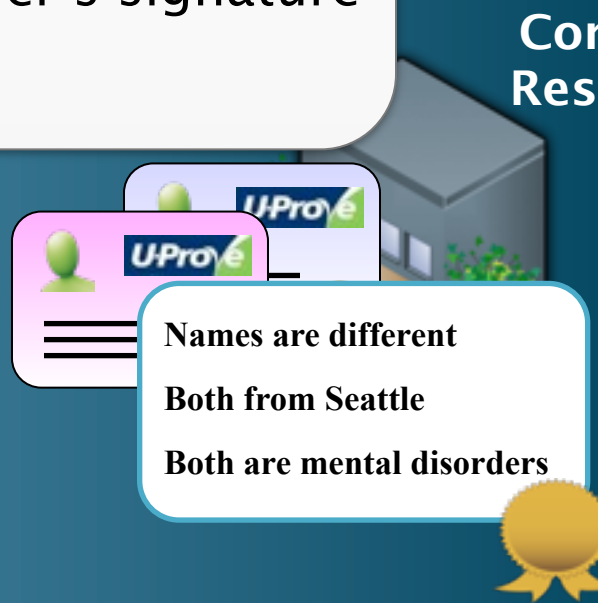
Broker-mediated disclosure

Clients from Seattle with mental disorder?



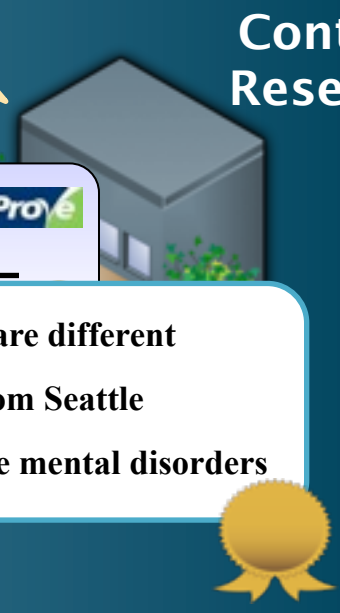
Broker-mediated disclosure

A broker can disclose anonymous data it collected to 3rd parties, while preserving the authenticity of the issuer's signature on the data



Broker-mediated disclosure

Clients from Seattle with mental disorder?



Revocation

Adatum
Auditor

Woodgrove Bank

asmith@adatum.com

Revocation

Name: Alice Smith
Email: asmith@adatum.com
Role: Auditor

Adatum
Auditor

Woodgrove Bank

asmith@adatum.com

Revocation

Adatum
Auditor

Alice Smith
asmith@adatum.com
Auditor

REVOKED

Woodgrove Bank

asmith@adatum.com

Revocation

Adatum Auditor

Alice Smith
asmith@adatum.com
Auditor

REVOKED

Prove that you are a valid auditor

Woodgrove Bank

asmith@adatum.com

Revocation

Adatum Auditor

Alice Smith
asmith@adatum.com
Auditor

REVOKED

Prove that you are a valid auditor

Woodgrove Bank

U-Prove

Name: Alice Smith

Email: asmith@adatum.com

Role: Auditor

asmith@adatum.com

Revocation

Adatum Auditor

Alice Smith
asmith@adatum.com
Auditor

REVOKED

U-Prove

Name: Ali not revoked proof

Email: [redacted]

Role: Auditor

asmith@adatum.com

Prove that you are a valid auditor

Woodgrove Bank

Revocation

Adatum Auditor

Name: Alice Smith
Email: asmith@adatum.com
Role: Auditor

REVOKED

Prove that you are a valid auditor

Woodgrove Bank

asmith@adatum.com

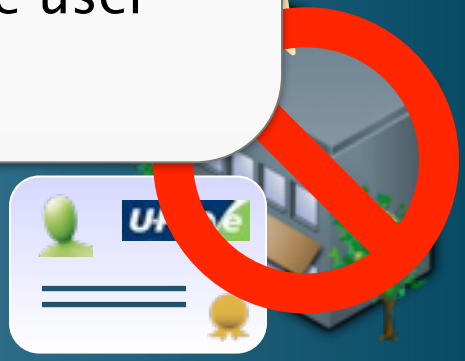
Revocation

Adatum Auditor

Alice Smith
asmith@adatum.com

REVOKED

Issued U-Prove tokens can be revoked by the issuer, even if no connection to the issuer is made when the user presents the tokens



Woodgrove Bank

asmith@adatum.com

Revocation

Adatum Auditor

Name: Alice Smith
Email: asmith@adatum.com
Role: Auditor

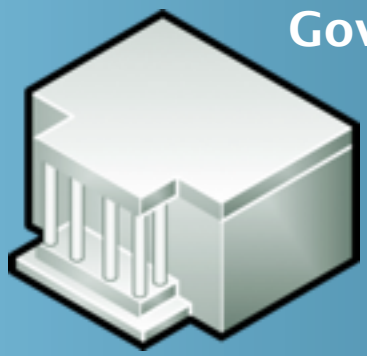
REVOKED

Prove that you are a valid auditor

Woodgrove Bank

asmith@adatum.com

Trusted device



Gov

University

Bookstore

Trusted device

Gov

University

Bookstore

Trusted device

Gov

sity

Bookstore

Trusted device

Gov

University

Bookstore

Trusted device

Gov

University

Bookstore

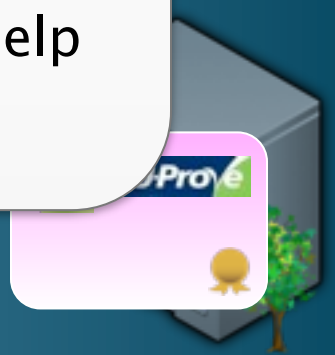
Trusted device

Gov

University

A trusted device (smartcard, TPM chip, remote service) can hold part of the tokens' private key (even those issued by other issuers) and efficiently help presenting them

Bookstore



Trusted device

Gov

University

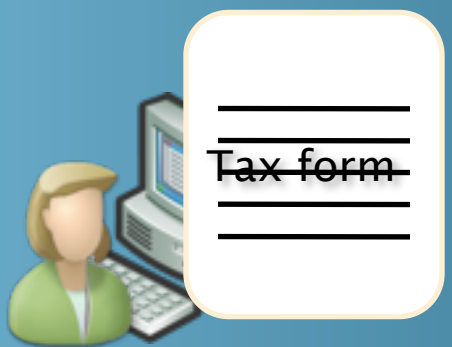
Bookstore

Data signing

Data signing

Gov

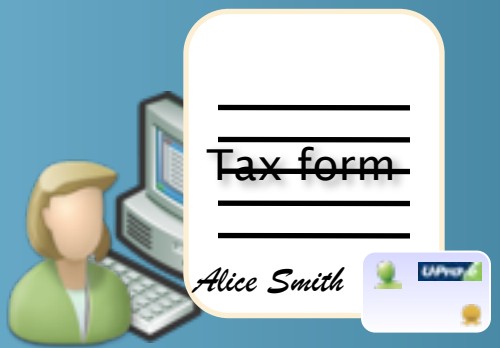
Revenue Agency



Data signing

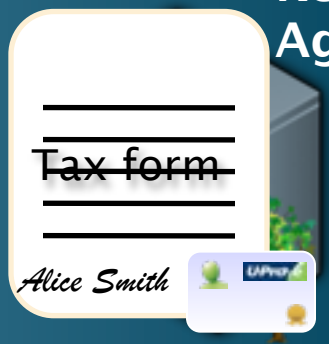
Gov

Revenue Agency



Data signing

Gov

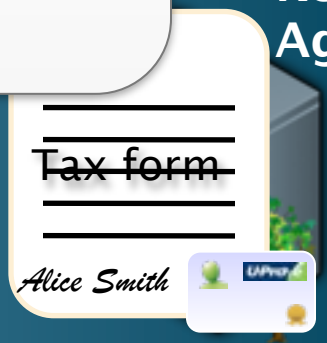


Revenue Agency

Data signing

Gov

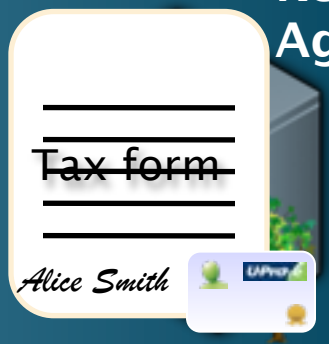
The user can non-interactively sign arbitrary data using a U-Prove token, attaching any encoded claim property to the signature



Revenue Agency

Data signing

Gov

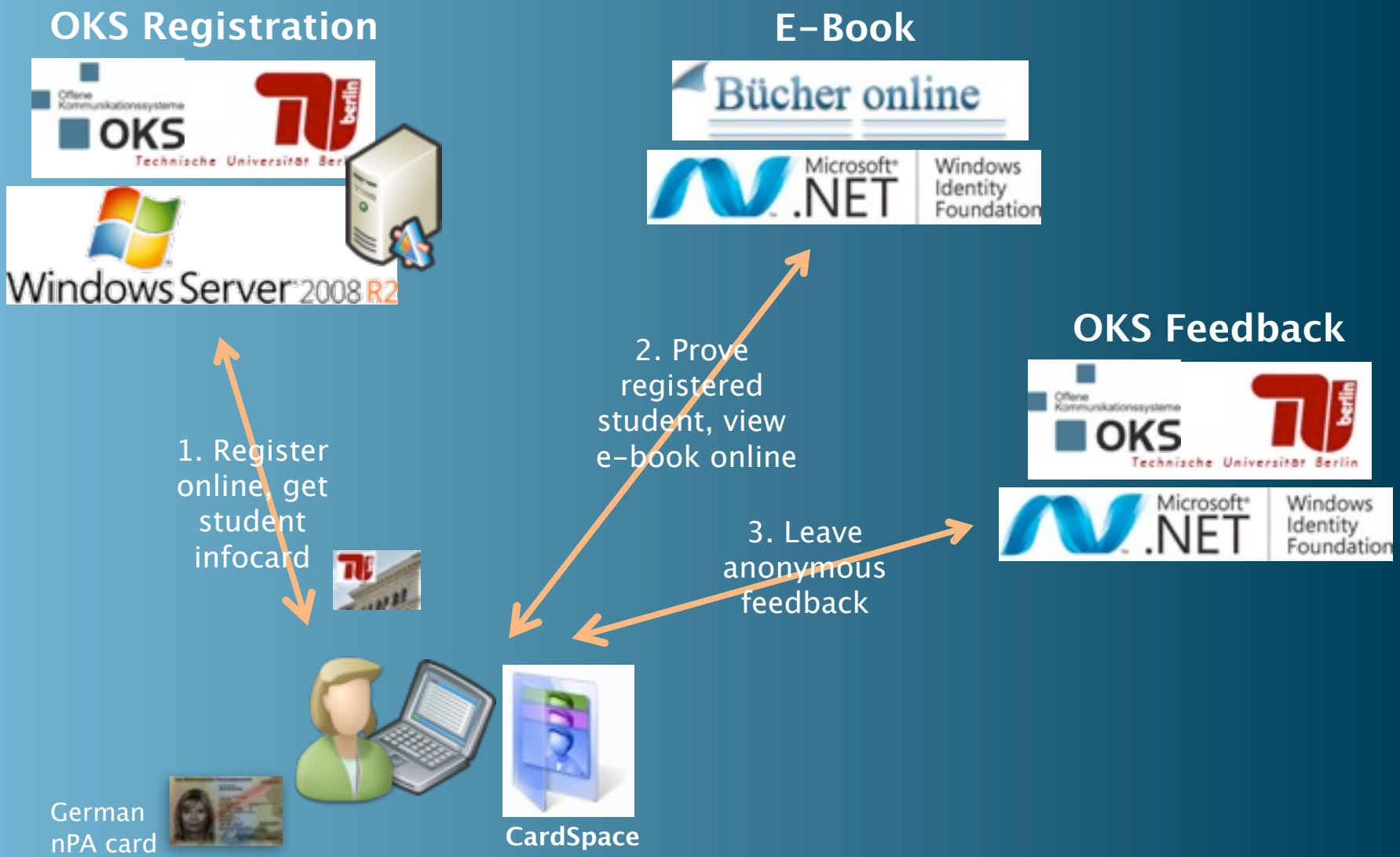


Revenue Agency

RSA 2010 Demo

- http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

RSA 2010 demo



RSA 2010 demo details

- User presents German nPA card to prove identity to university when registering online
- University issues a student (U-Prove) information card supporting claims from the nPA card and registration data
- Student visits online book store, proves that she is a registered computer science student, and can view a book for free
- Student visits a university feedback portal, discloses her registered classes (and optionally her gender), and submits

Conclusion

Summary of benefits

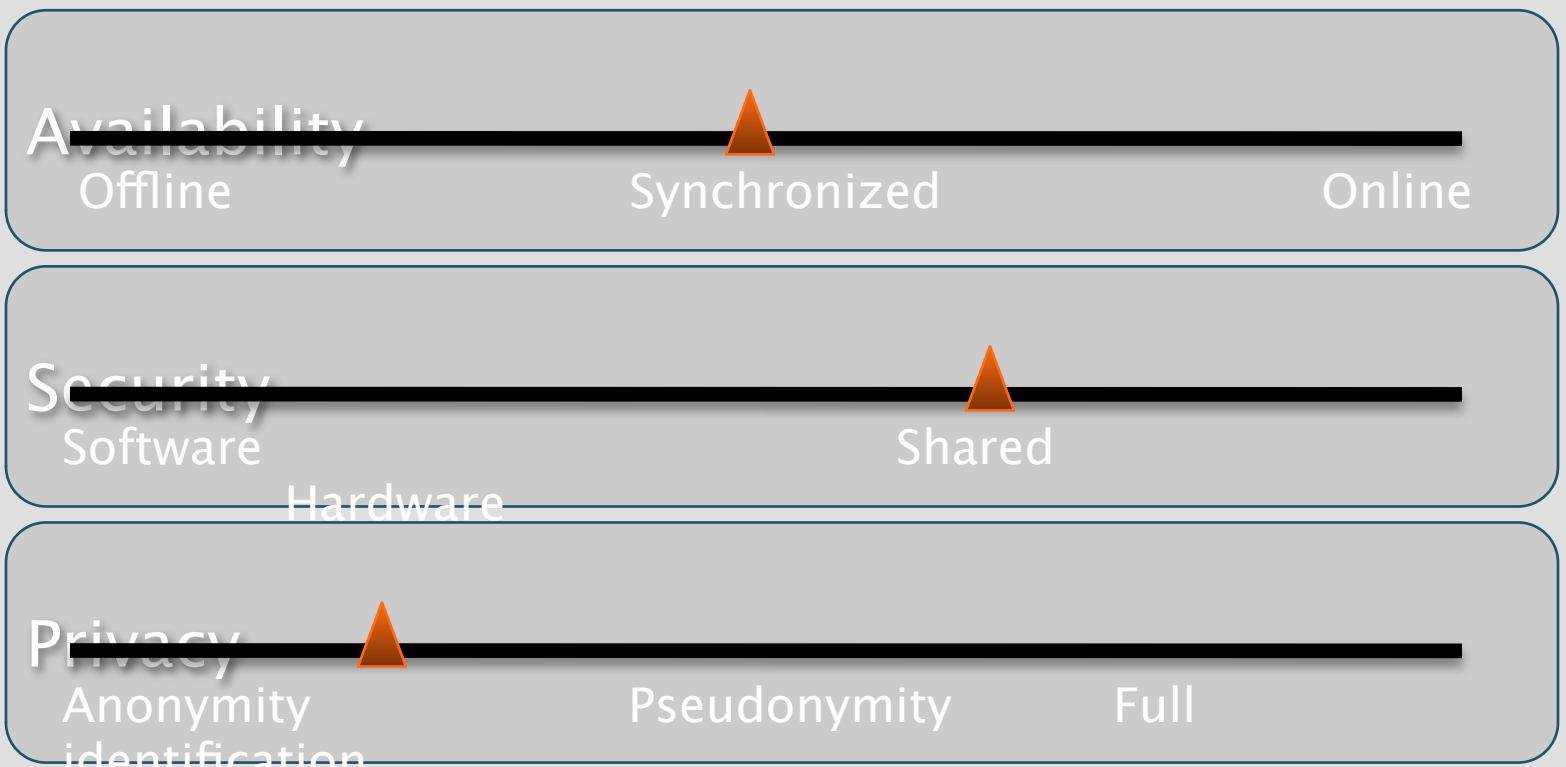
- Support for full spectrum of assurance
  - From anonymity, to pseudonymity, to full identification
  - Maintains strong accountability (revocation, audit trail, misuse tracing)
  - Minimal disclosure and user control
- Strong multi-party security
  - Phishing-resistant strong authentication
  - Eliminates some insider attacks at IdP / CA
  - Lending / pooling / reuse protections
  - Efficient hardware protection
- On-demand or disconnected

Resources

- Videos:
  - Scott Charney's RSA 2010 announcement: http://www.rsaconference.com/2010/usa/recordings/keynote-catalog.htm
  - Intro: http://channel9.msdn.com/shows/Identity/Announcing-Microsofts-U-Prove-Community-Technical-Preview-CTP
  - Technology overview: http://edge.technet.com/Media/Learn-what-Microsofts-U-Prove-release-is-all-about
- U-Prove CTP (March 2010):
  - Download location: http://www.microsoft.com/u-prove
  - Developer video: http://channel9.msdn.com/shows/Identity/U-Prove-CTP-a-developers-perspective/

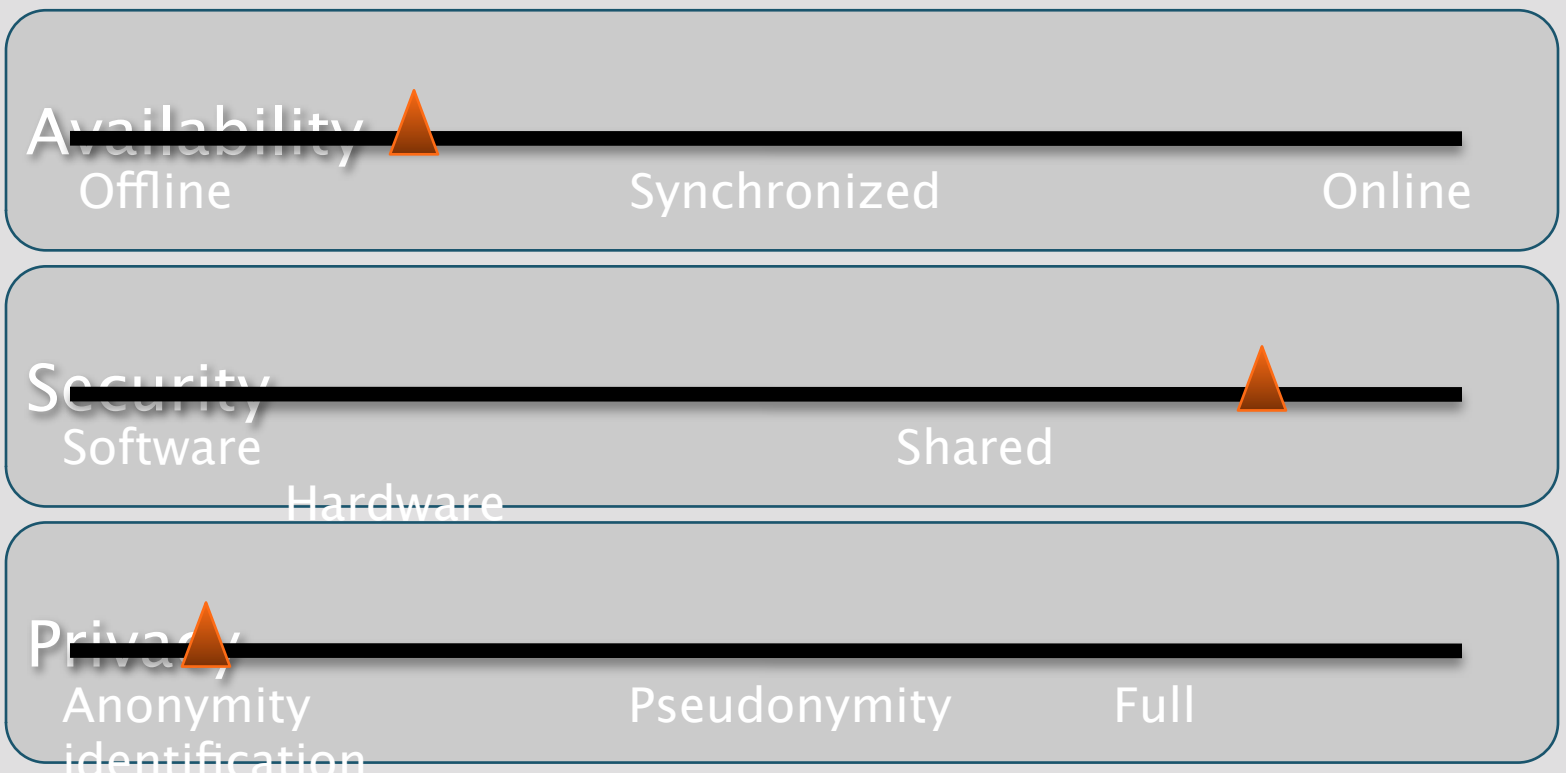
The U-Prove mixing

enabling a larger use-case spectrum



The U-Prove mixing

enabling a larger use-case spectrum

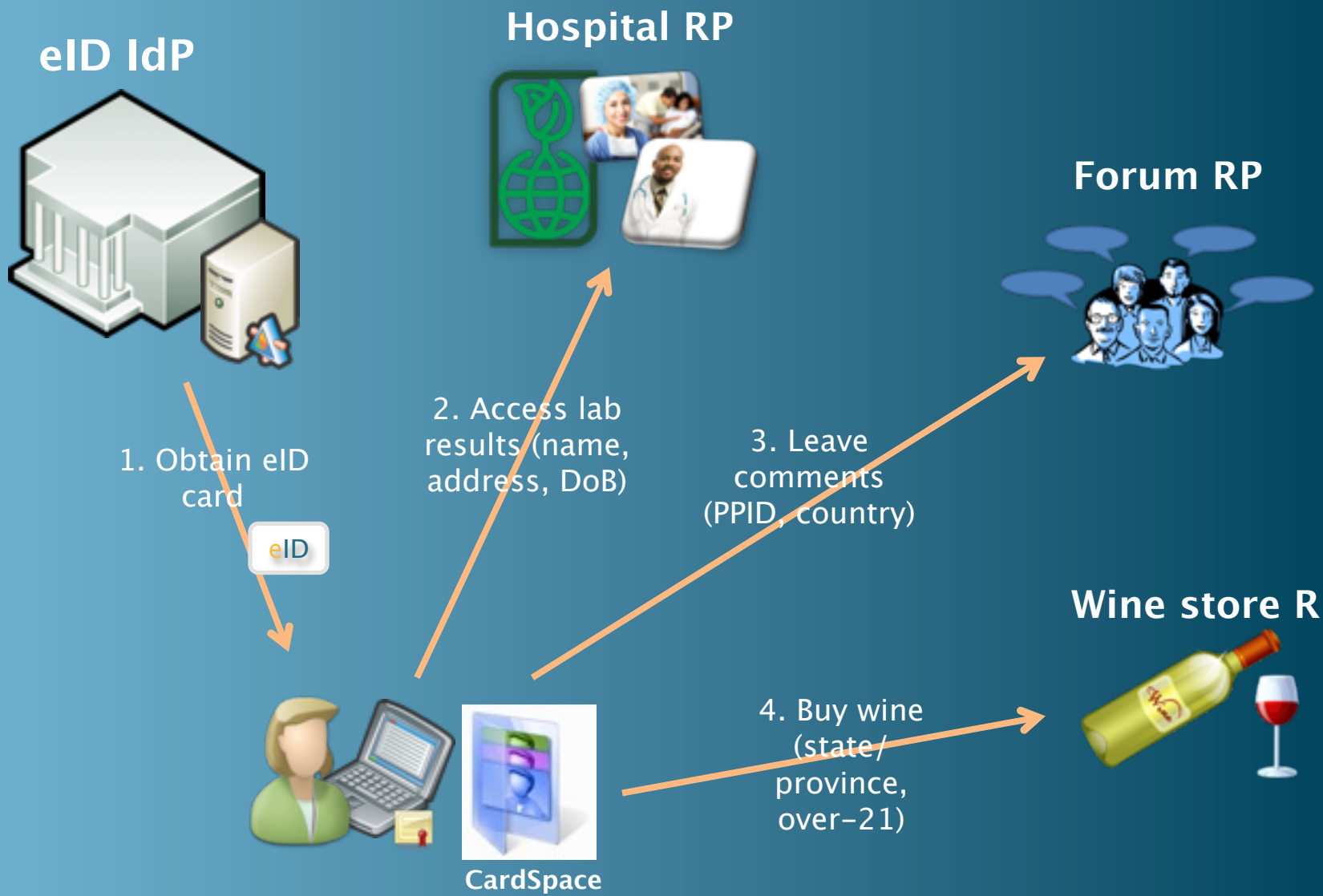


Demo
(using March 2010 CTP)

Scenario

- Alice is issued an eID information card
  - The information card is protected by a X.509 certificate, e.g., stored on the eID smartcard. (Here, the certificate is installed on the machine)
- She then
  - Obtains lab results from a hospital after proving who she is
  - Leaves anonymous comments at her government citizen forum
  - Buys wine online, proving she is over-21 and from Washington, leaving behind an auditable presentation transcript of these facts

Scenario summary



eID Card Provisioning

- User downloads eID information card (after appropriate identity proofing)
  - E.g., visits point of service in person and receives an activation code
- CardSpace efficiently retrieves multiple U-Prove tokens encoding the card claim values
  - The user authenticates to the STS using her X.509 cert
  - Tokens are stored securely encrypted on the machine
- Benefits:
  - Reduces load on IdP's STS, which won't get hit every time the user presents the card
  - IdP will not be aware of the user's card usage

Hospital lab results

- User presents full address, name, and D.o.B., and hospital locates her lab results
- Same security/privacy as if the user presented her ID in person

Government forum

- User leaves comments on a forum using an “authenticated” pseudonym
  - Users are anonymous, but only members of the community (e.g., US resident) can leave comments
  - No one (including the IdP itself) can hijack the pseudonym and post “forged” comments
    - PPID claim value is derived from the presented U-Prove token

Wine store

- User buys some wine online, proving she is over-21 and in which province/state she resides
  - CardSpace applies the U-Prove token's private key when presenting the token; resulting presentation token is an auditable proof
    - In contrast, "proof keys" are not applied by identity selectors in web scenarios

Crypto Details

Blind Signature protocol

Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

Issuer

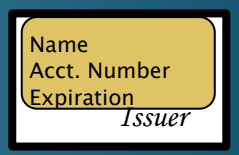
- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

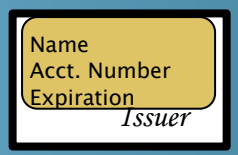
Blind Signature protocol



Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol



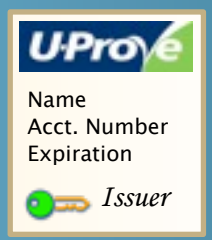
Issuer

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Blind Signature protocol

- Illustrates a simple blind signature
- U-Prove token issuance uses a "restrictive" blinding technique
  - More complex process to certify attributes

Proof of Knowledge Protocol



Verifier

Notes:

- Verifier only learns disclosed information, and is convinced that Alice knows the private key

Proof of Knowledge Protocol

Notes:

- Verifier only learns disclosed information, and is convinced that Alice knows the private key

Proof of Knowledge Protocol

Notes:

- Verifier only learns disclosed information, and is convinced that Alice knows the private key

Proof of Knowledge Protocol

Notes:

- Verifier only learns disclosed information, and is convinced that Alice knows the private key

Proof of Knowledge Protocol

Proof

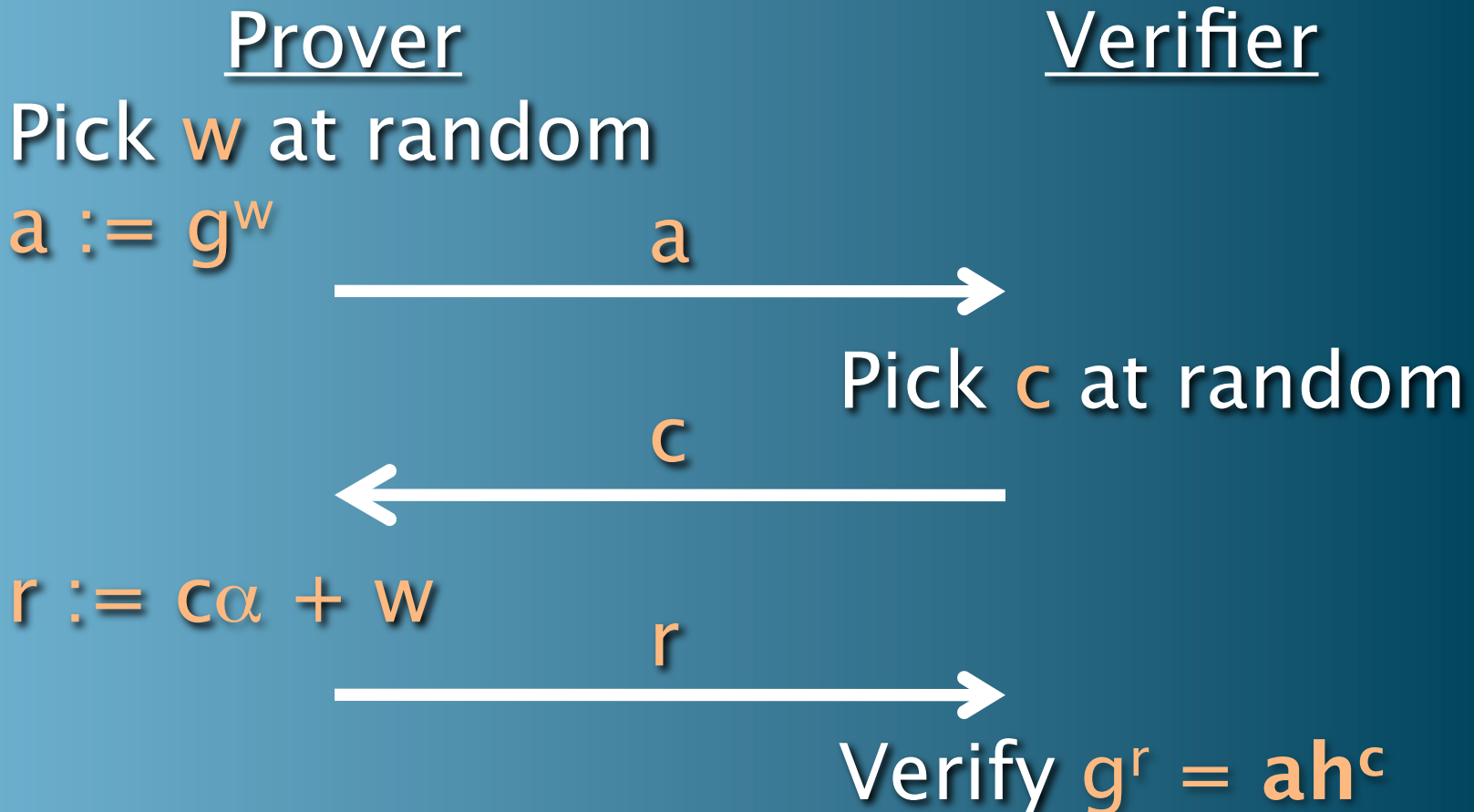
Verifier

Notes:

- Verifier only learns disclosed information, and is convinced that Alice knows the private key

Schnorr protocol

- Goal: prove knowledge of α w.r.t. g on the public element $h = g^{\alpha}$



U-Prove protocols

- U-Prove public key is a bit more complex:
  $h := (g_0\ g_1^{x_1} \ldots g_k^{x_k})^{\alpha}$
- The x_i values encode the attributes
- Uses Schnorr protocol as a primitive to prove properties of the attributes, e.g.,
  - $x_1 = 1$
  - x_2 != “alice”
  - x_3 >= 21
  - $(x_1 - x_3) / x_2 > x_4$