IBM Zurich Research Lab

Privacy in Enterprise Identity Federation
- Policies for Liberty Single Signon -

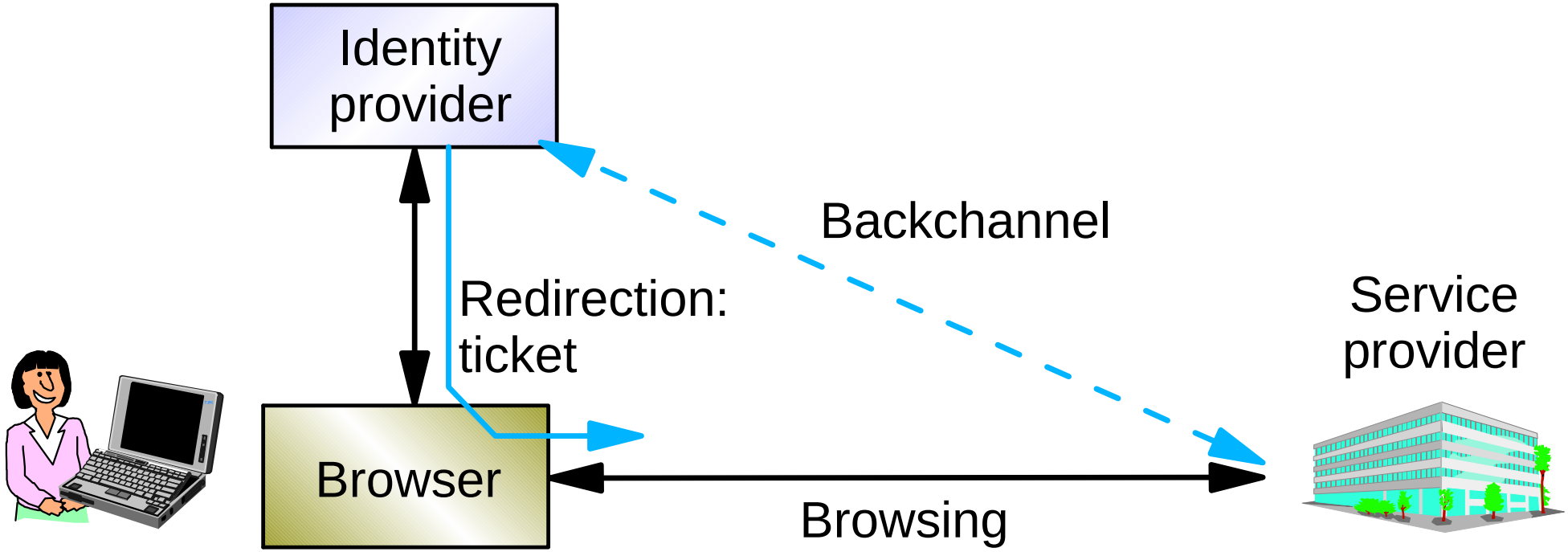
Birgit Pfitzmann

Content

- Privacy options in the design space of Passport, Liberty, etc.

- Exact policies for a single-signon protocol with claimed privacy

Enterprise Identity Federation
Browser-based Attribute Exchange

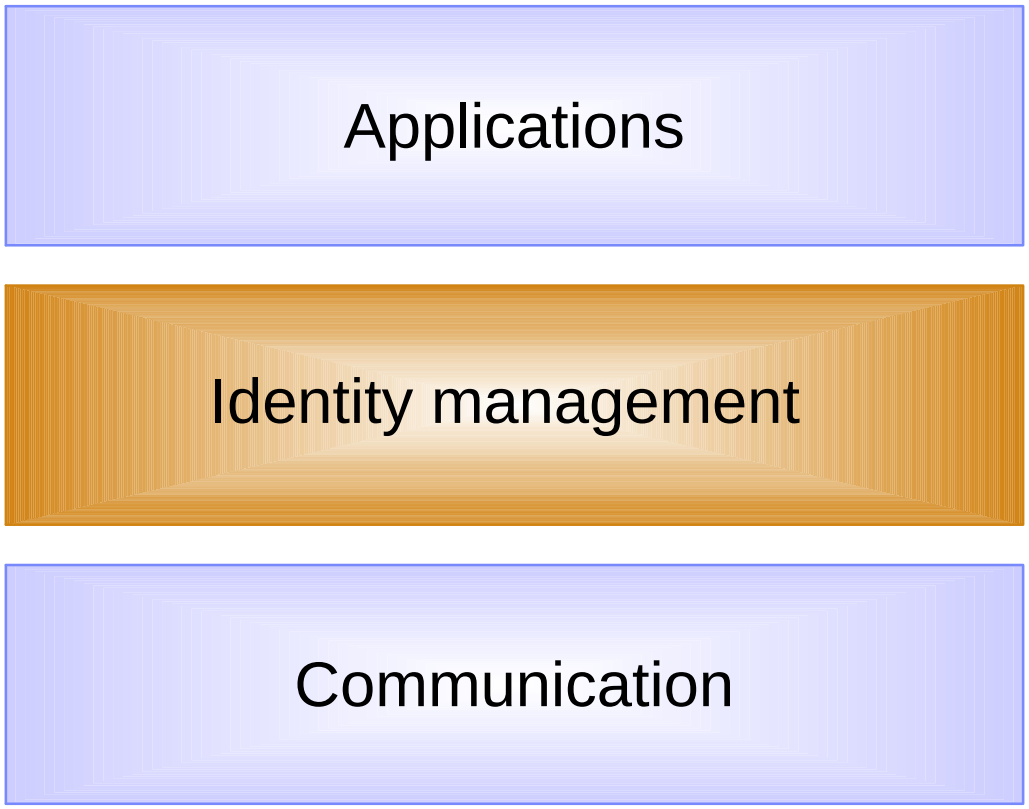


Zero-footprint

Why Should You Care?
— Version for Strong Privacy Supporters

- Such protocols may become prevelant
- For some situations they can offer strong privacy
- But that needs care
- Their interfaces may be the integration points for anything stronger

What Do They Compete With?



- In-enterprise
- B2B (supply chain, bonus miles)
- Shopping

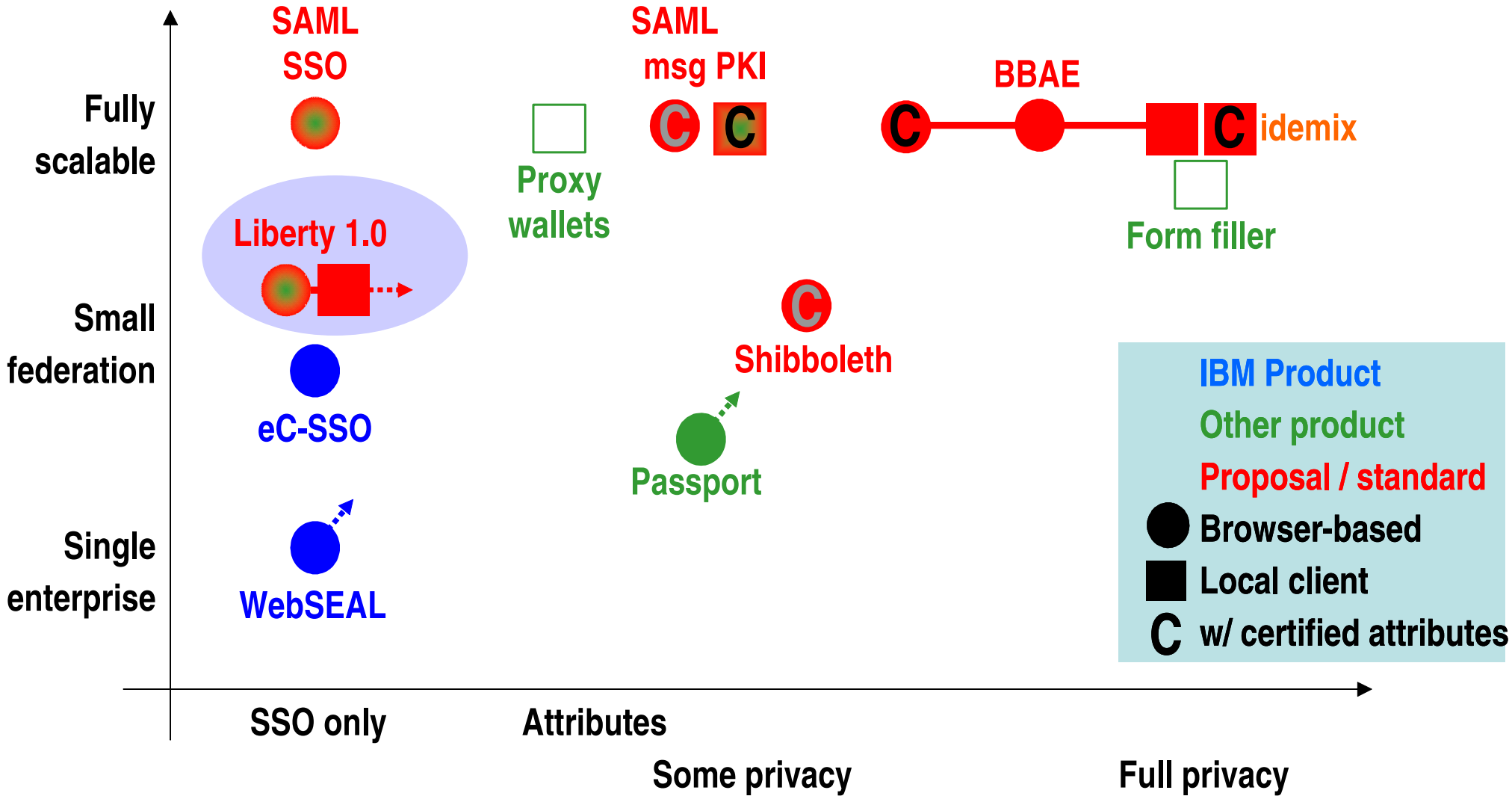
- Form filling
- Database join
- PKI
- Cryptographic credentials

- HTTP
- Mixes

Why Should You Care?
— Version for Enterprises

- Lack of trust major inhibitor for e-commerce
- Market analyses about Passport (2001/02)
  - Very wary of "putting all eggs in one basket"
  - 80-90% concerned about privacy; about 25% at considerable inconvenience
  - Surveys give no party average trust of 5 on 1-7 scale for address and credit-card info
  - Only 2% of (real) Passport users because they like it
- People may be forced to use attribute-exchange standard

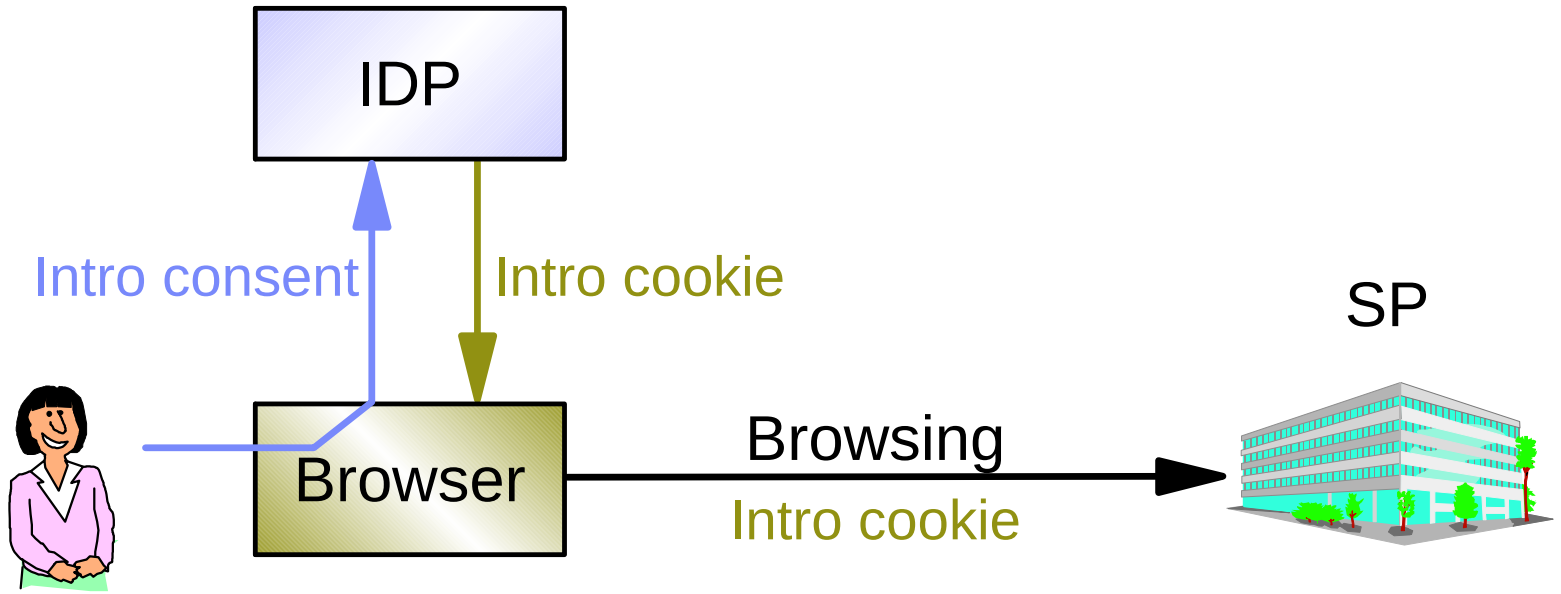
Existing Proposals



Why Look Specially at Liberty SSO?

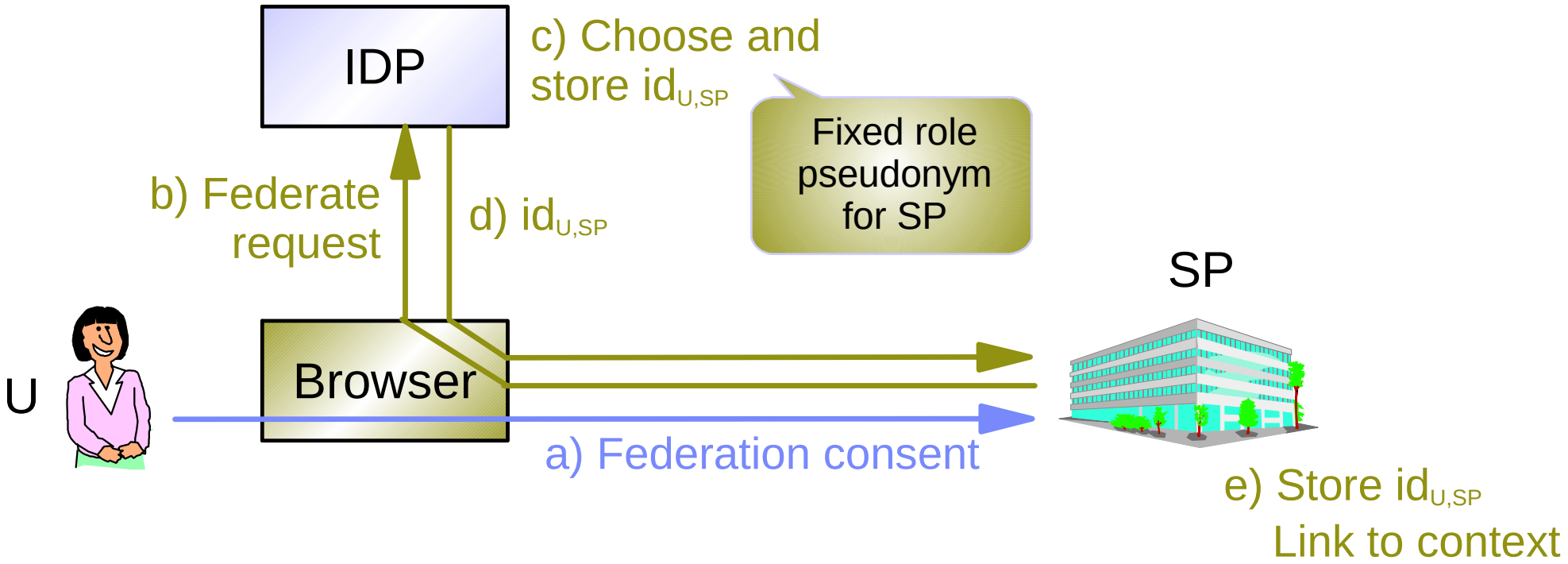
- Goal: Try out policies concretely
- Single signon should be the simplest case
  - Only one type of attributes
  - Seems to have concrete privacy policy with few options
- Liberty SSO contains privacy features
  - Pseudonyms
  - Everything voluntary
  - (Much more than Passport or proxy pseudonym servers)

Data in Liberty SSO - 1. Introduction data



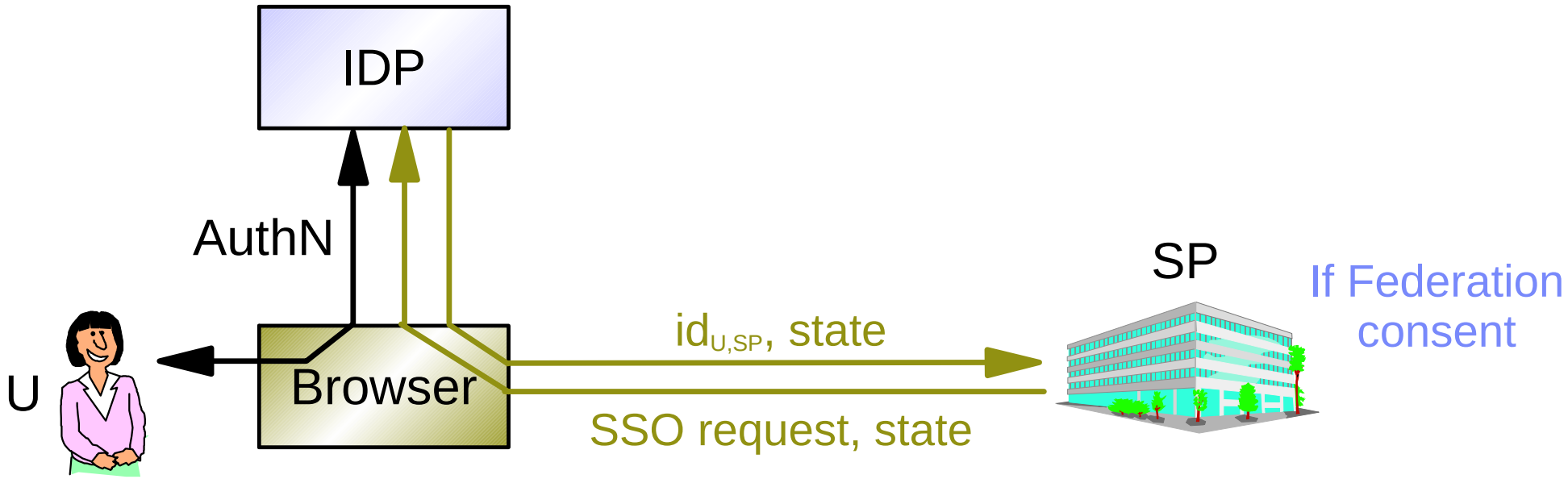
- Preferred rule (refined)
  - Cookie states id_{IDP}; not login state
  - May be sent to everyone (mainly: also future federation members)
  - No other use of common domain

Data in Liberty SSO - 2. Federation



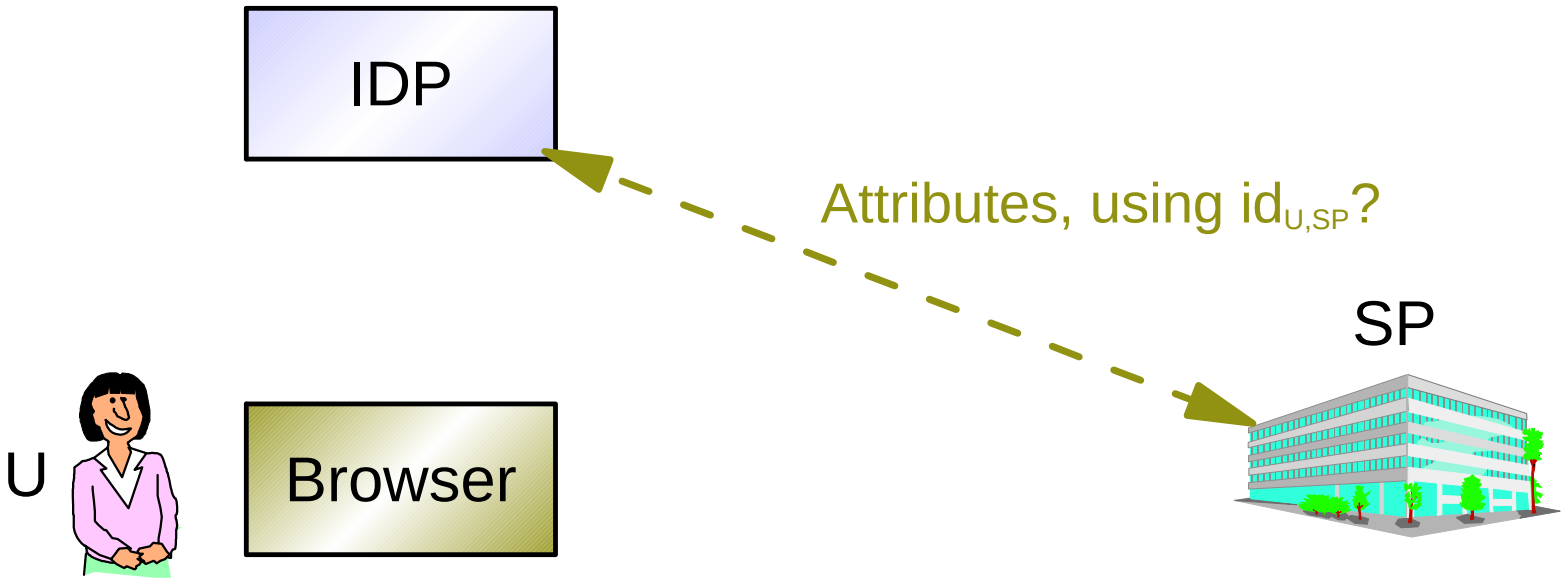
- Preferred rule:
  - SP: Only if federation consent at SP
  - IDP: Only if federation consent for this SP at IDP (new, to fulfil claims)

Data in Liberty SSO - 3. Single Signon (SSO)



- Preferred rule:
  - SP: If federation consent unknown, get SSO consent (new, to fulfil claims)
  - SP: Only random "state" (new)
  - Store transcripts only if required (refined)

Data in Liberty SSO - 4. Attributes?



- Very unclear. Proposed rule:
  - Only IDP → SP
  - Only if explicit agreement to privacy policy, and easily avoidable

Other Aspects

- Termination: Essentially already possible
- Notification, access rights: Mostly inherent
- Retention, disputes, assurance: Should get minimum standards

What Changes with Attribute-Exchange?

- Real-time release possible
- Multiple roles possible
- User choices can be bundled differently

More Information

- Passport security: Korman/Rubin 2001, Slemko 2001
- Liberty security: Pfitzmann/Waidner: Token-based Web SSO ...(Report)
- Overall view of privacy options: PW, ACM WPES 2002
- Detailed privacy-protecting protocol BBAE: PW, Cambridge Security Protocols 2003
- Our preprints: http://www.zurich.ibm.com/security/publications/

Summary

- Browser-based attribute exchange may become almost mandatory
- Important: Privacy, security, no control point
- Limits
  - Operational security
  - Not certified attributes + unlinkability; then idemix
- Enterprises may choose single signon + separate attribute transfer
  - Cannot completely circumvent policy problem
  - Even single-signon policies not trivial
  - One pseudonym per partner often not best choice