

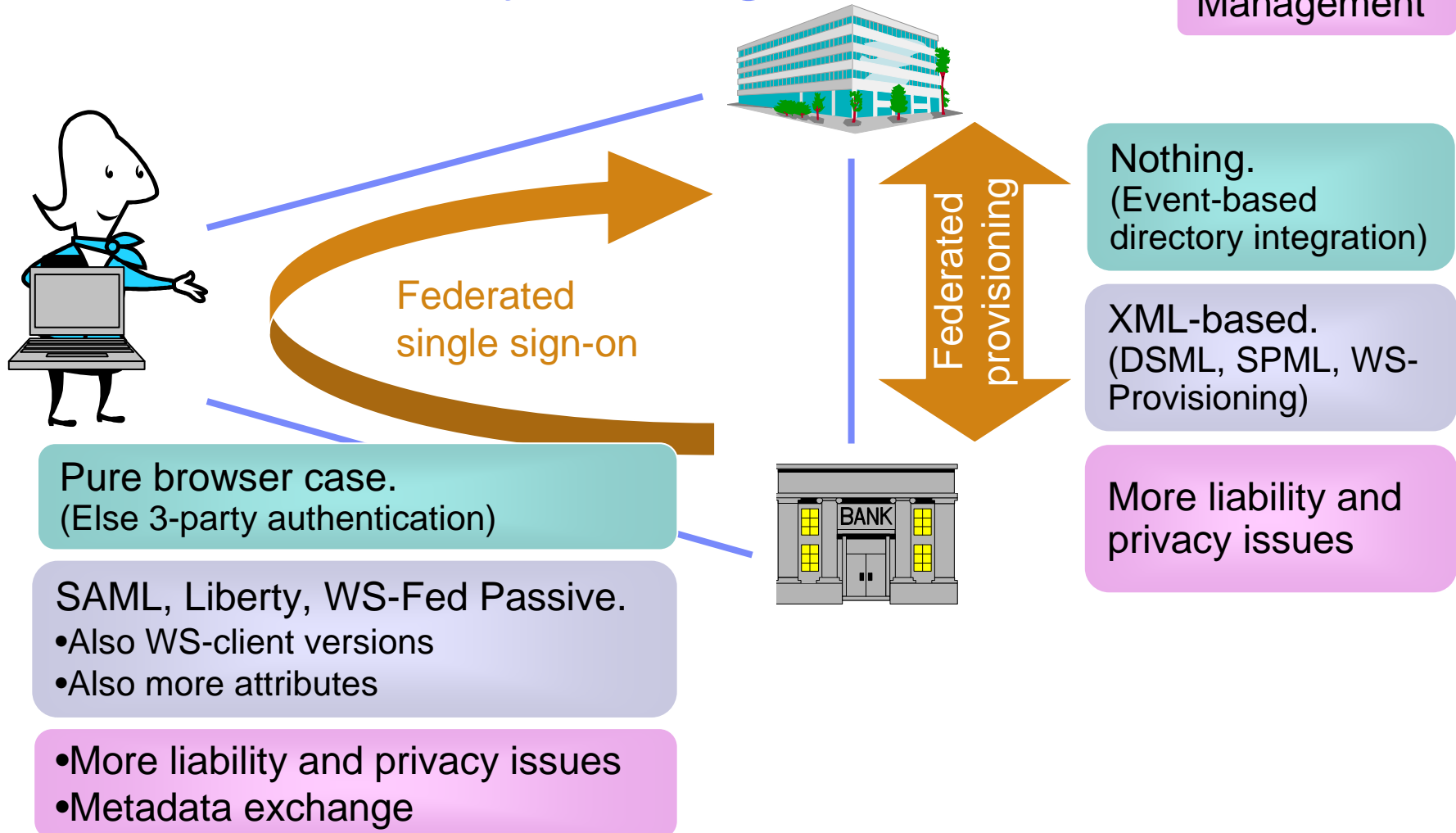


Zurich Research Laboratory

# Web Services and Federated Identity Management

Birgit Pfitzmann, [bpf@zurich.ibm.com](mailto:bpf@zurich.ibm.com) ::  
with Thomas Gross, Ahmad Sadeghi

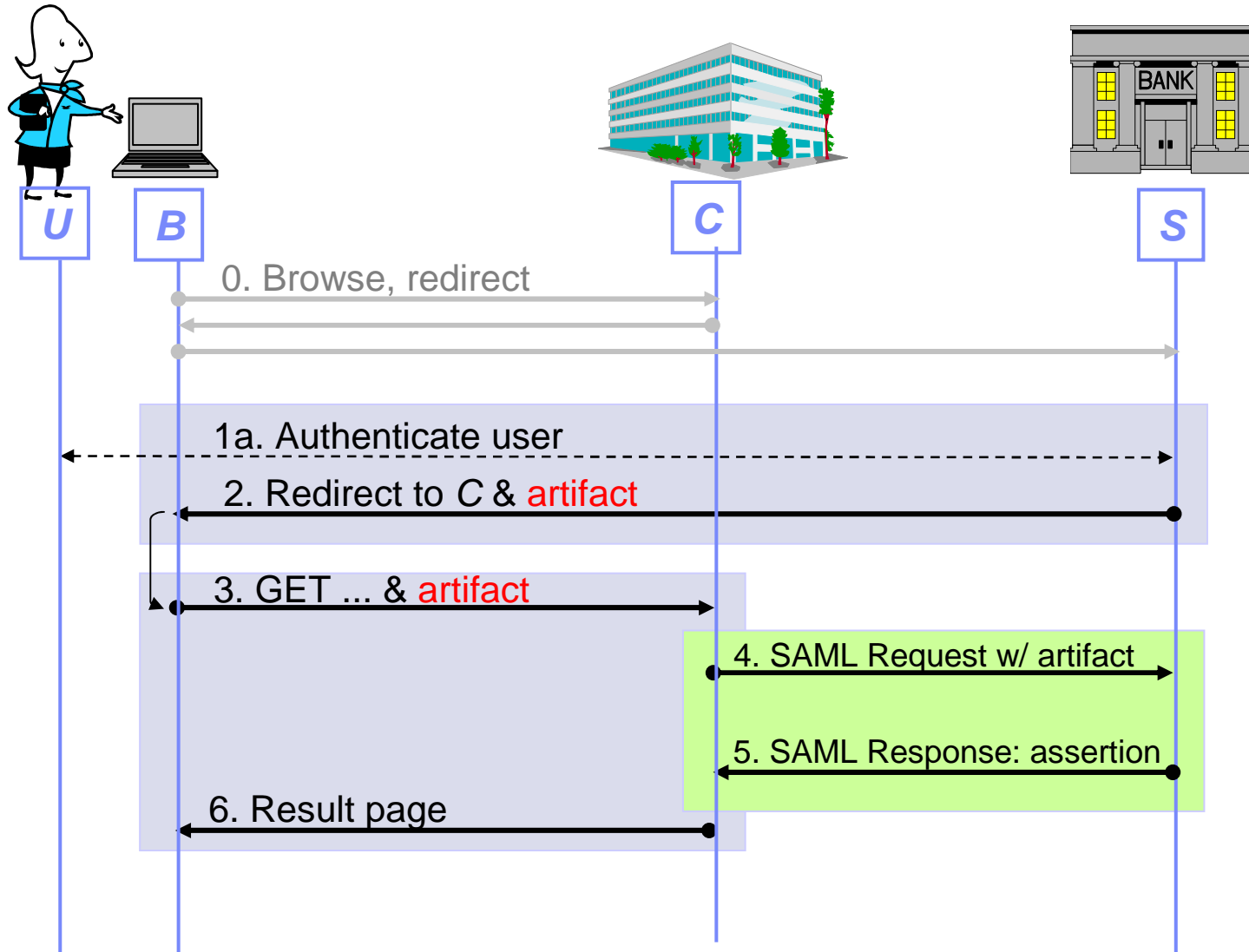
# What's New about Federated Identity Management?



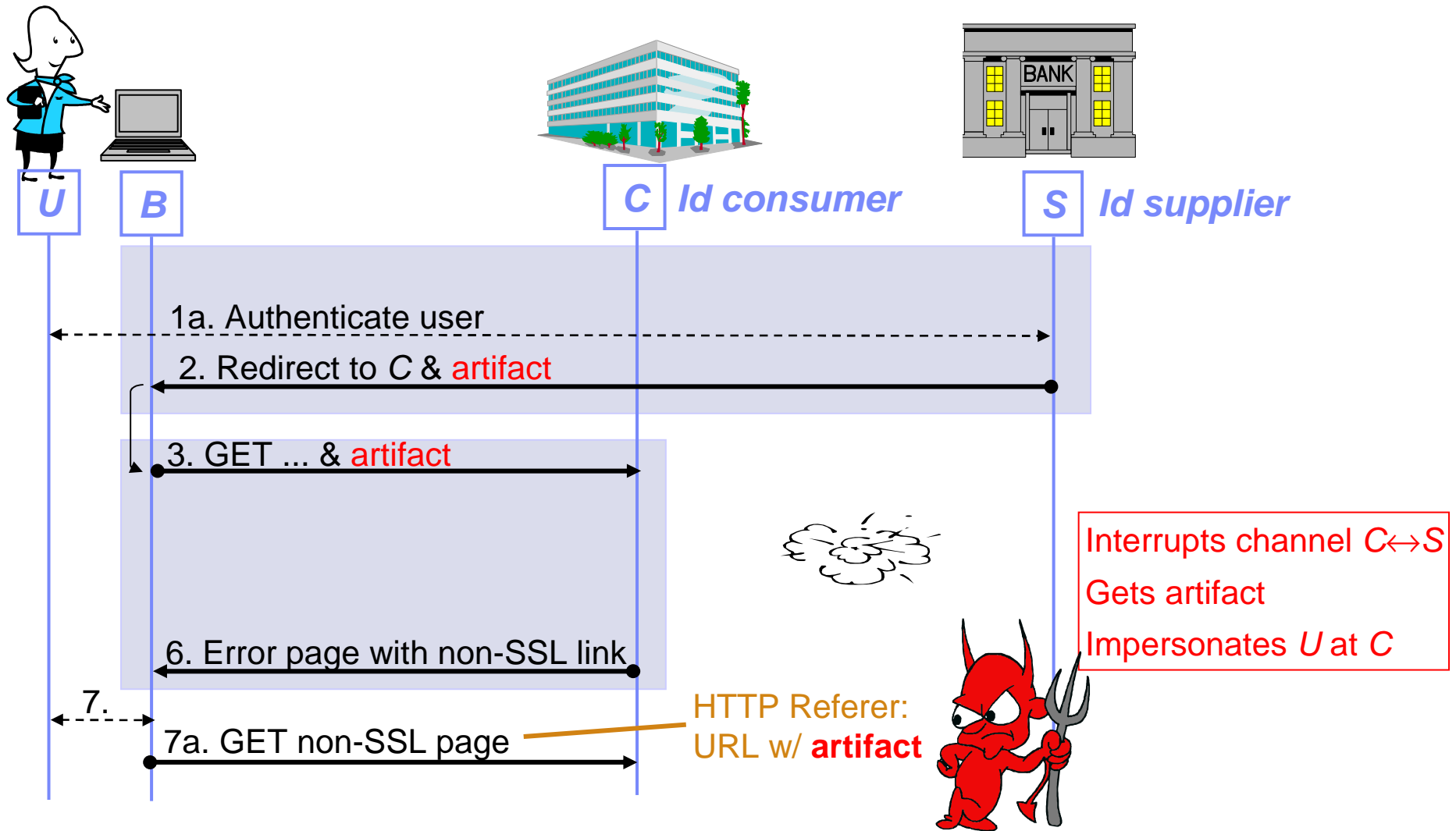
## State of the Art

- 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 based on “top-down” browser assumptions
- (Gross/Pfitzmann/Sadeghi 05: Detailed browser and user model, reproving “bottom-up”)

# Attack Example: SAML Artifact Profile



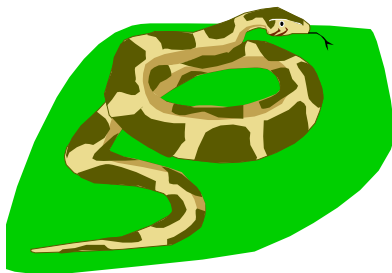
# A Multi-Layer Vulnerability



## What Can We Hope to Prove?

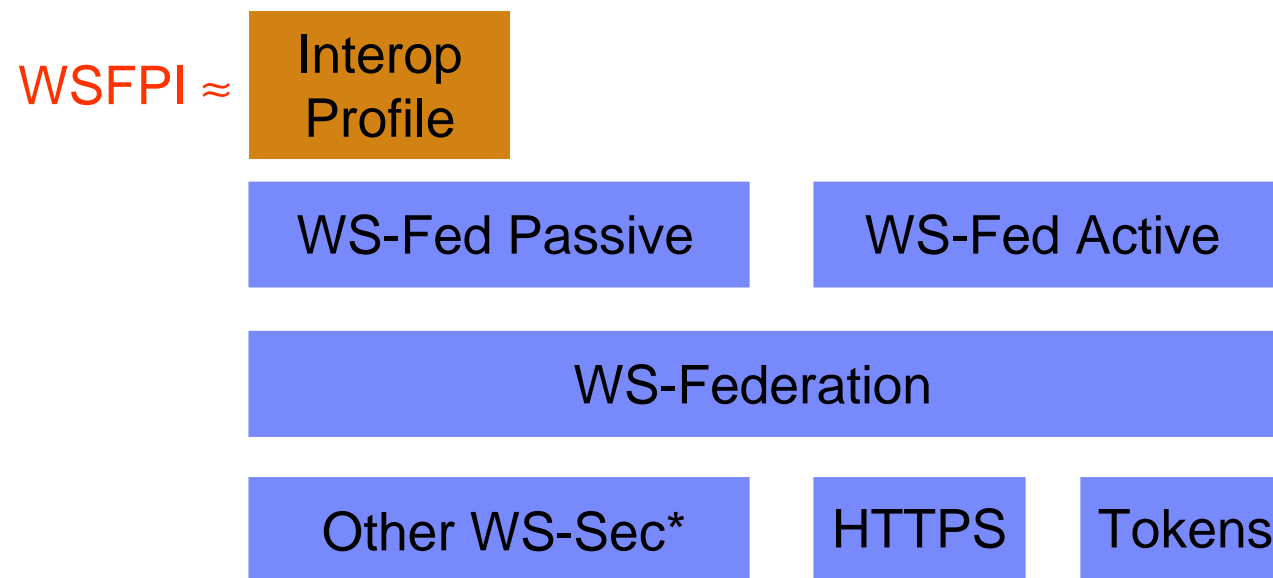


- Vulnerable operational environment
  - Based on passwords
  - Fake-screen attacks easy
  - Browser security assumed
  - OS security assumed
- Identity supplier can impersonate user
- Privacy can be good except
  - Not anonymity AND certified attributes
  - Id supplier learns trail of id consumer URIs



**Here: Secure channel establishment under appropriate operational assumptions**

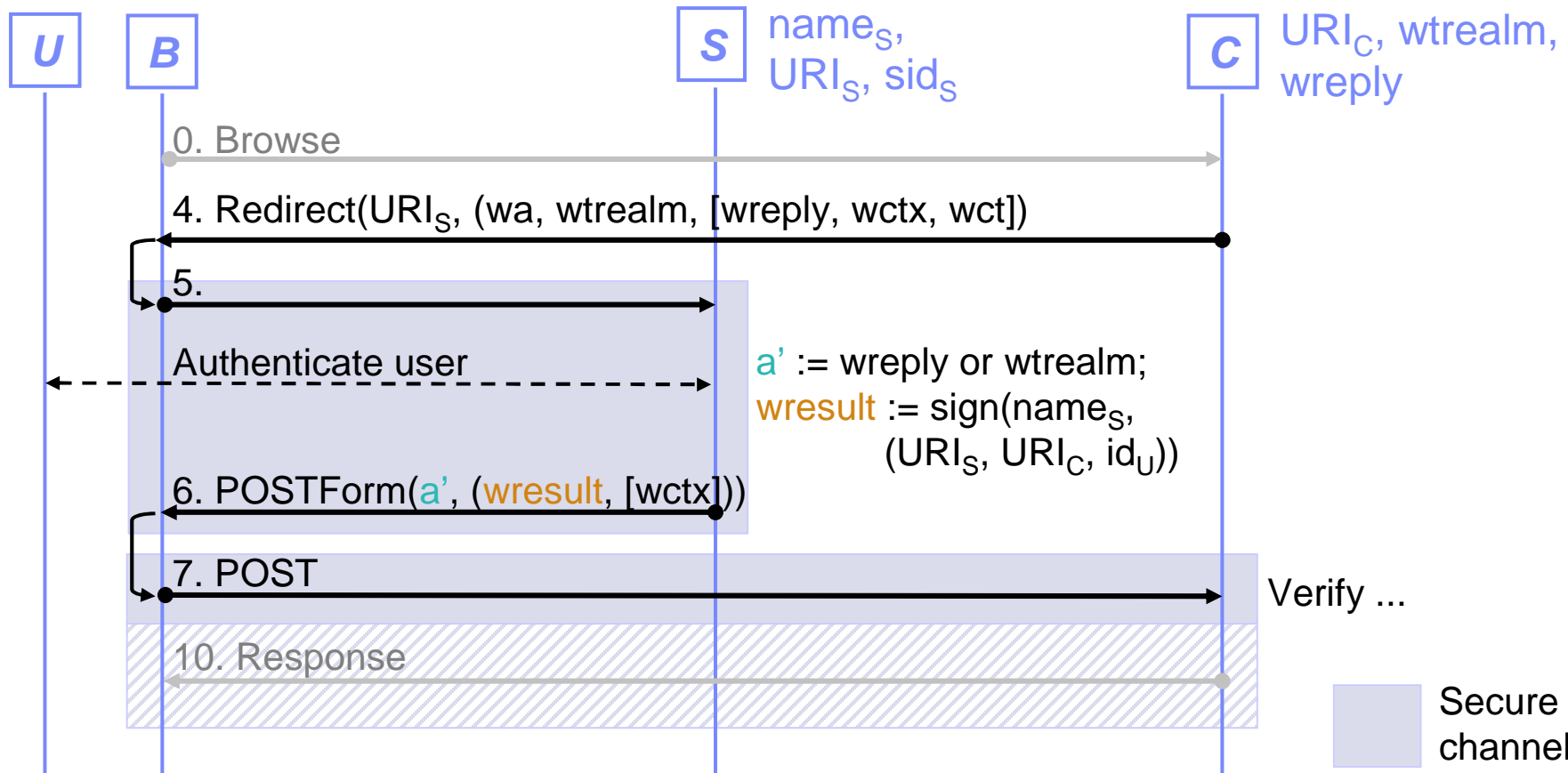
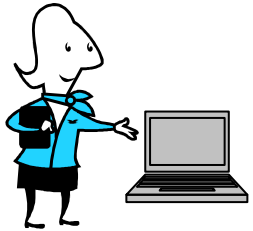
# The WSFPI Protocol – Basis for a Proof



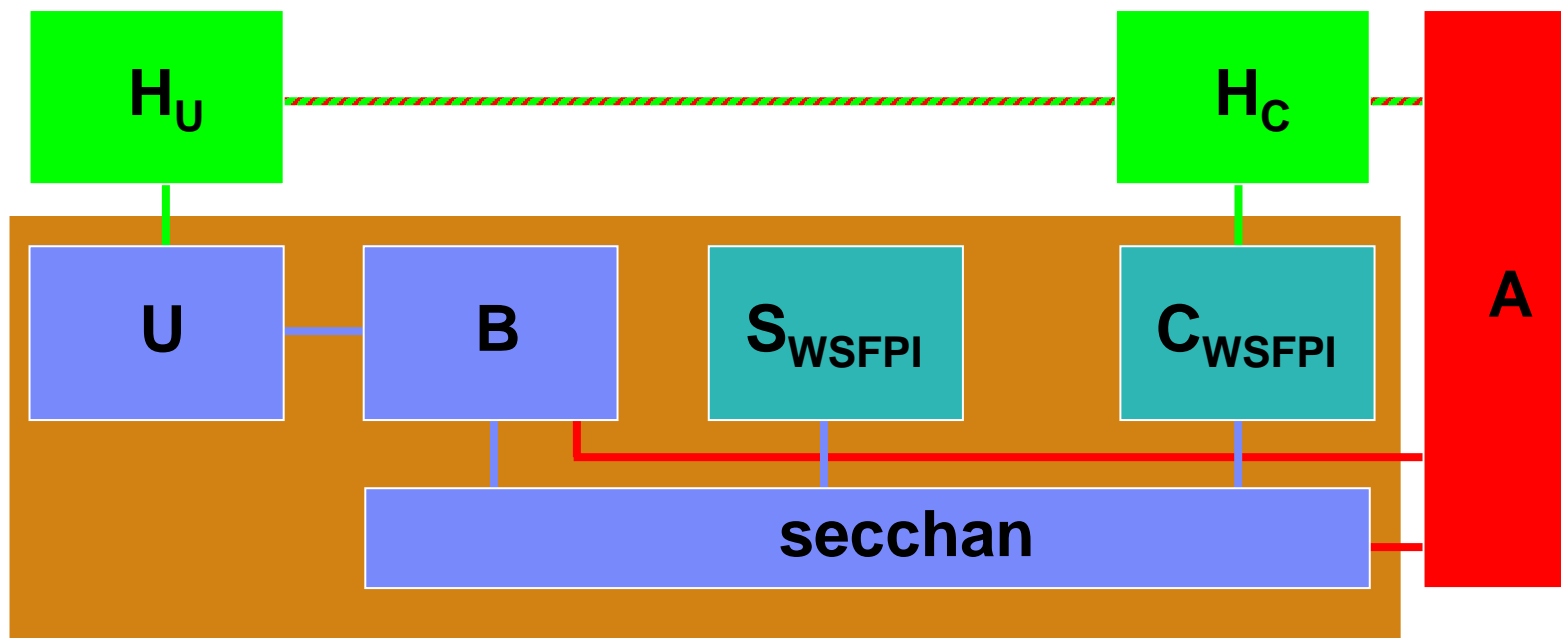
# Proof Challenges

- 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



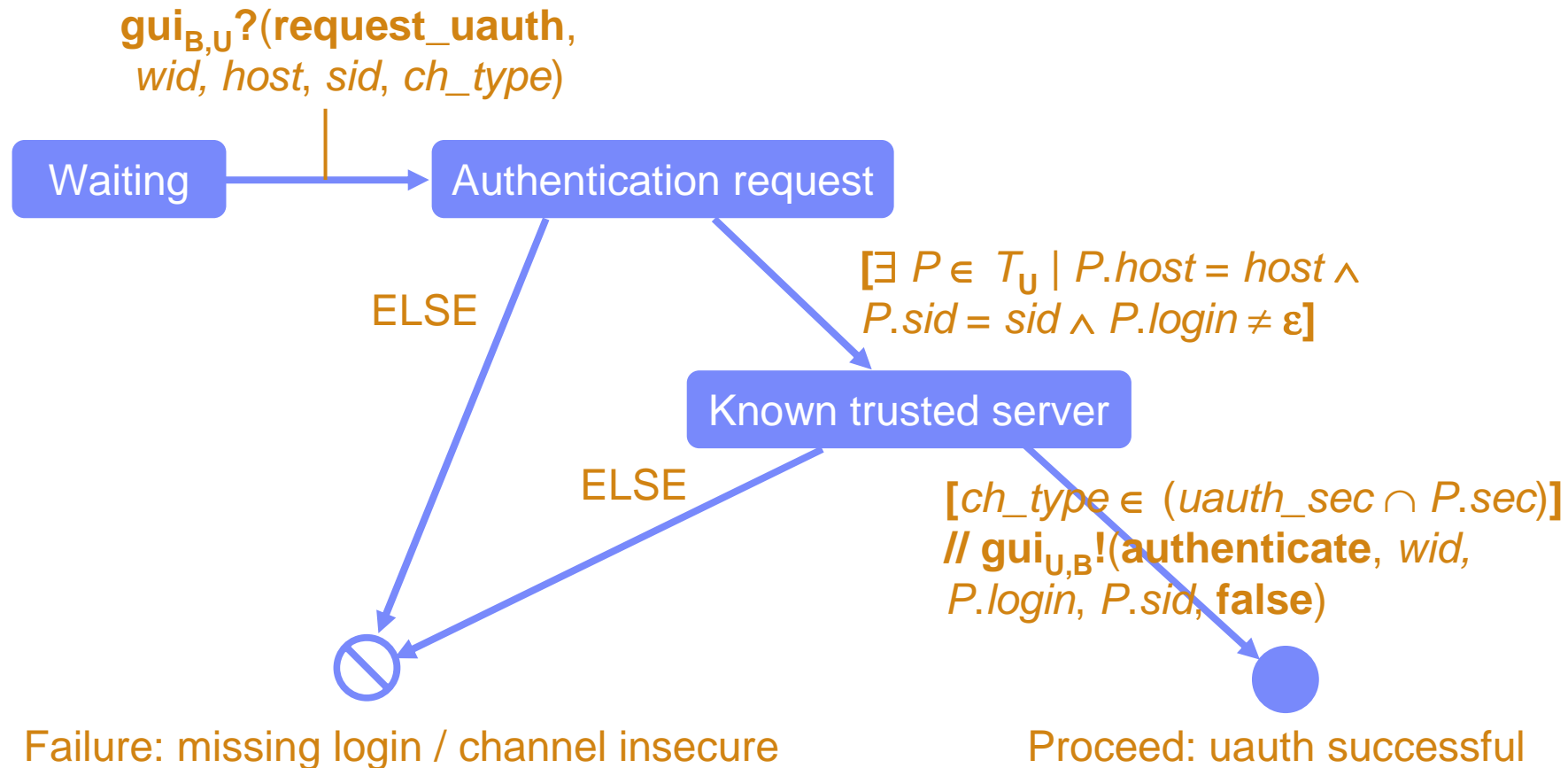
# Machines in Proofs WITH browser model



**Claim: Secure channels again**

## Small Example from the Model

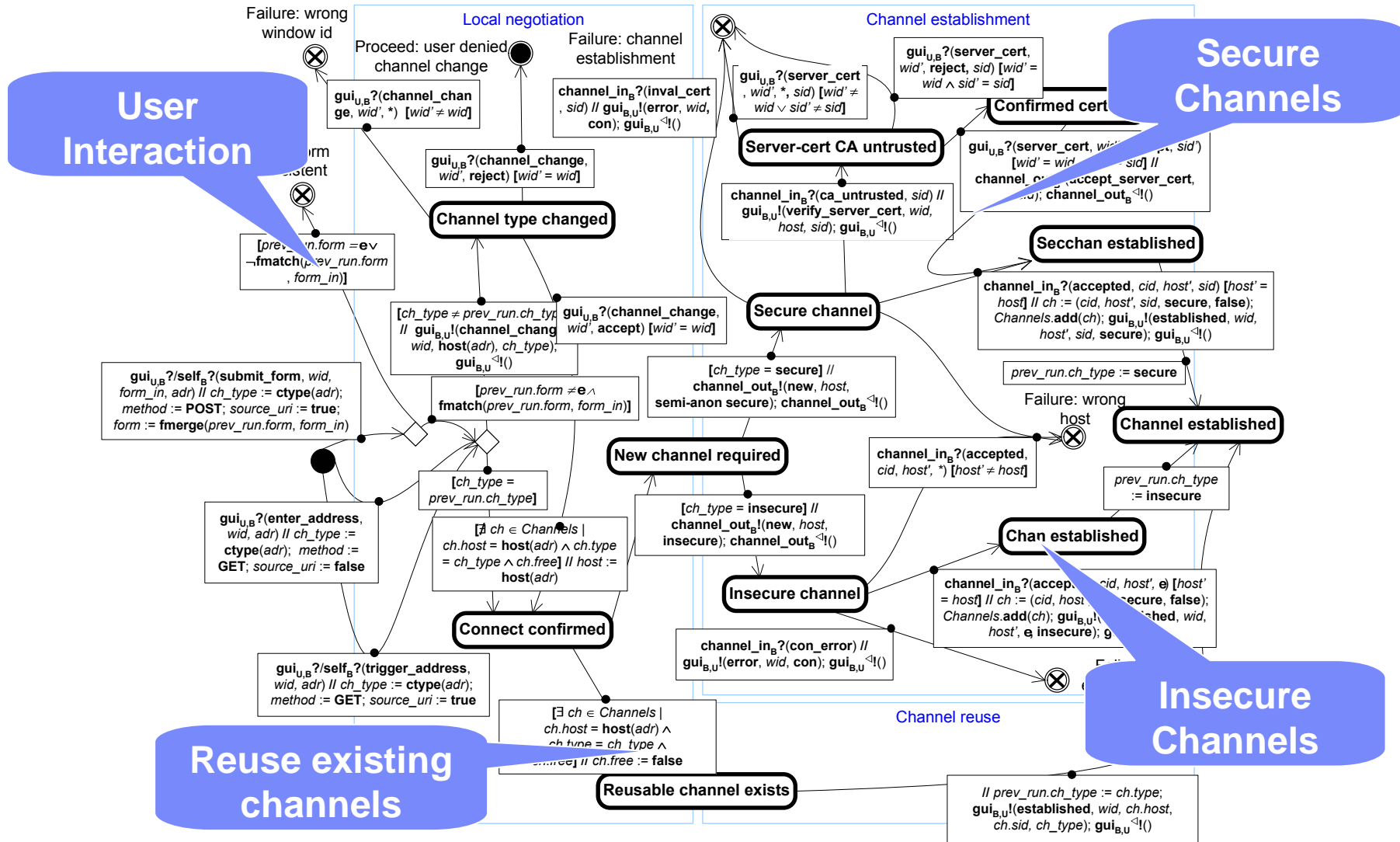
- Behavior of U upon authentication request (critical part to prevent phishing)



## Some Remarks on Browser Model

- Channel handling and main HTTP transactions
- User interaction
- Redirect and POSTform for 3-party protocols
- Leakage function, in particular Referer Tag
- Storage and loss of passwords, history, cache
  
- Proofs need assumptions that unmodeled information leakage really does not occur
  - Usable as future reference for what browsers should NOT do for use in FIM.

# First half of B's state diagram for 1 HTTP transaction



# Summary and Outlook

- **FIM:**
  - 3-party authentication
  - Often with attribute exchange and channel establishment
  - Special: Browser and user instead of dedicated machine
- **Our recent work:**
  - First protocol proof, based on strong assumptions
  - First detailed browser and user models + a lemma
- **Next step:** FIM proof based on browser model

## More Information

- Authors:
  - <http://www.zurich.ibm.com/~bpf/>
  - <http://www.prosecco.ruhr-uni-bochum.de/index.html>
- Our FIM and WS literature:
  - <http://www.zurich.ibm.com/security/identities/>
- IBM Zurich network security and crypto group:
  - <http://www.zurich.ibm.com/security/>