Zurich Research Laboratory

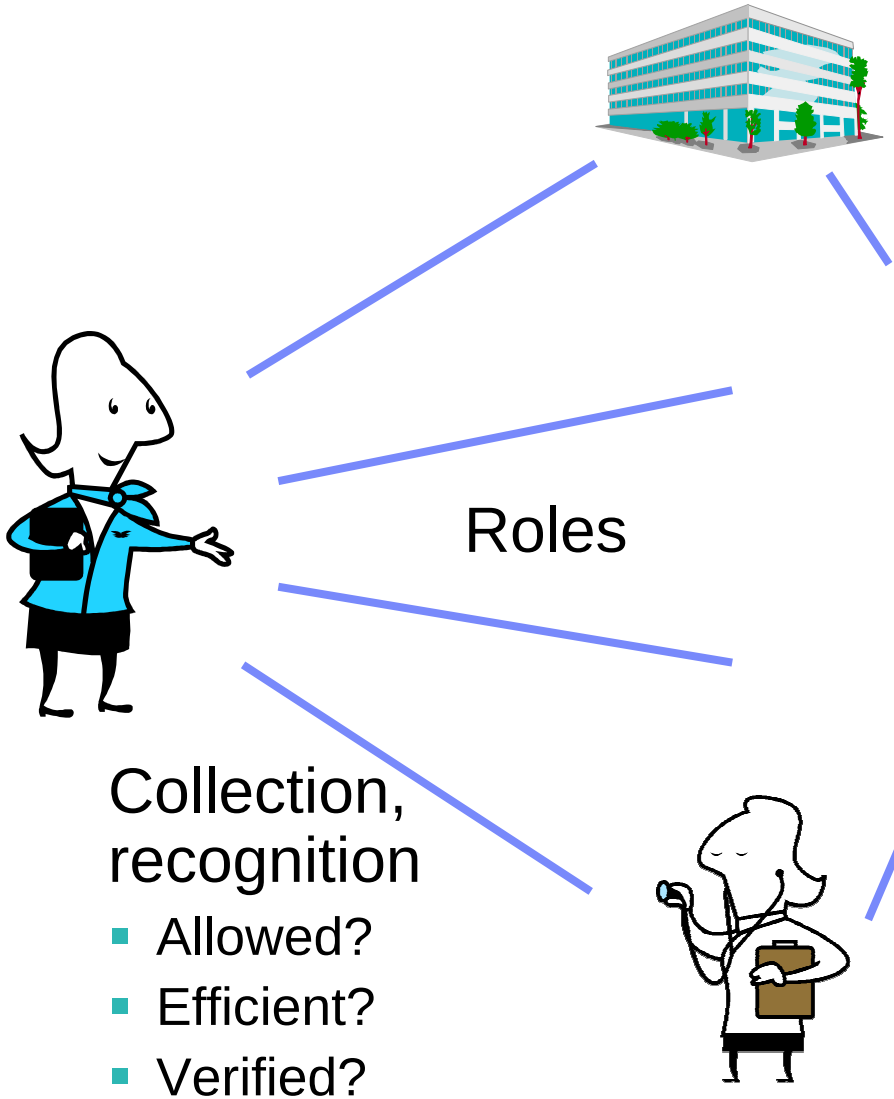
Web Services Security and Federated Identity Management

Birgit Pfitzmann, bpf@zurich.ibm.com
with Thomas Gross

March 8, 2005

www.zurich.ibm.com

Federated Identity Management (FIM)



Roles

Exchange
- Possible?
- Allowed?
- Efficient?

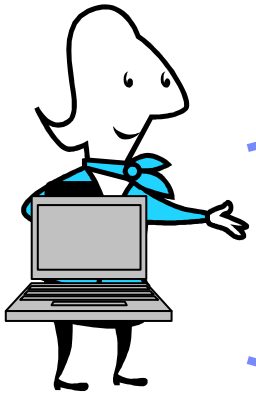
Collection, recognition
- Allowed?
- Efficient?
- Verified?

What's New?

Scientifically

Standards

Management



Federated single sign-on

Federated provisioning

Nothing.
(Event-based directory integration)

XML-based.
(DSML, SPML, WS-Provisioning)

More liability and privacy issues

Pure browser case.
(Else 3-party authentication)

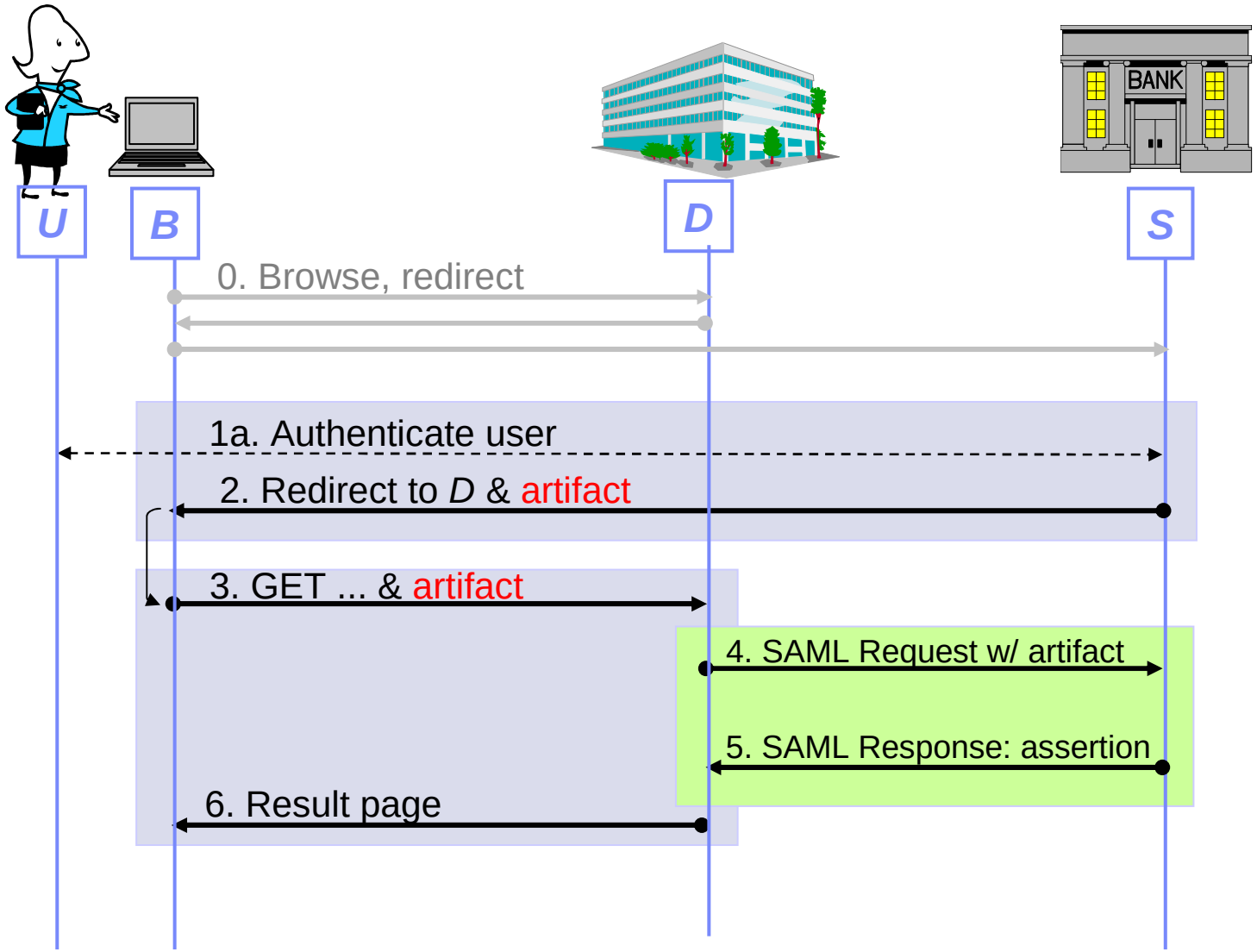
SAML, Liberty, WS-Fed Passive.
- Also WS versions
- Also more attributes

- More liability and privacy issues
- Metadata exchange

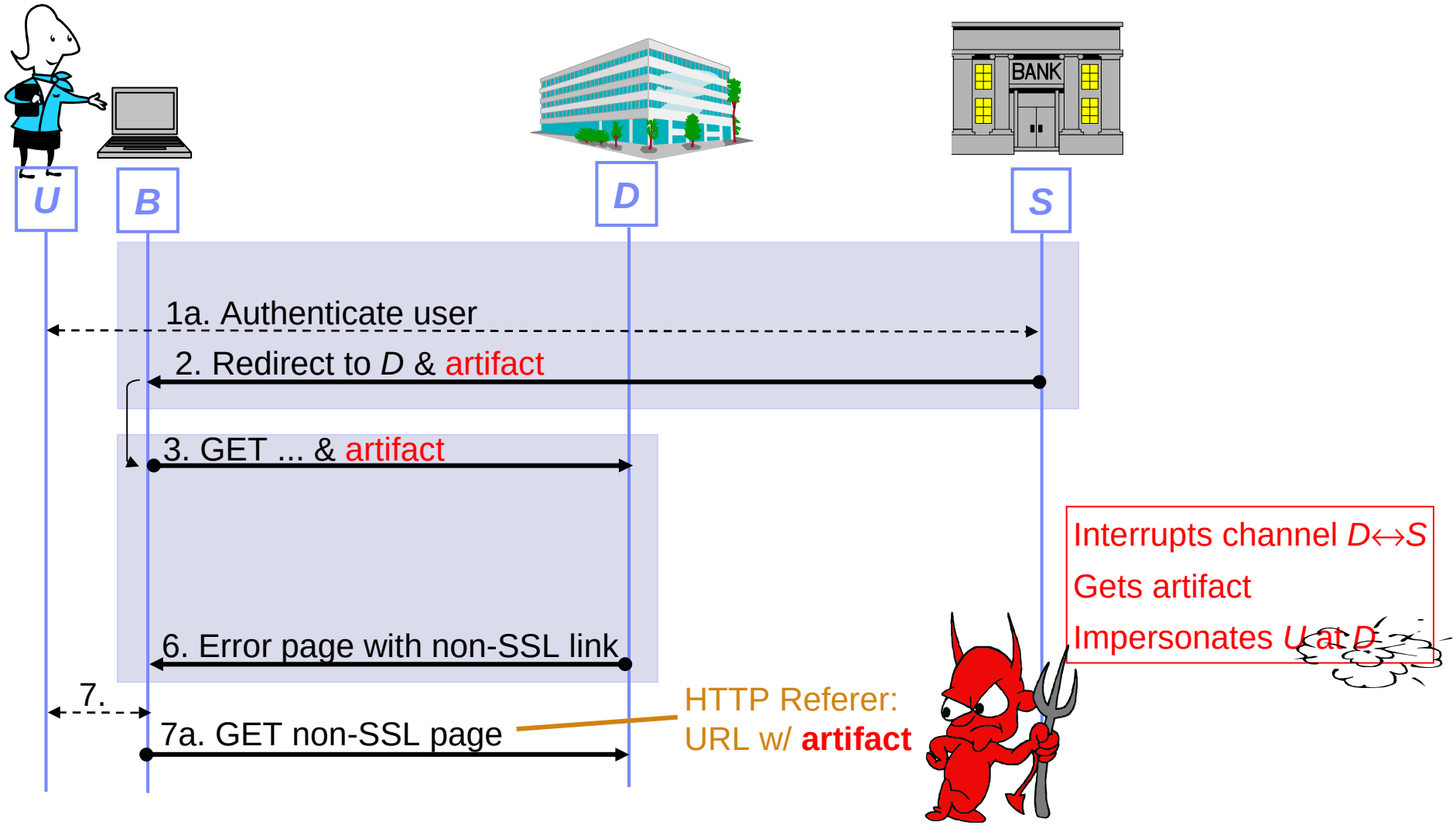
Literature

- Korman/Rubin 00: Passport problems
- Pfitzmann/Waidner 02 etc.: Privacy
- Pfitzmann/Waidner 02, Gross 03: Liberty and SAML problems
- Gordon et al: WS protocols, but not FIM
- Gross/Pfitzmann 04: Positive analysis of WSFPI

Attack Example: SAML Artifact Profile

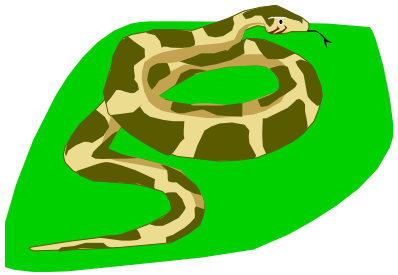


A Multi-Layer Vulnerability



What Can We Hope to Prove?

- Vulnerable operational environment
  - Based on passwords
  - Fake-screen attacks easy
  - Browser security assumed
  - OS security assumed
- Identity provider can impersonate user
- Privacy can be good except
  - Not anonymity AND certified attributes
  - Id supplier learns trail of id consumer URIs



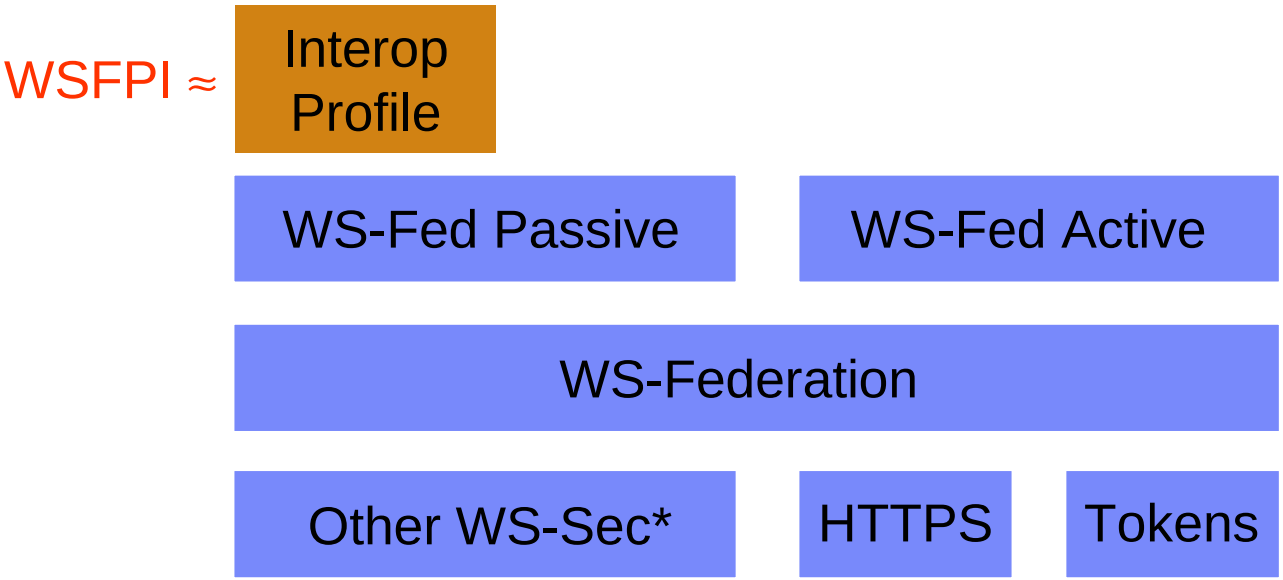
Here: Secure channel establishment under appropriate operational assumptions

Privacy Overview

Attributes about a person P are only given to an organization O, used there, or forwarded with P's consent.

- "Standard" implication
  - Explicit privacy policy for attributes (exceptions by law)
- Special cases:
  - Attribute = ID ⇒ Multiple roles
  - Attribute = URL ⇒ Traffic privacy
  - O = wallet holder ⇒ Allow multiple wallets, in particular local wallets

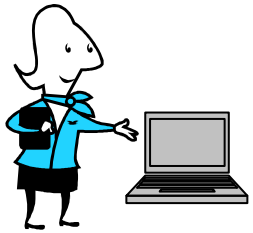
The WSFPI Protocol – Basis for a Proof

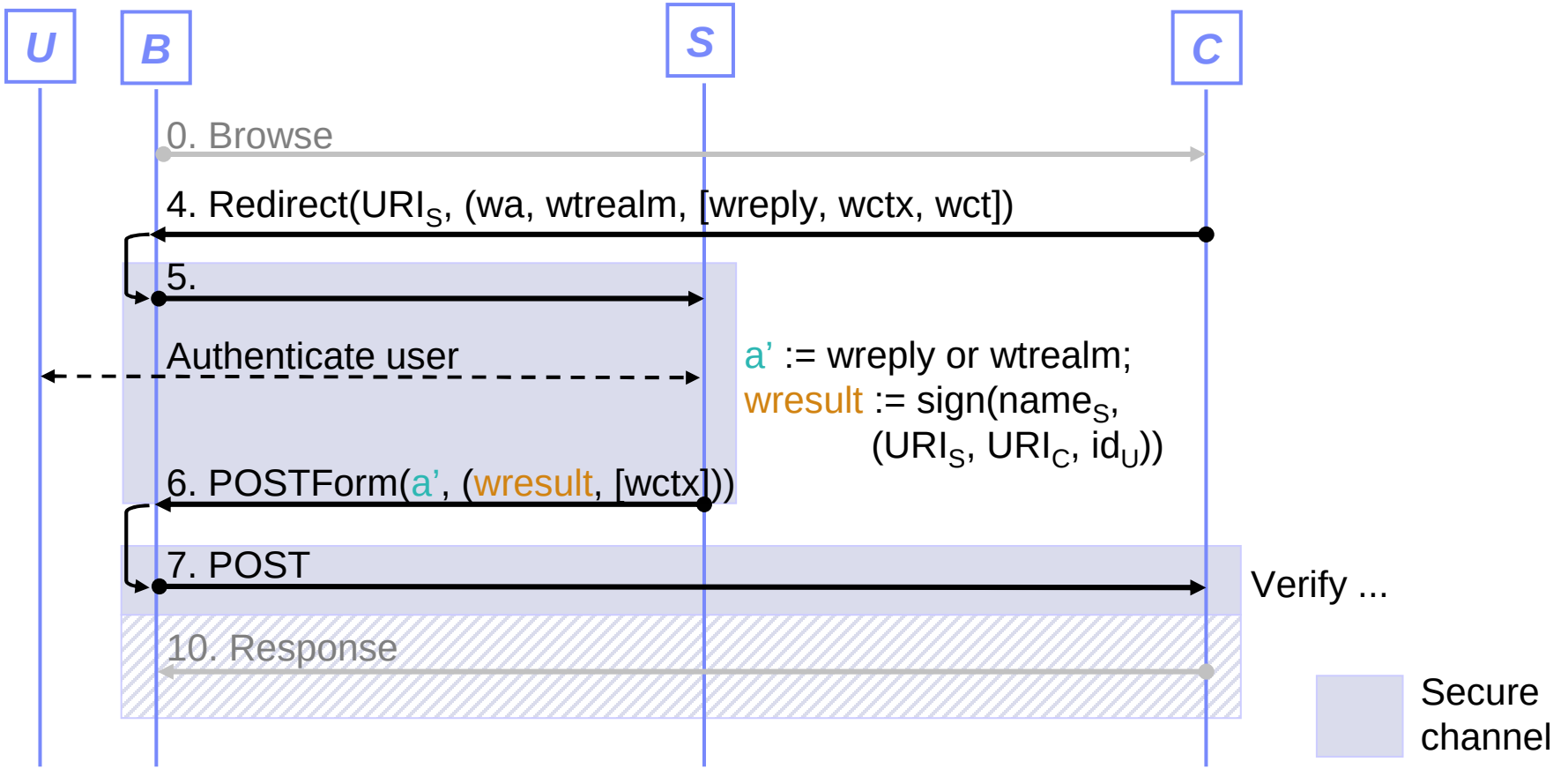


Proof Challenges

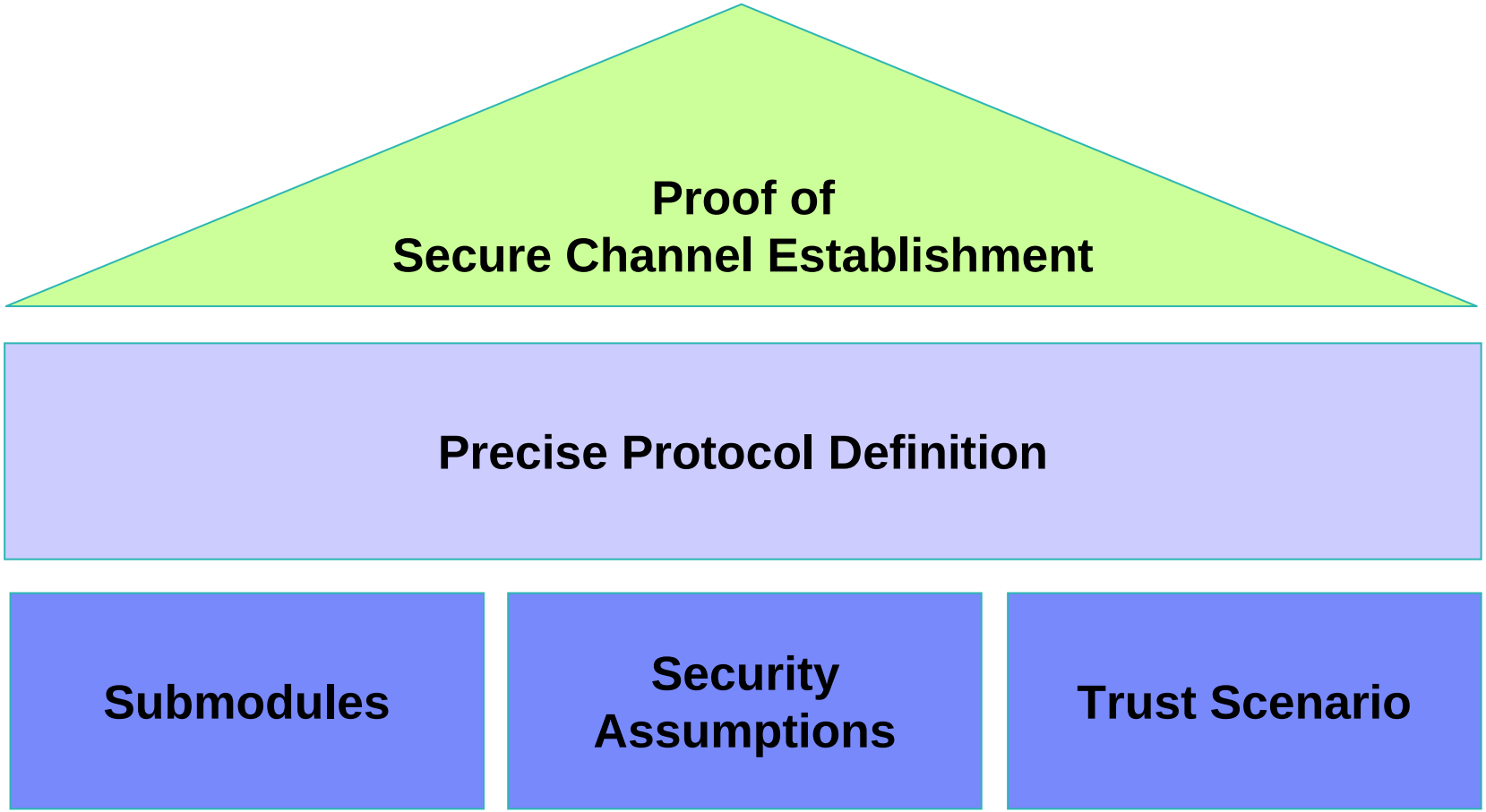
- Browsers and users
  - Browser as protocol party – restricted abilities
  - User also a protocol party – zero-footprint browser contains no identity
  - Browser and user might leak “protocol-internal” secrets
- Modularity, e.g., use of secure channels and SAML tokens
- Standard-style presentations
  - We prove rigorous instantiation

WSFPI: Correct Message Flow





Structure of the Proof



Summary and Outlook

- FIM: 3-party authentication, often with attribute exchange
- First protocol proof exists
- Next steps:
  - Relate assumptions to more detailed browser and user models
  - Use such models as criteria for browser evaluation
- Privacy:
  - Protocols *can* achieve privacy with 2 exceptions
  - For private use, GUI and policies equally important