IBM Zurich Research Lab

Web Services Security and Federated Identity Management

Birgit Pfitzmann
with Th. Gross, A.-S. Sadeghi, M. Waidner

PaRISTIC, Bordeaux, Nov. 22, 2005

IBM Security and Privacy Research -- Goals

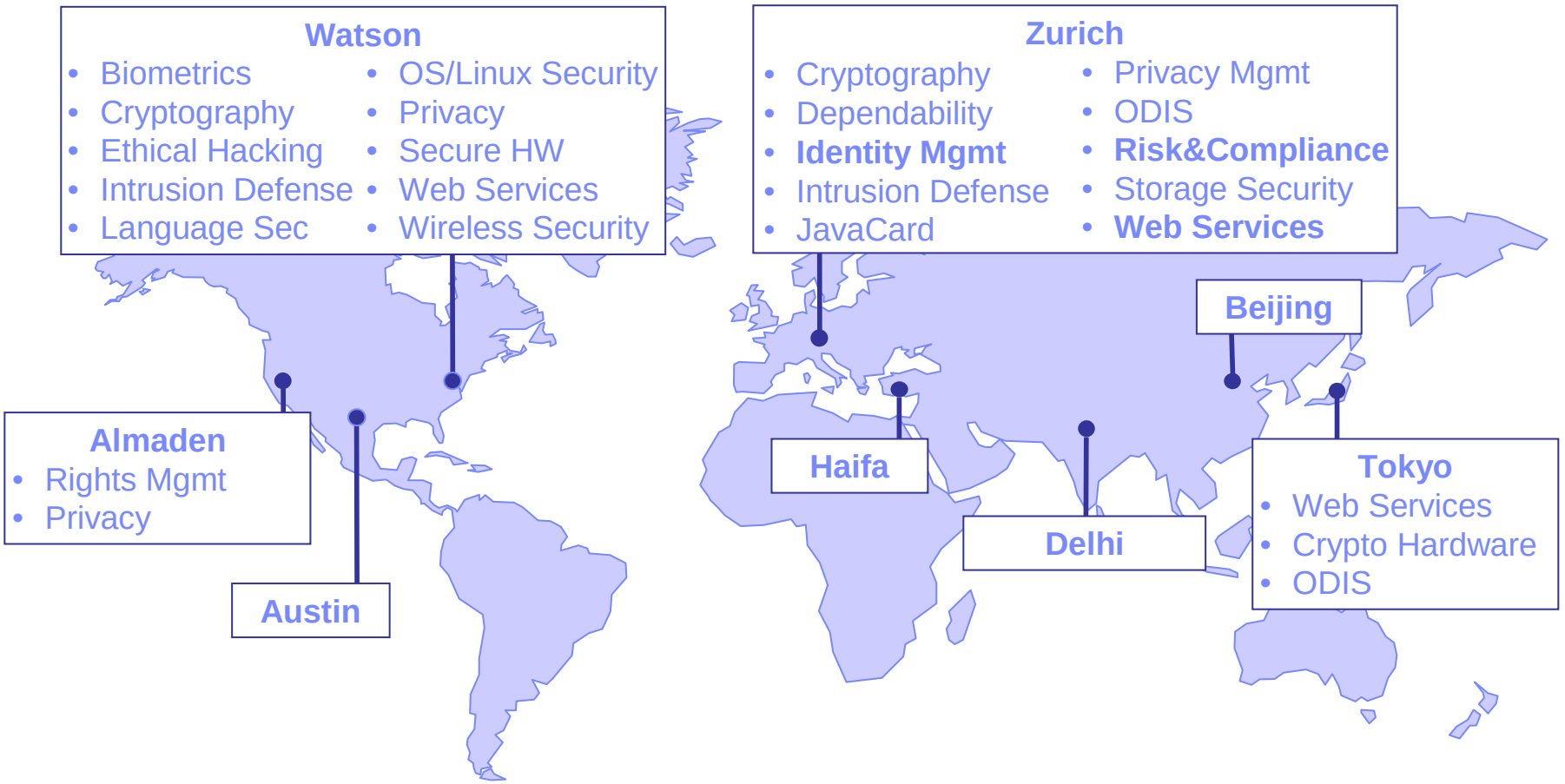
The right security and privacy in all of IBM's products (systems, software, services, solutions)

Innovative security and privacy products

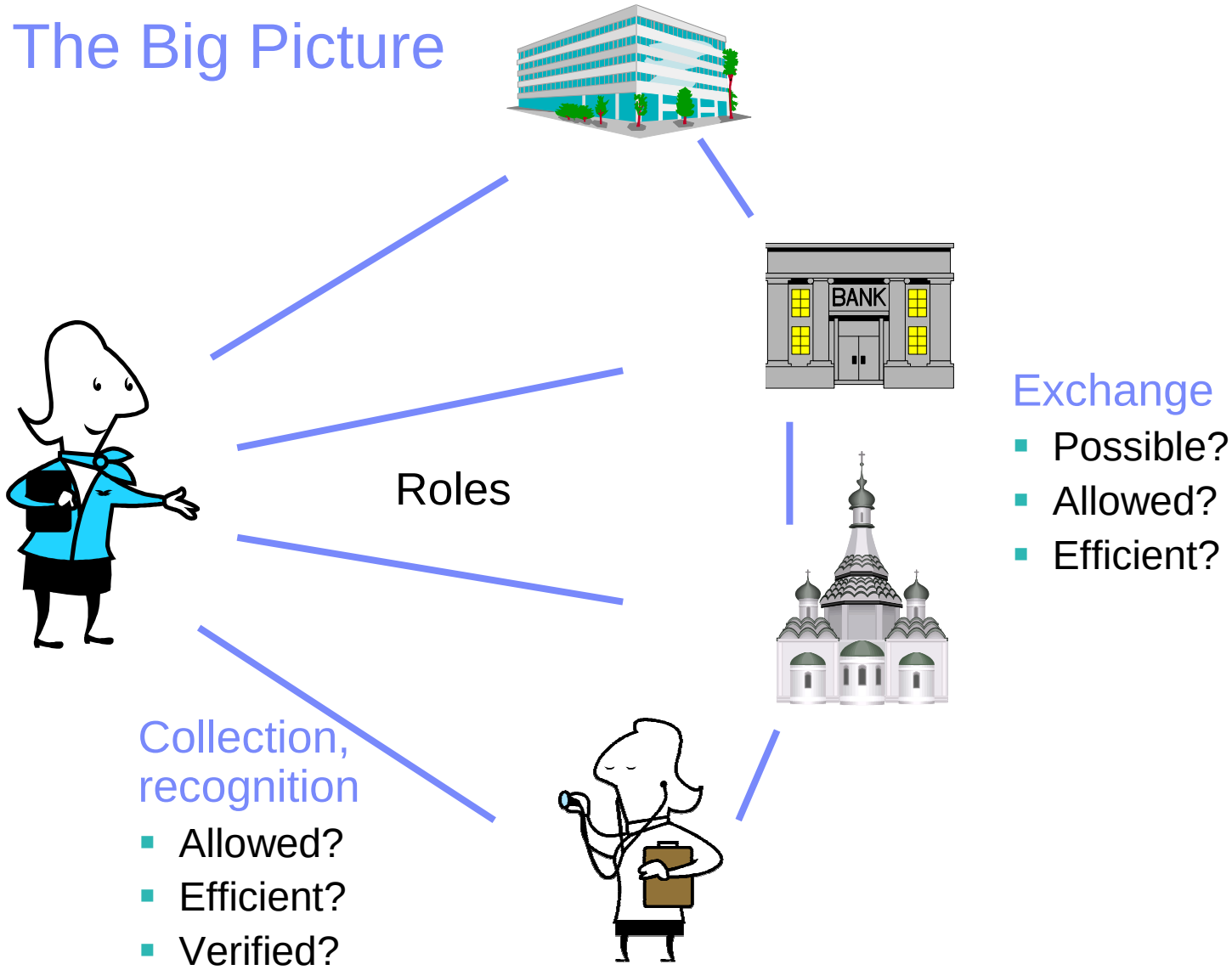
Innovative security and privacy solutions for specific customer problems

Leading research in security and privacy
Interface with the academic research community

IBM Security and Privacy Research -- Topics



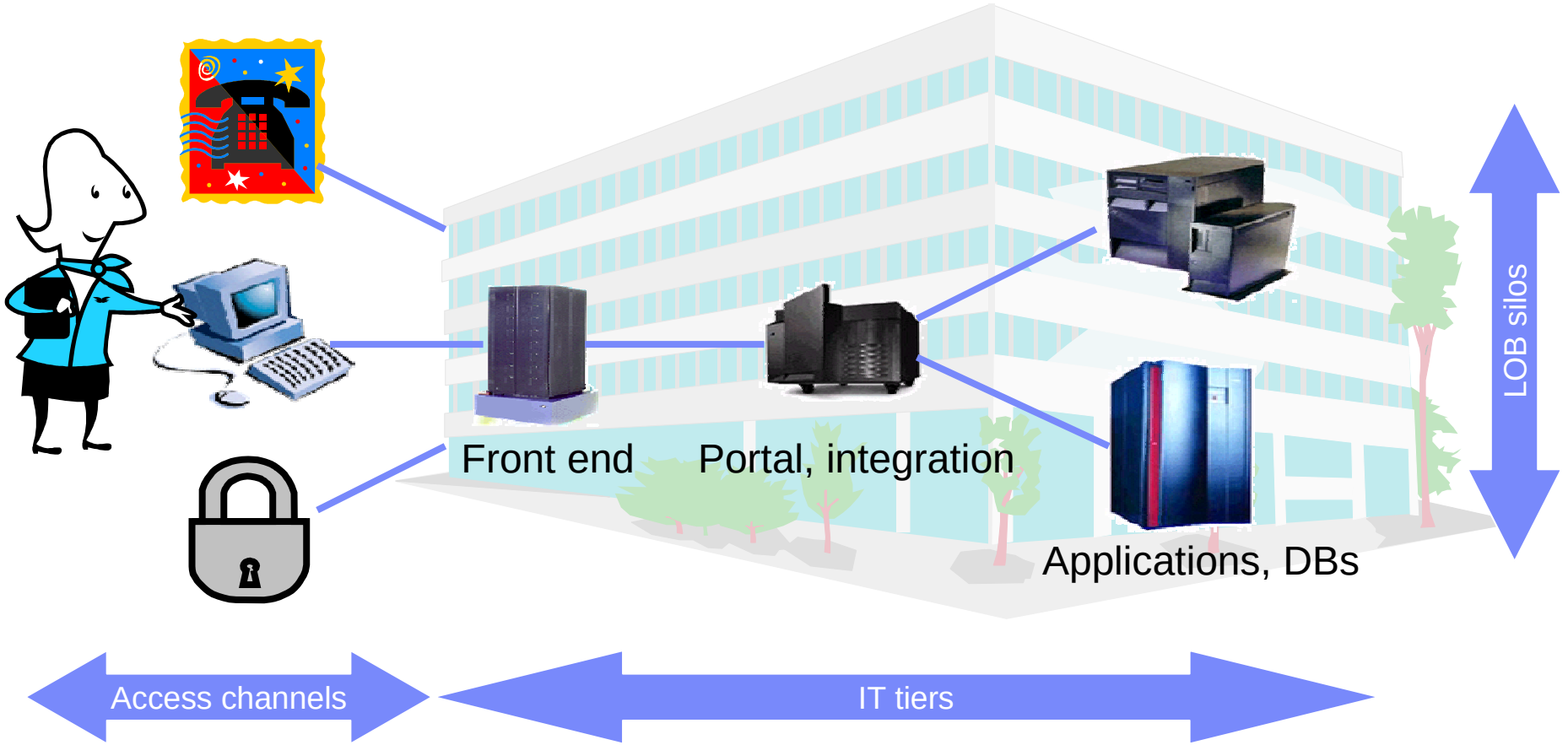
Identities: The Big Picture



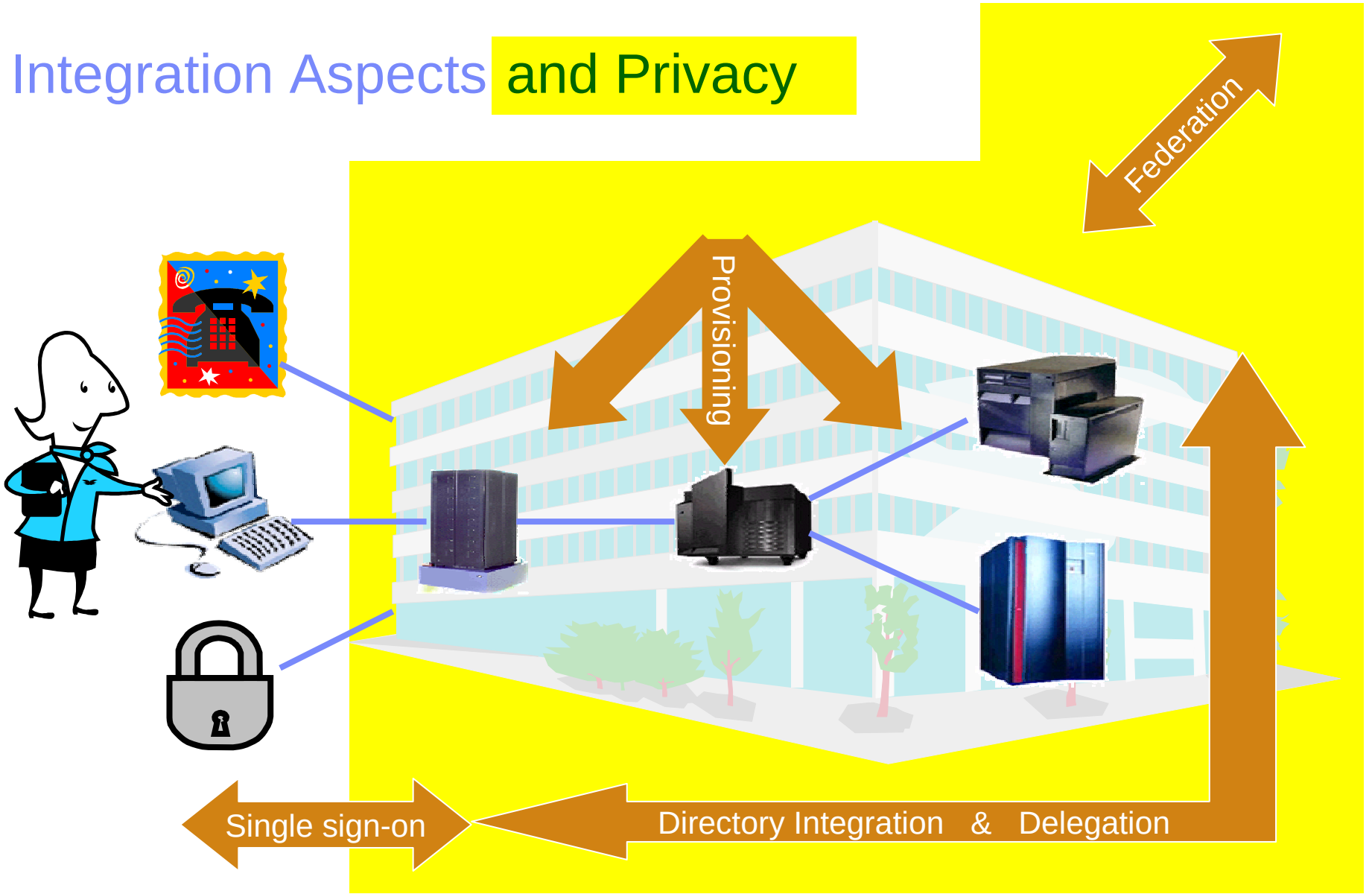
Content

- The big picture
- Security
- Privacy
- Summary

Identity in an Enterprise



Integration Aspects and Privacy



Drivers for Transforming Identity Infrastructure

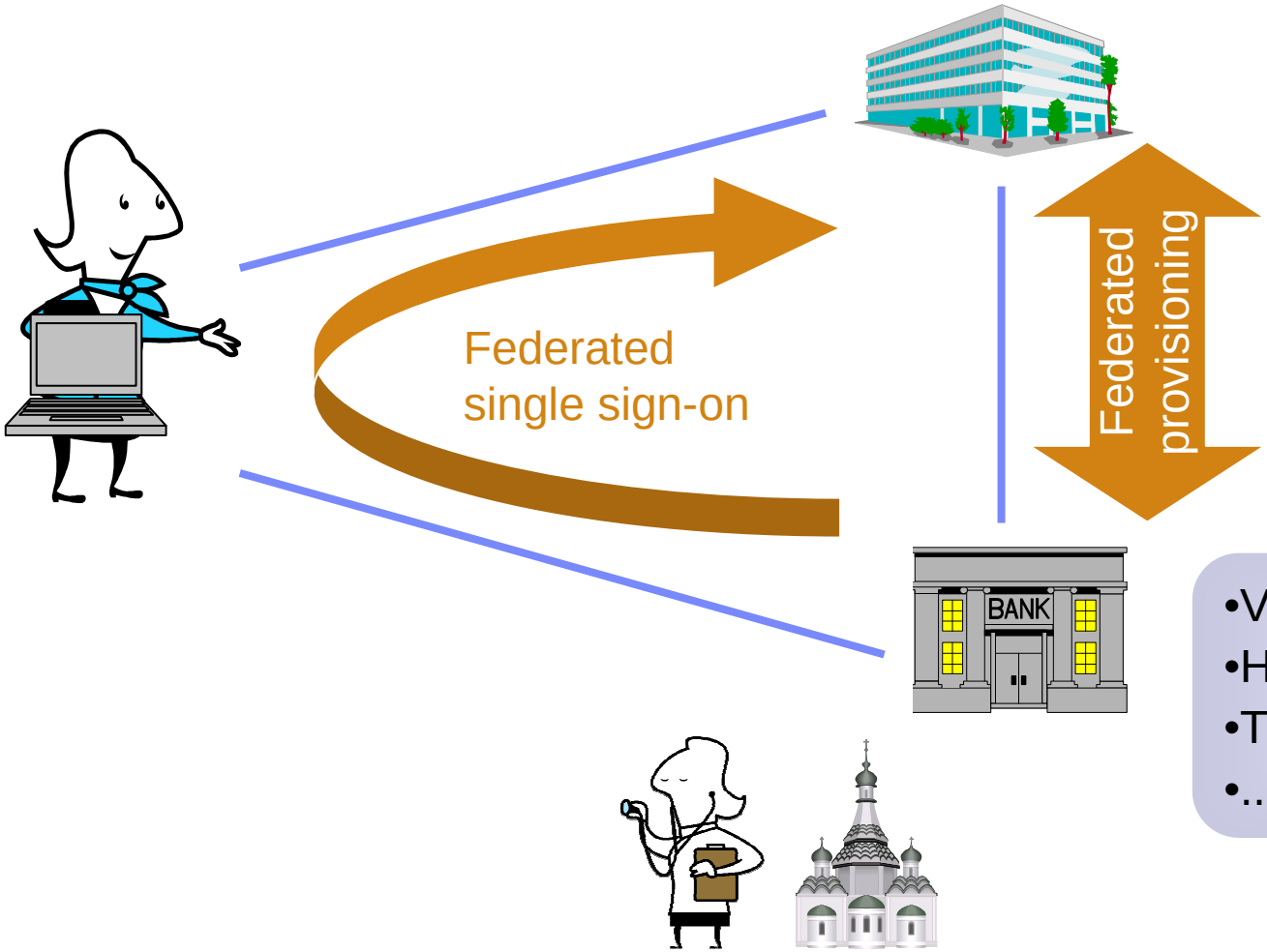
Business

- Efficiency
  - Consistent customer contacts
- Compliance
  - Privacy
  - Auditing, controls
  - Know-your-customer
- Federation
  - More flexible enterprise relationships

IT

- Efficiency
  - Password helpdesks
  - Consistent access rights
  - De-provisioning
- Federation
  - Easier updates in existing enterprise relationships

Federated Identity Management



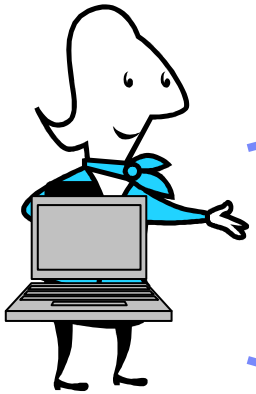
- Value-chain partner
- Health insurer
- Travel agent
- ...

What's New?

Scientifically

Standards

Management



Federated single sign-on

Federated provisioning

Nothing.
(Event-based directory integration)

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

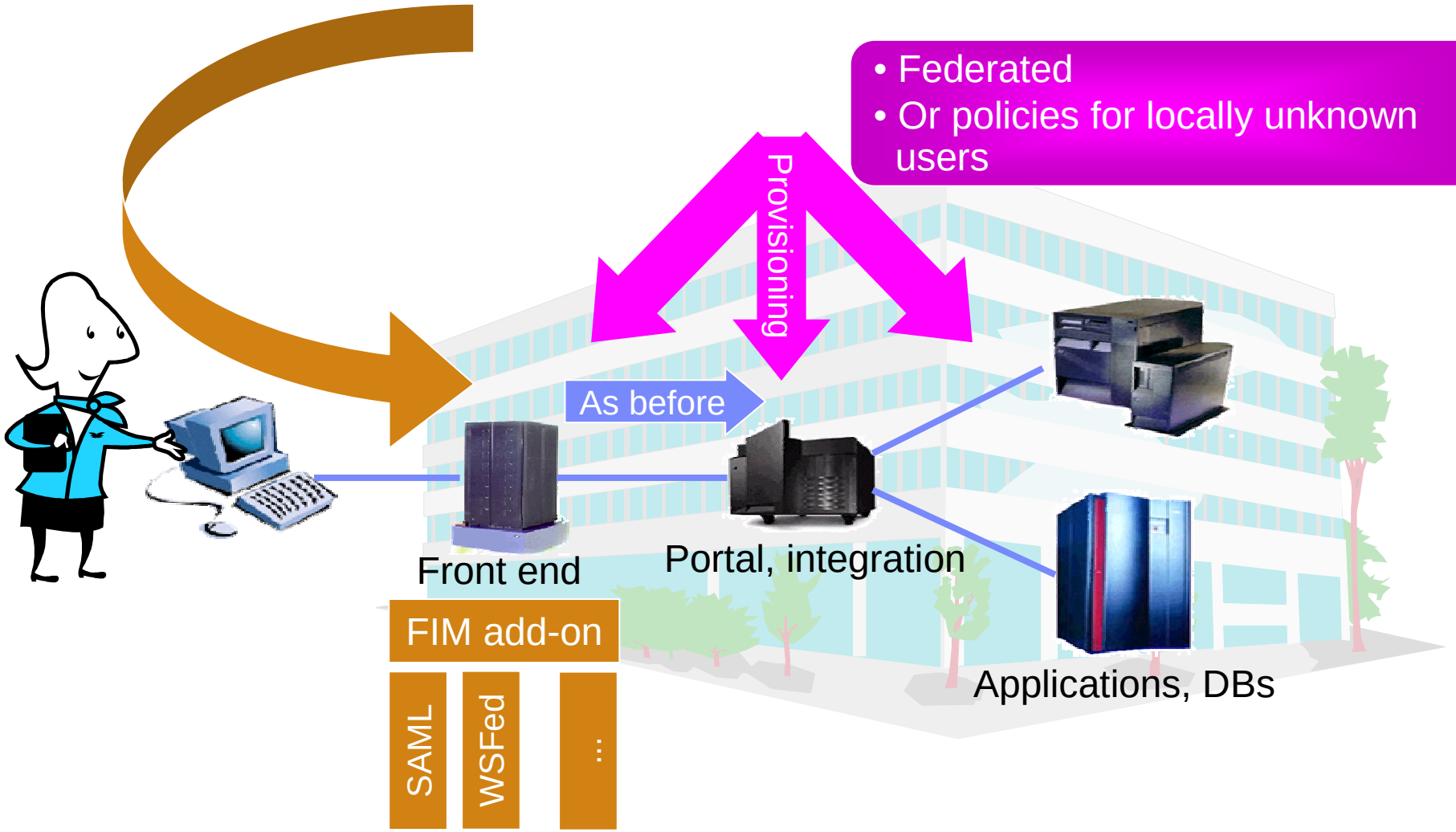
More liability and privacy issues

Pure browser case.
(Else 3-party authentication)

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

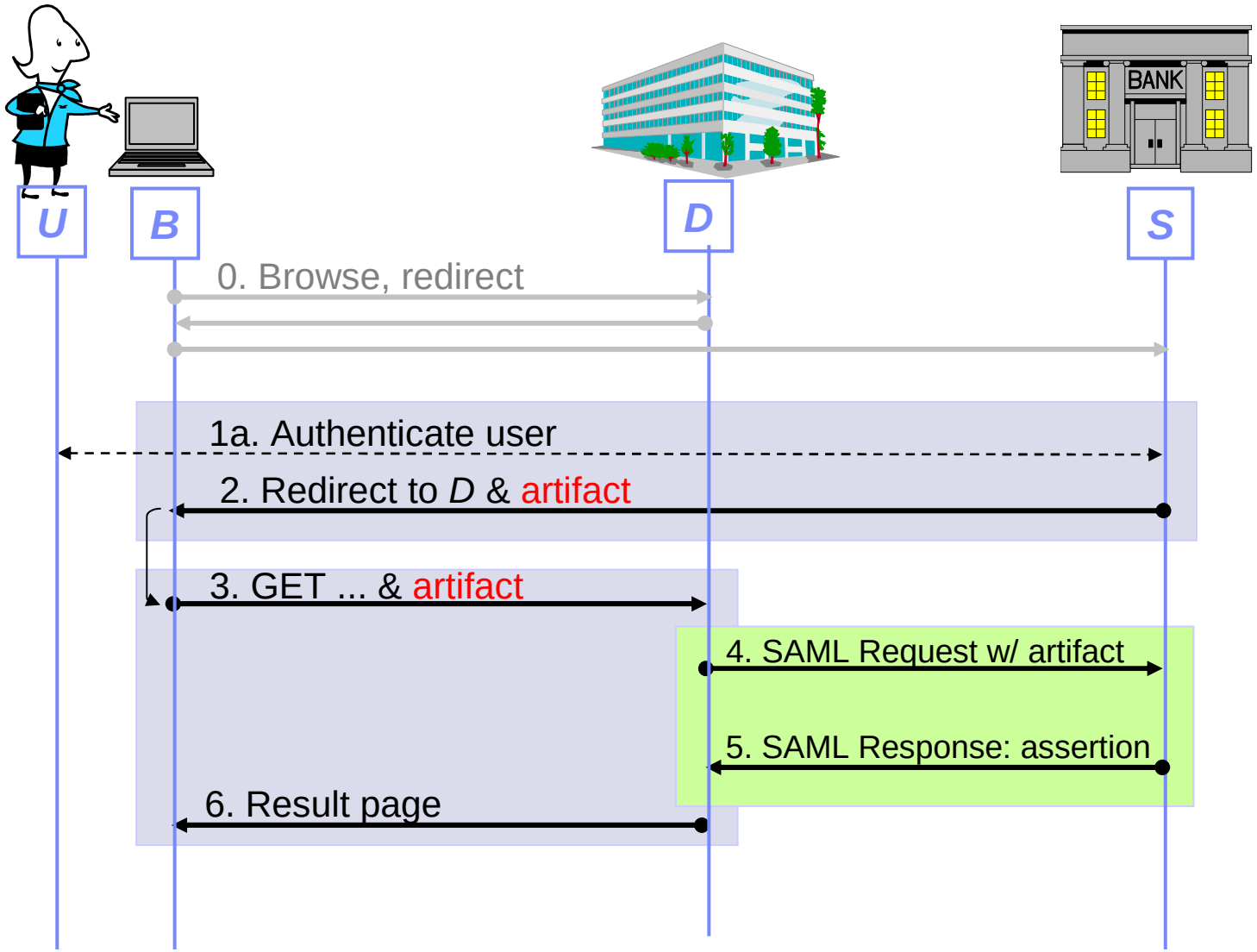
- More liability and privacy issues
- Metadata exchange

Integrating Federated SSO

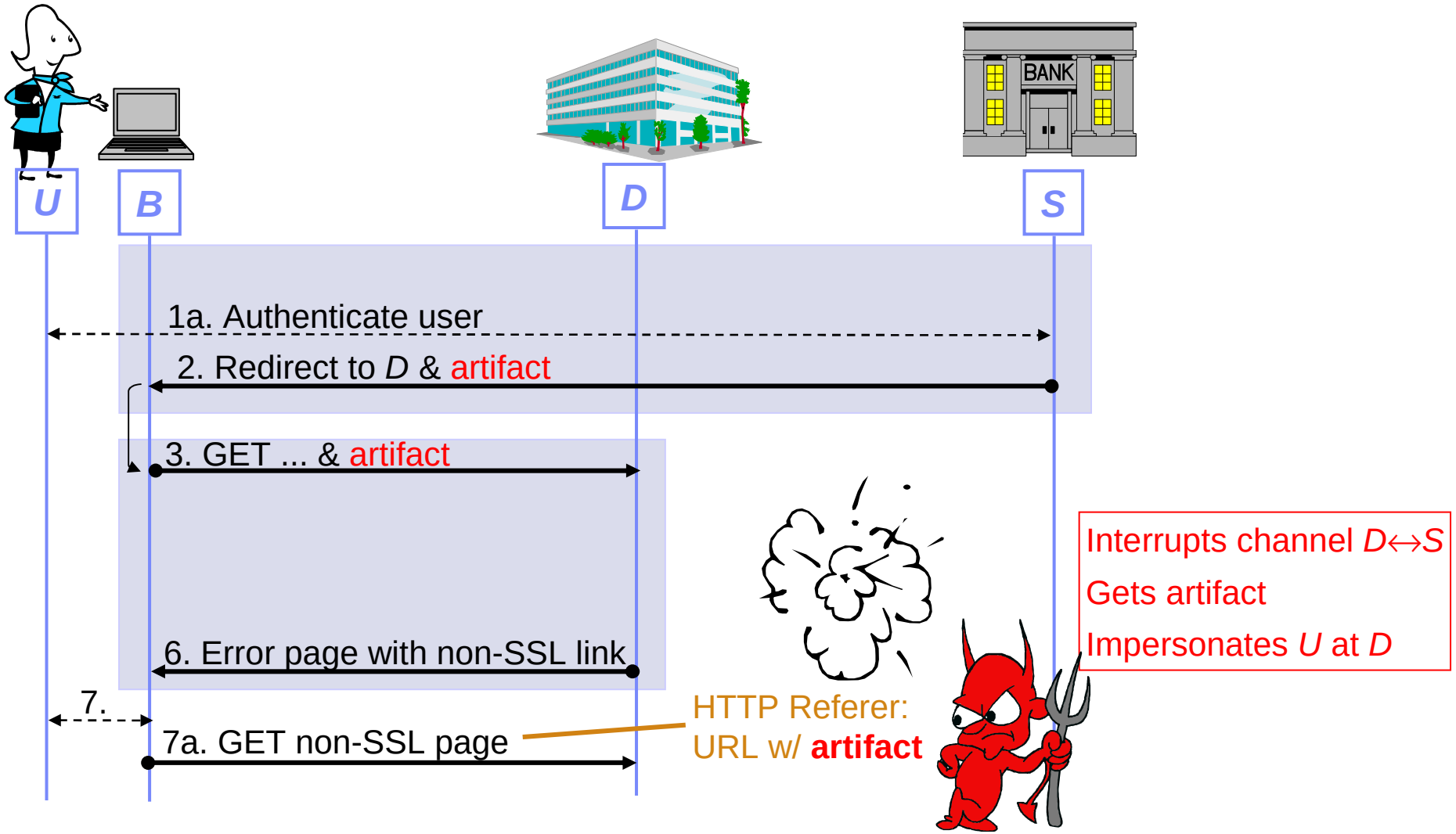


Security

SAML Artifact Profile



A Multi-Layer Vulnerability in SAML Artifact Profile



http://www.zurich.ibm.com/security/identities/#Gros1_03

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 02-05: 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”

Our Goal

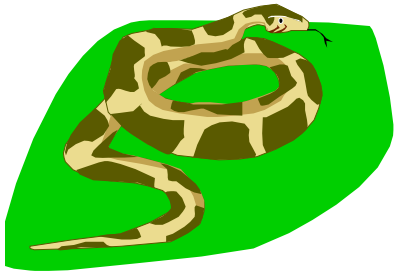
- Rigorous security statements of browser-based FIM protocols (mathematical proof)

Challenges for proving:

- Browsers and users
  - Browser as protocol party
    - Predefined protocol-unaware behavior
    - 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 instantiations

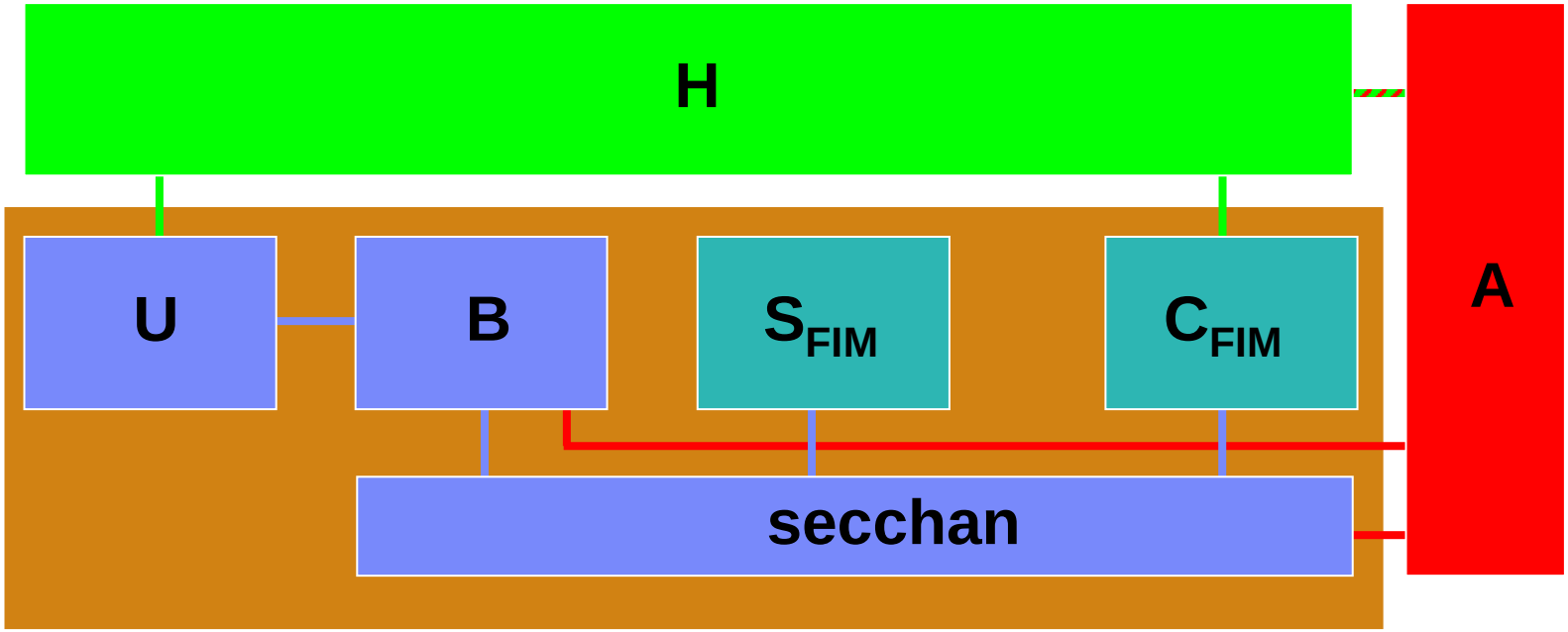
What Can We Hope to Prove?

- Vulnerable operational environment
  - Based on passwords
  - Fake-screen attacks easy
  - Browser security assumed
  - OS security assumed
- Identity supplier can impersonate user



We prove secure channel establishment
under appropriate operational assumptions

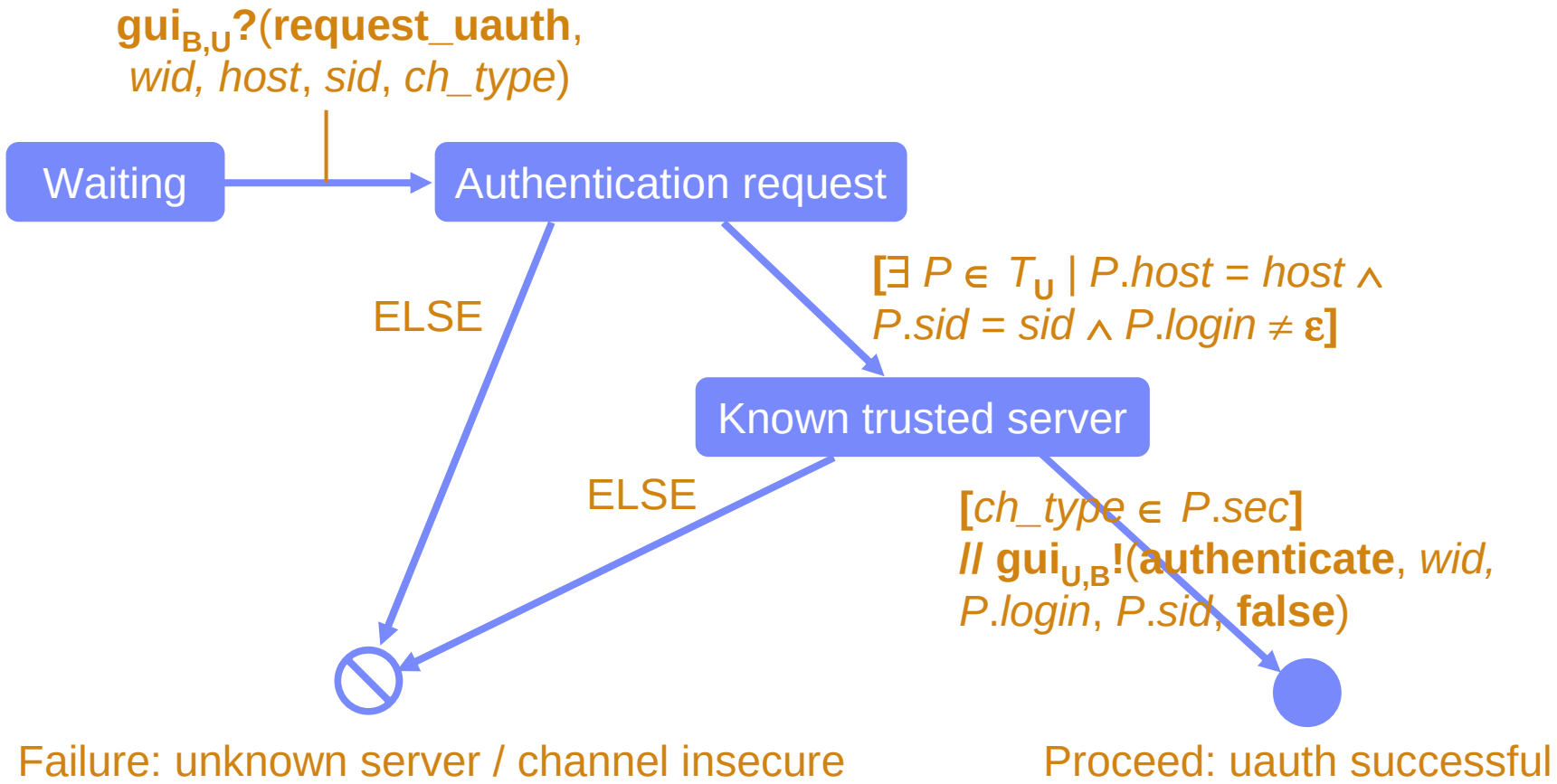
Big Picture: Proofs with Browser Model



Claim: Secure channels again

Part of the User Model for this Authentication

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

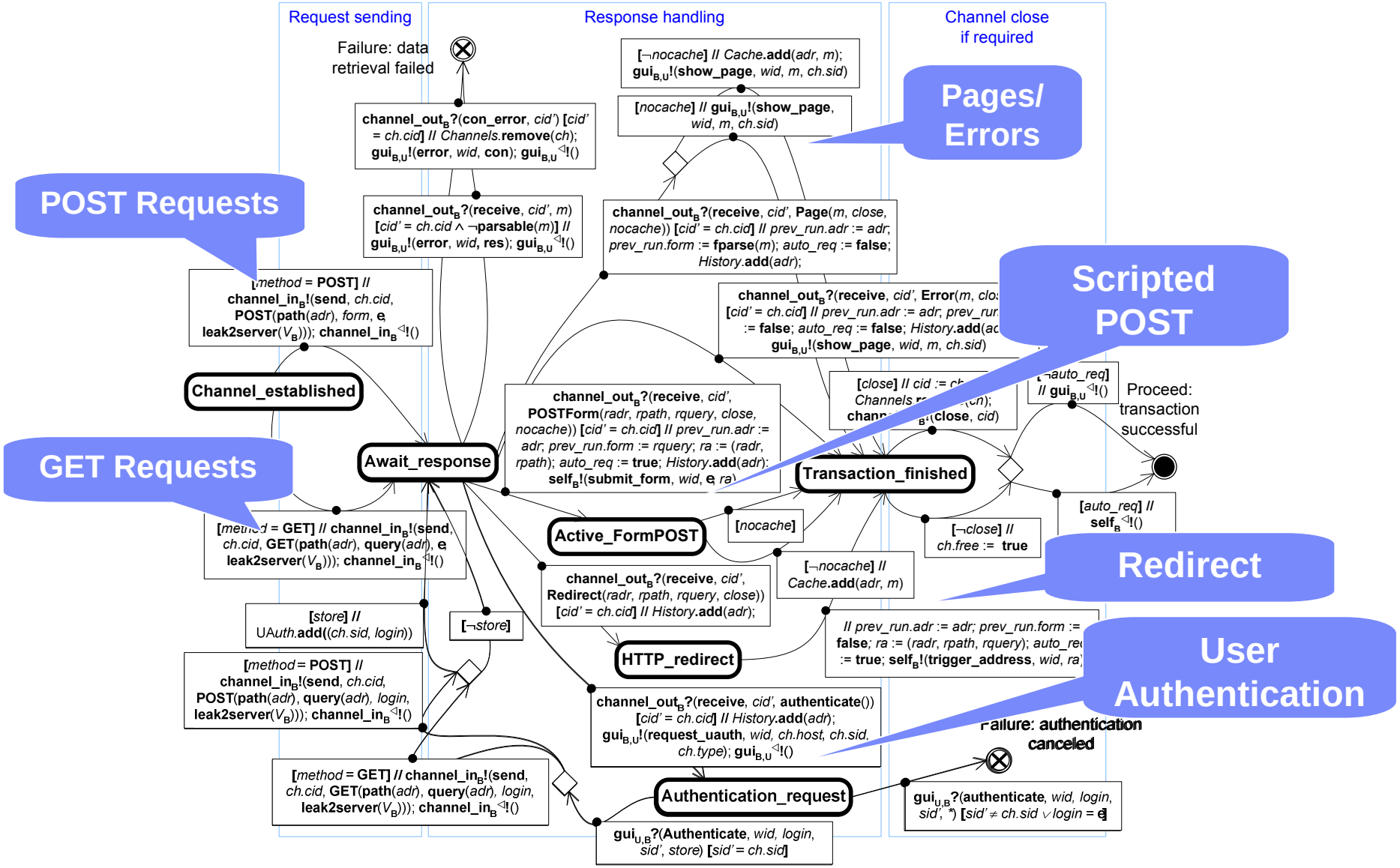


Crucial Aspects of the Browser Model

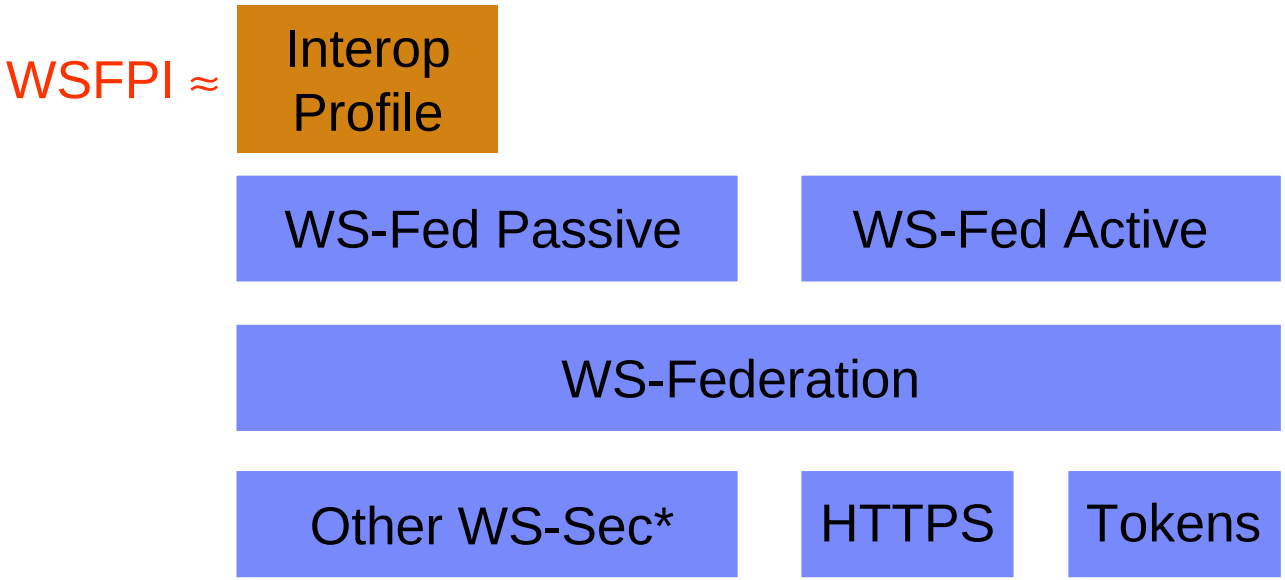
- Channel handling and main HTTP transactions
- User interaction
- Redirect and POSTform for 3-party protocols
- Leakage function, in particular Referer Tag
- Storage and loss of passwords, history, cache

- Proofs need assumptions that unmodeled information leakage really does not occur
  - Usable as future reference for what browsers should NOT do for use in browser-based protocols

Second half of B's state diagram for 1 HTTP transaction



The WSFPI Protocol – Basis for a Proof



Privacy

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 / pseudonyms

  Attribute = URL ⇒ Browsing behavior privacy

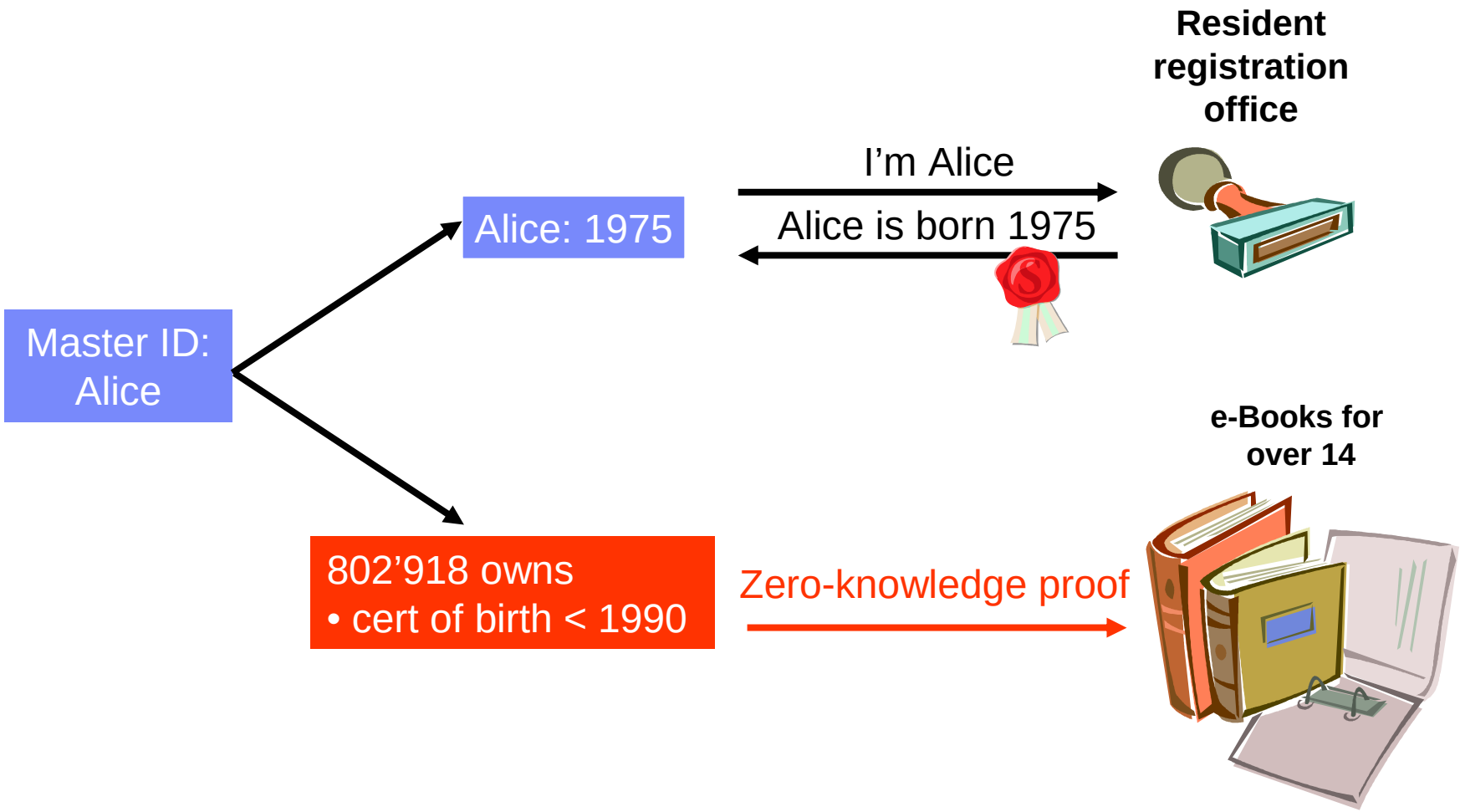
  O = identity supplier ⇒ Allow multiple suppliers, in particular local supplying

- Standards and middleware should allow maximum privacy, deployments should ensure appropriate privacy

Privacy Limits of “Normal” Federated Identity Management

- Privacy can get quite good, except
  - Not certified (role) attributes with anonymity
  - Identity supplier learns destination site trail (for redirections)

idemix – Anonymous Role-based Access



http://www.zurich.ibm.com/security/idemix

Used by TCG TPM 1.2, EU PRIME

Scheduled applications of idemix

- Direct Anonymous Attestation

  Trusted Computing Group TCG
  TPM 1.2 Specification

- EU IST Prime, “Privacy and Identity Management for Europe”

  Base technology

Summary

Summary and Outlook

- Identity management is major issue
  - Drivers: compliance, efficiency, and federation (web-based or web services)
- Browser-based FIM protocols are at least as error-prone as other security protocols
- Protocol-unawareness as major new challenge
- Addressed by detailed browser and user model; proofs now possible
- Privacy can be quite good, but needs care in protocol design and deployment
  - Fat-client cryptographic FIM can go one step further

For more information …

- How to reach me

  Birgit Pfitzmann <bpf@zurich.ibm.com>

  http://www.zurich.ibm.com/~bpf

- IBM Research

  IBM Zurich Research Lab:

  http://www.zurich.ibm.com

  Federated Identities at IBM Zurich Research Lab:

  http://www.zurich.ibm.com/security/identities/

  Security research at IBM Zurich :

  http://www.research.ibm.com/compsci/security