Claim-based versus network-based identity management: a hybrid approach

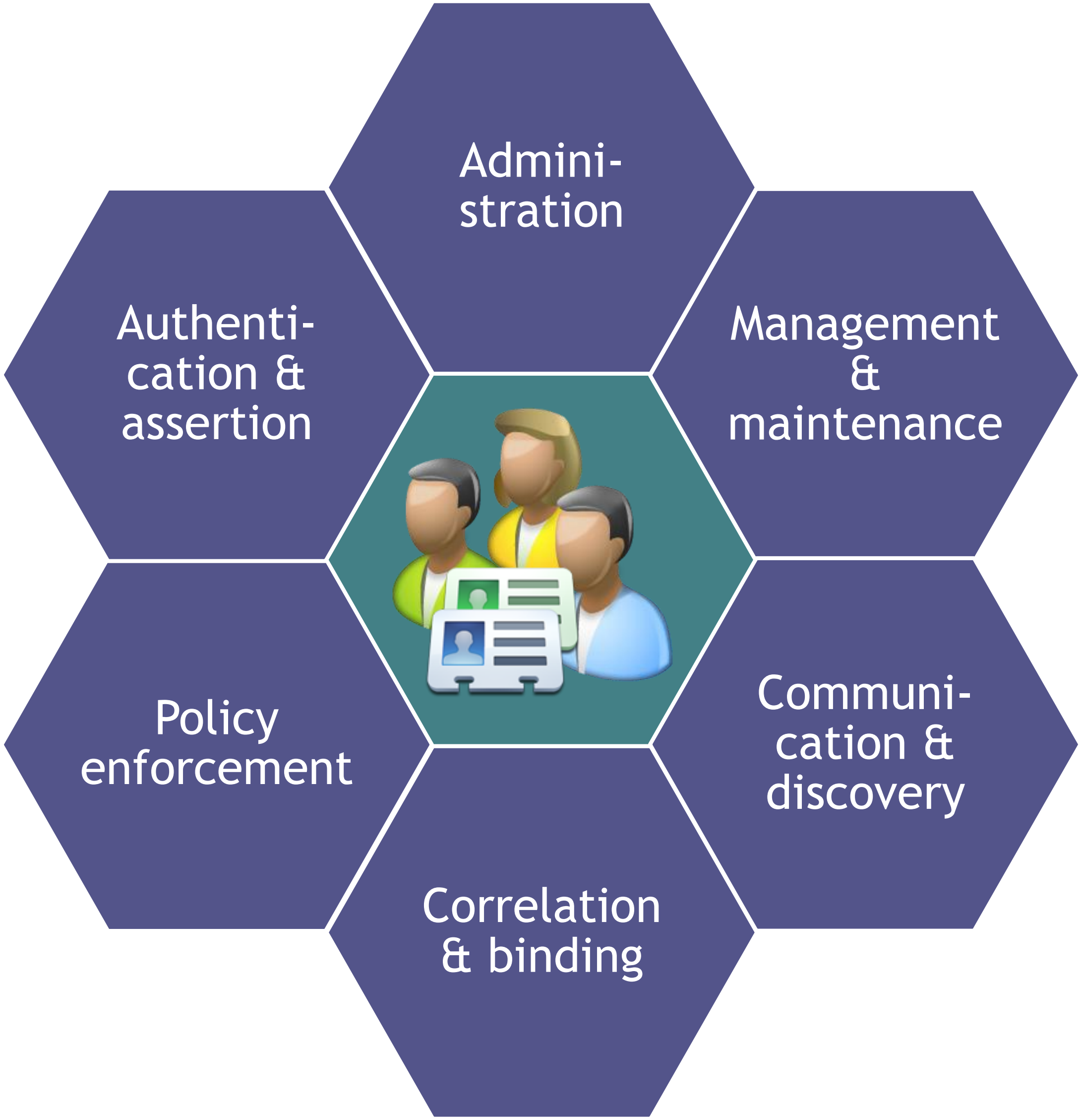
Faysal Boukayoua
MSEC research group
KaHo Sint-Lieven, Ghent

MOBISEC, Frankfurt am Main
June 25-26, 2012

Overview

- Introduction
- Motivation
- Architecture
- Prototype
- Evaluation
- Future work

Introduction: identity management



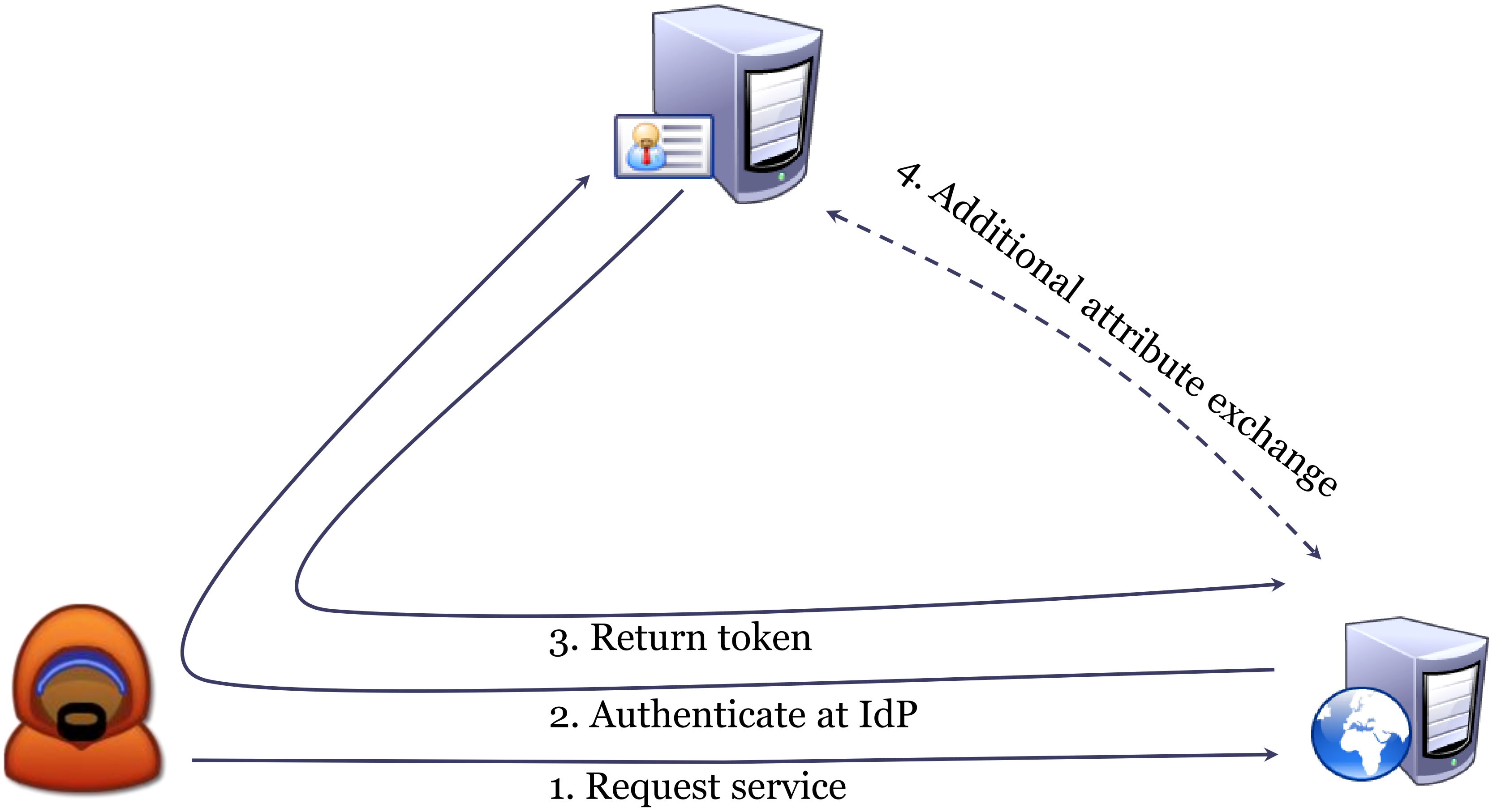
Goals:

- Identity assurance
- Enable business & security applications

Loosely based on the *ITU Y.2720* standard

Based on *The Identity Crisis: Security, Privacy and Usability Issues in Identity Management* (Alpár et al)

Introduction: network-based identity management



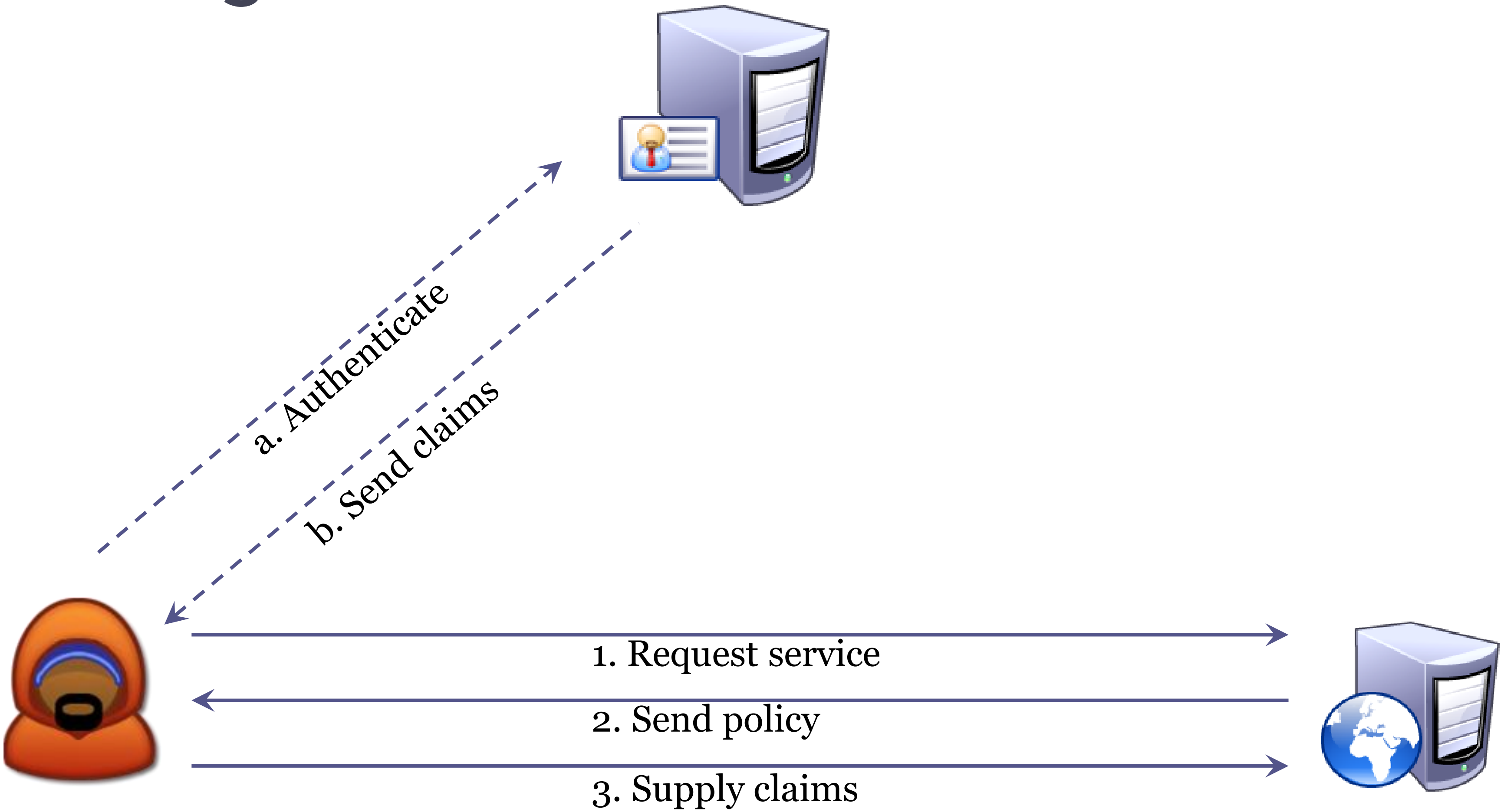
Introduction: network-based identity management

Examples

- Password-based Shibboleth
- Password-based OpenID
- Google ClientLogin

Based on *The Identity Crisis: Security, Privacy and Usability Issues in Identity Management* (Alpár et al)

Introduction: claim-based identity management



Introduction: claim-based identity management

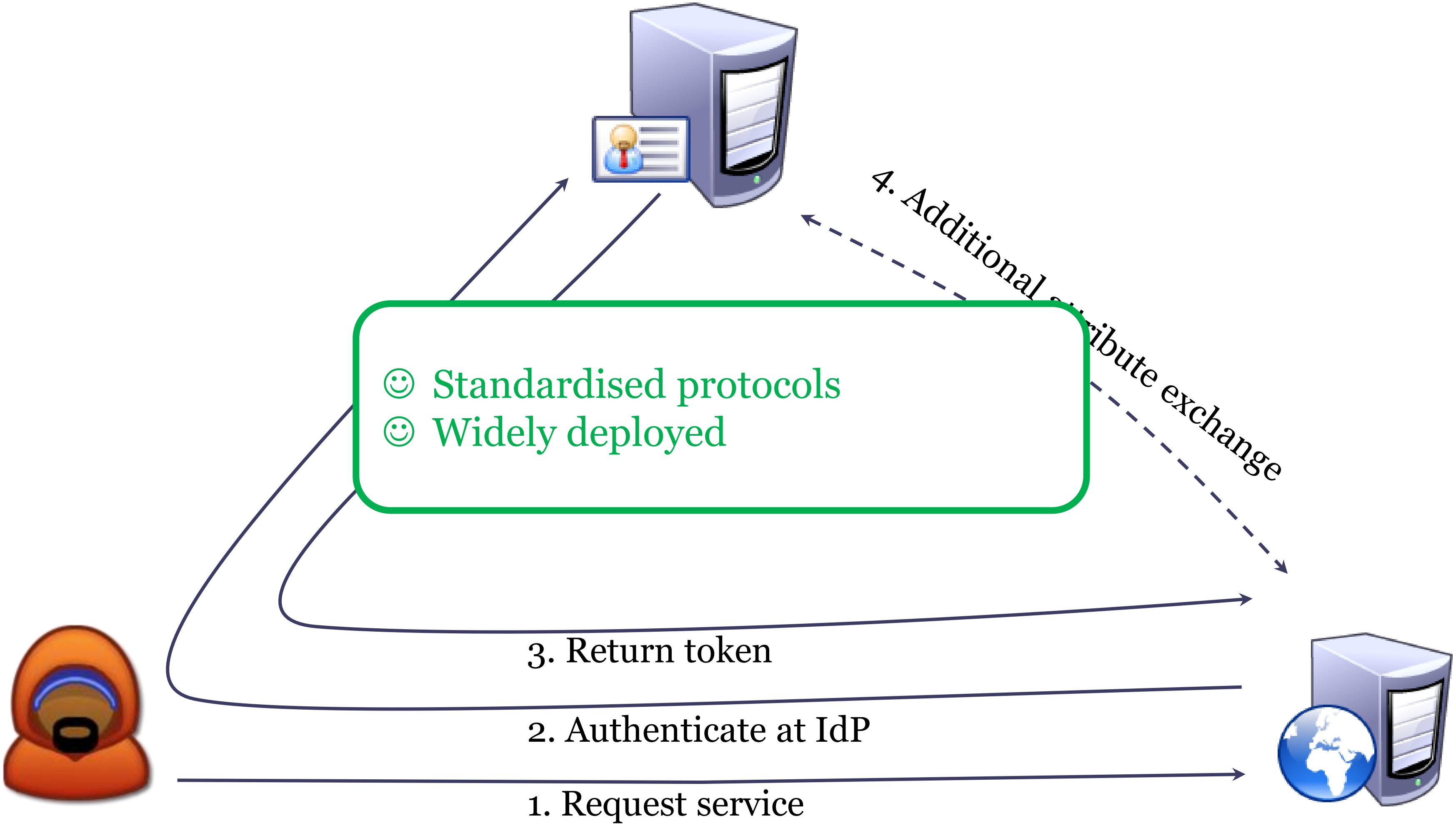
Examples

- eID technology
- Anonymous credential systems
- Standalone X509 certificates

Introduction: hybrid examples

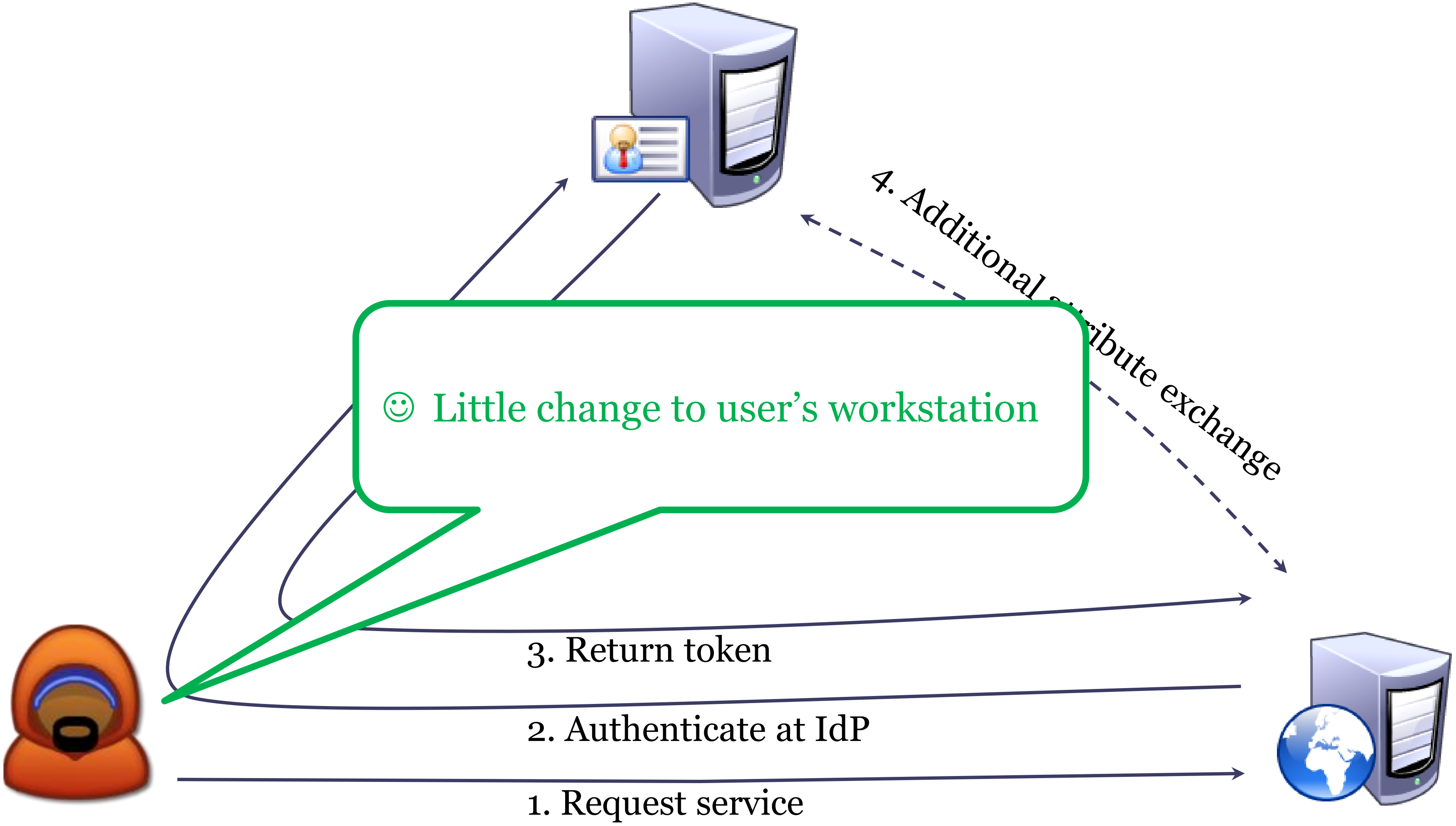
- SAML authentication context classes:
  - Smartcard PKI
  - MobileTwofactorContract
  - …
- Shibboleth and OpenID with alternative authentication
- eID authentication portals

Motivation: network-based IdM



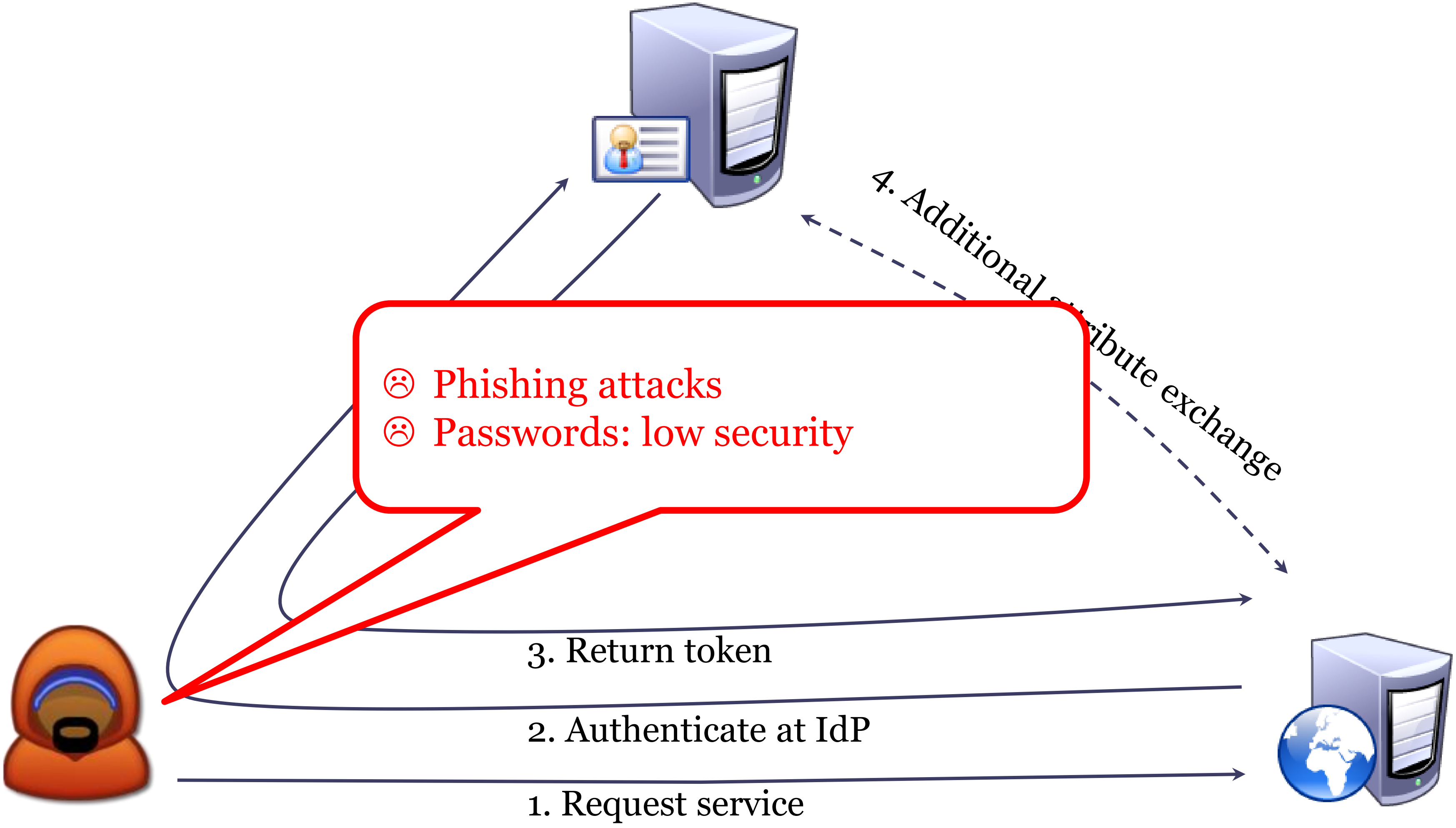
- ☺ Standardised protocols
- ☺ Widely deployed

Motivation: network-based IdM



☺ Little change to user’s workstation

Motivation: network-based IdM



☹ Phishing attacks
☹ Passwords: low security

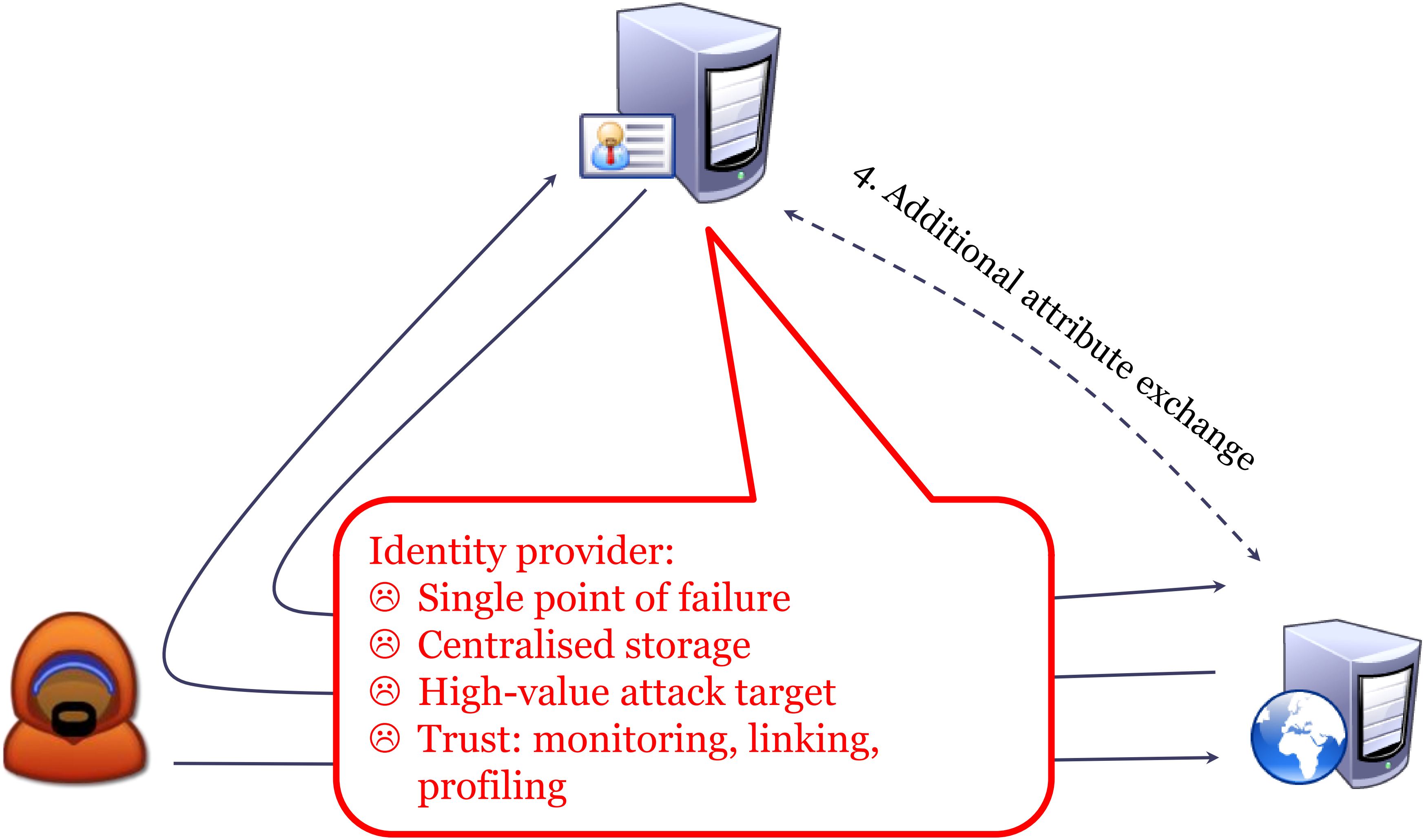
4. Additional attribute exchange

3. Return token

2. Authenticate at IdP

1. Request service

Motivation: network-based IdM



Identity provider:

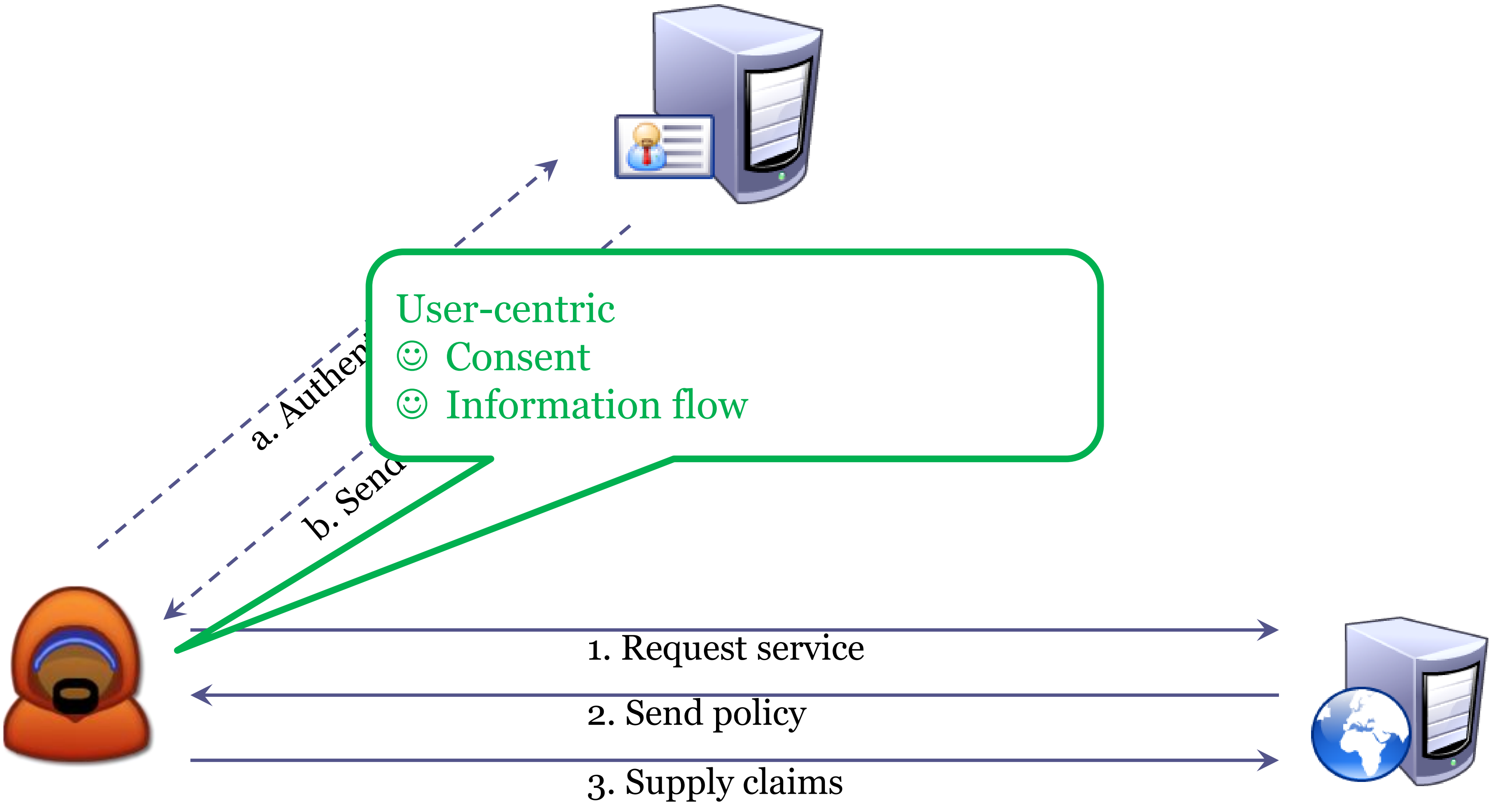
☹ Single point of failure

☹ Centralised storage

☹ High-value attack target

☹ Trust: monitoring, linking, profiling

Motivation: claim-based IdM

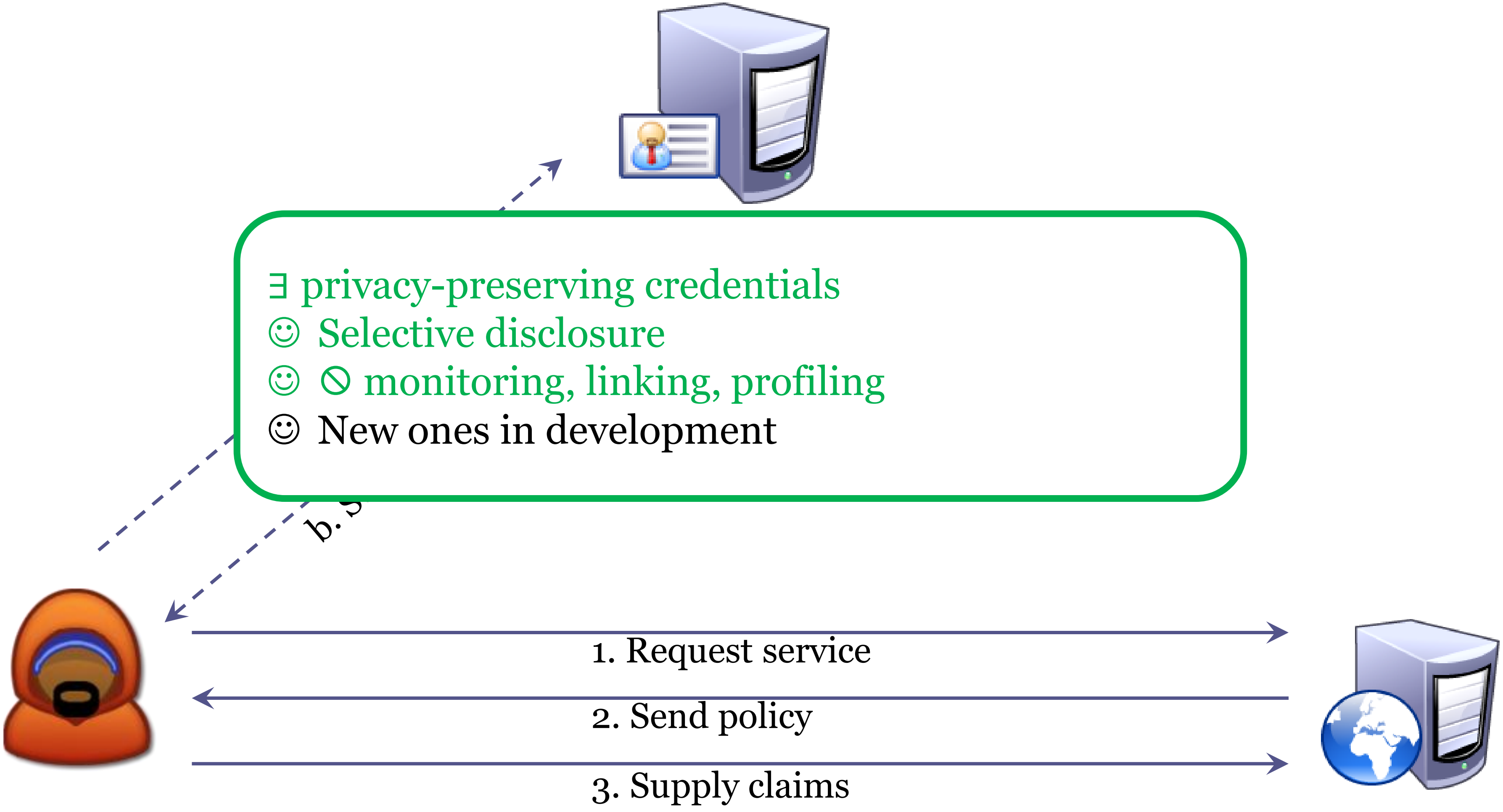


User-centric

☺ Consent

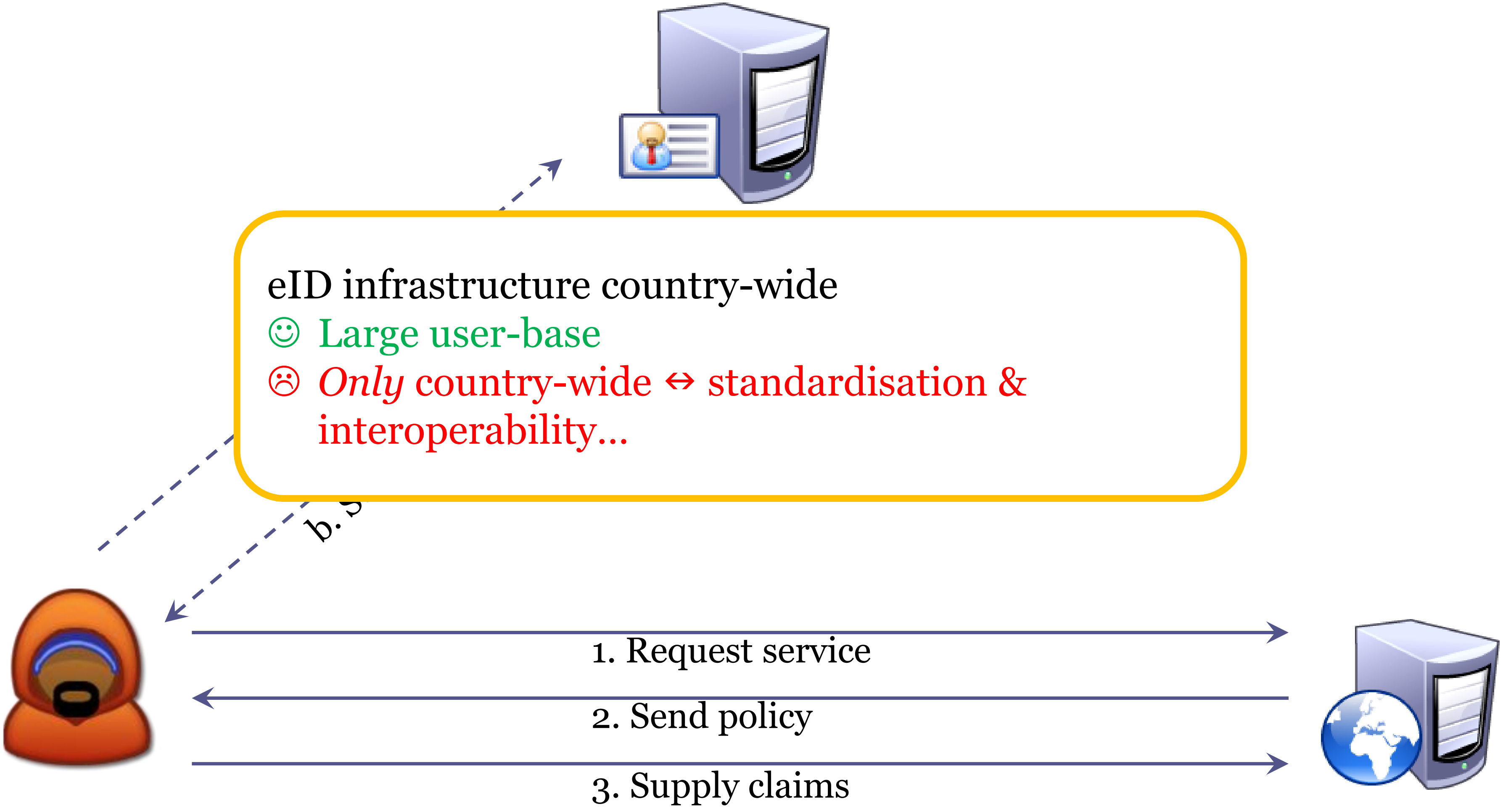
☺ Information flow

Motivation: claim-based IdM



∃ privacy-preserving credentials
☺ Selective disclosure
☺ ⦸ monitoring, linking, profiling
☺ New ones in development

Motivation: claim-based IdM



eID infrastructure country-wide

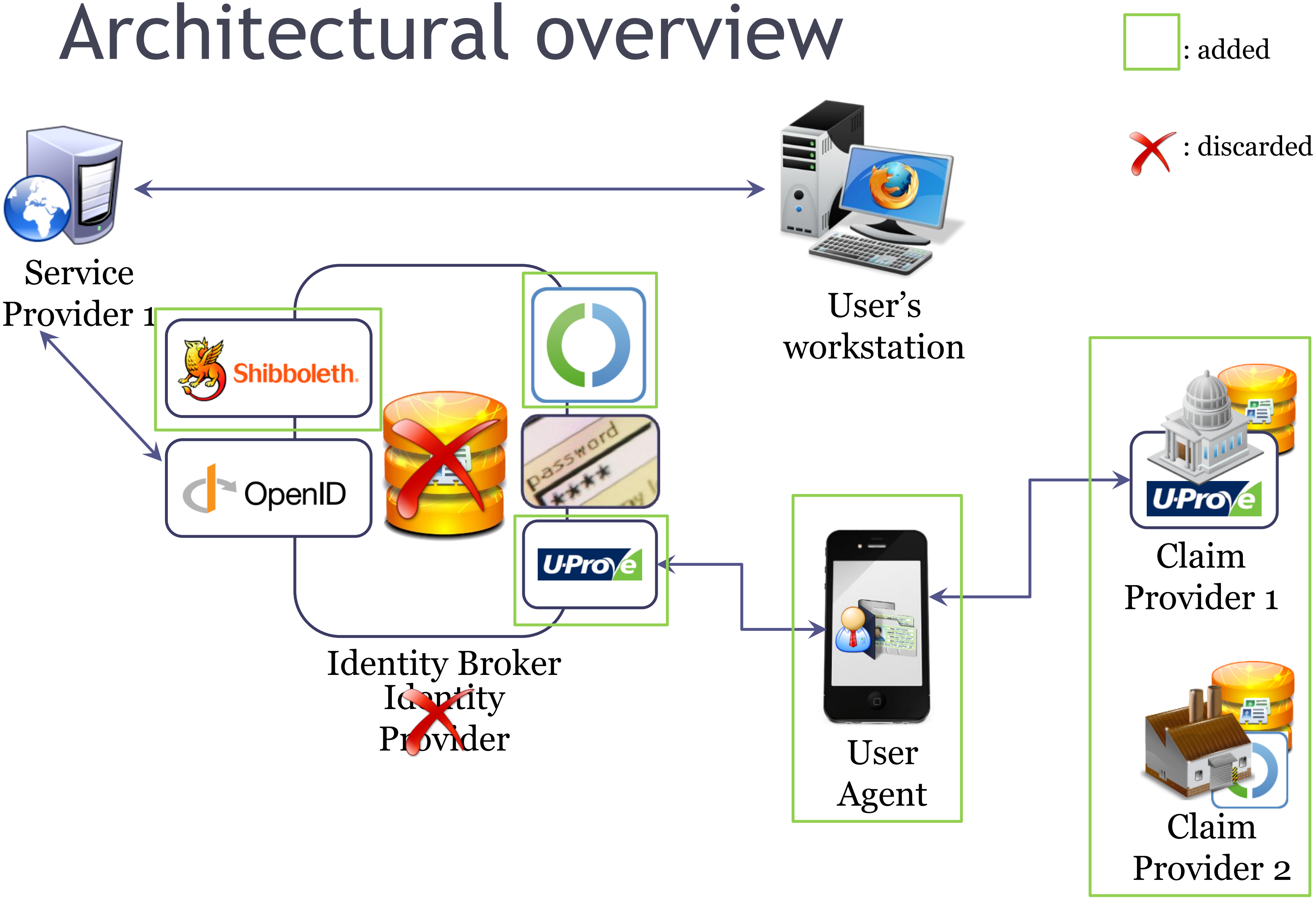
☺ Large user-base

☹ *Only* country-wide ↔ standardisation & interoperability…

Motivation: other considerations

- Service provider
  - Reliable user info
  - Broaden user base
  - Externalise IdM cost
- User
  - Easily switch to other claim-based technologies
  - Use credentials across services

Architectural overview



Architecture: service provider

- Unmodified at protocol level
- Minor configuration required
  - Prerequisite exchange (=required user attributes)
  - @ trust establishment logic

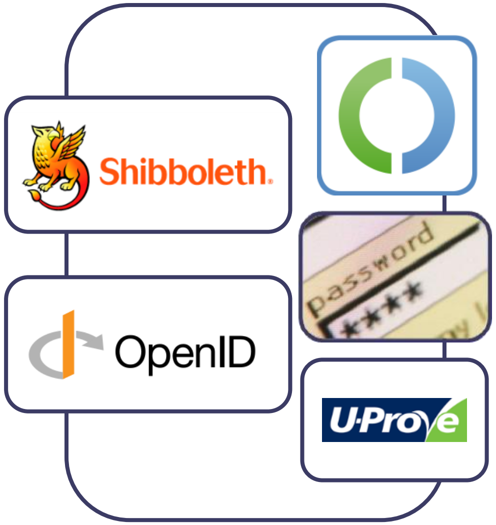
Architecture: claim provider

- Claim issuance
- Storage of partial identities
- Multiple providers
- ∃ privacy-preserving credentials

Architecture: user agent

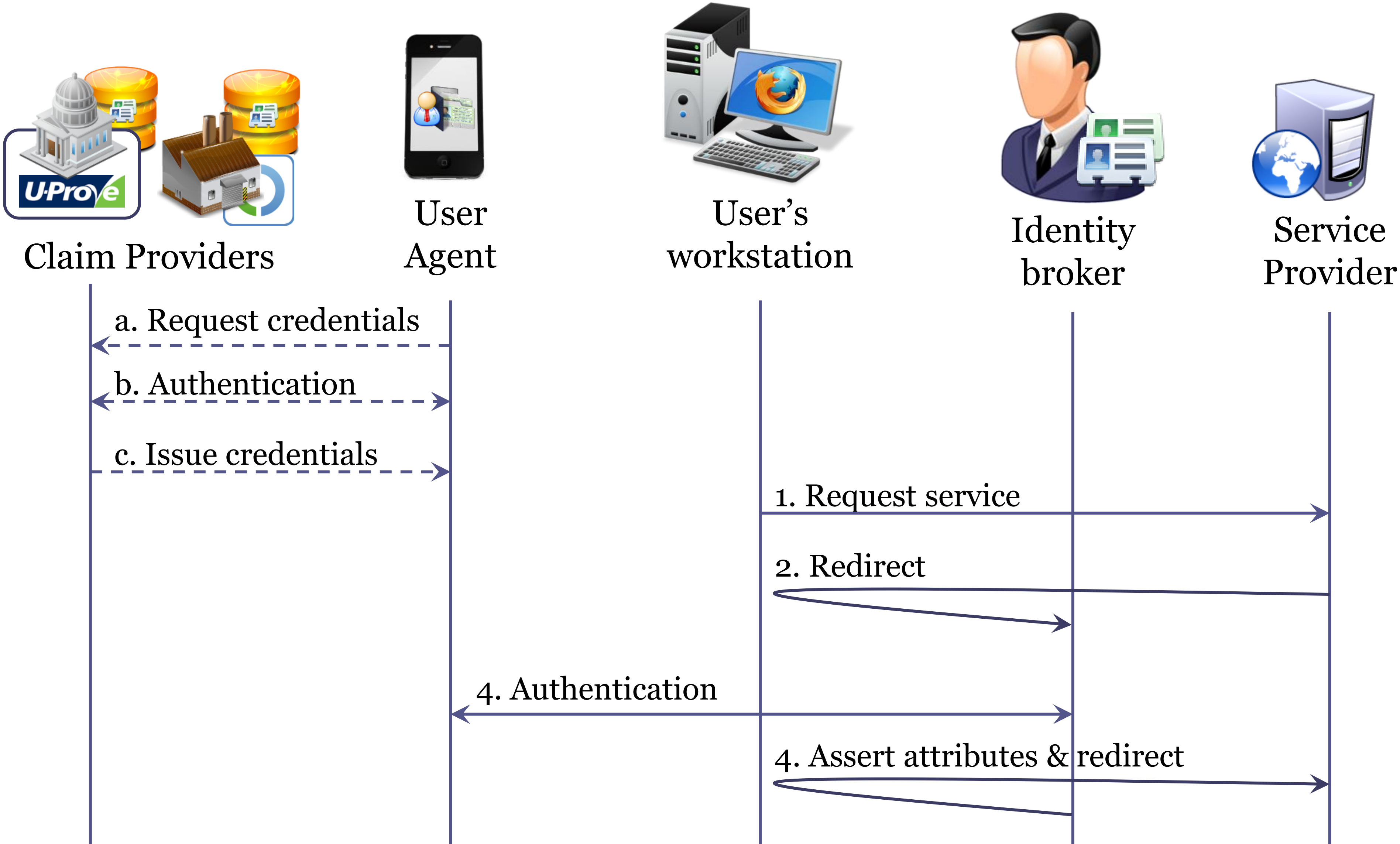
- Present claims to identity broker
- Claims management
- User feedback & consent
- Automated policies
- Phishing protection
- Various support functions
- …

Architecture: identity broker

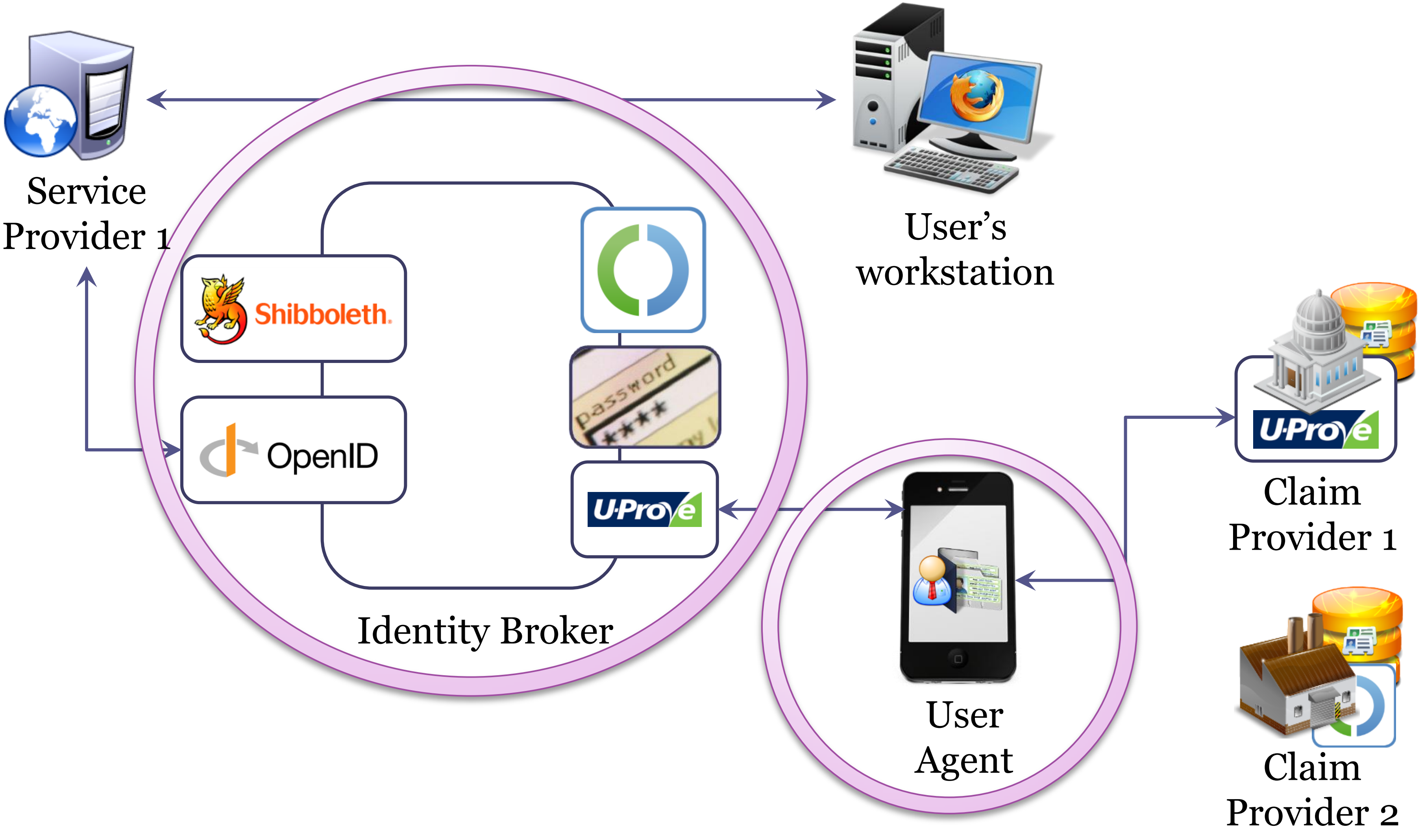


- Support claim technologies
- Authentication & assertion to service provider
- No attribute storage
  - No storage-related user dependence ➔ generic functionality
- Privacy-preserving claim technologies
  - 🛇 monitoring, linking, profiling

Architecture: message flow



Prototype



Service Provider 1

User's workstation

Identity Broker

User Agent

Claim Provider 1

Claim Provider 2

Prototype: user agent

- Samsung Galaxy S
- Android 2.3.4
- Tamperproof storage: *Giesecke & Devrient Mobile Security Card*
- 2 setups:
  - Service accessed on smartphone
  - Out-of-band authentication

Prototype: identity broker

- Claim technologies:
  - Idemix
  - Proof-of-concept IdM architecture
- Authentication & attribute assertion protocol:
  - Shibboleth
  - Service provider prerequisites in SAML metadata
  - (others in progress)

Evaluation

IdP:	identity provider
IdB:	identity broker
SP:	service provider

	Compared to network-based IdM	Compared to claim-based IdM
Phishing	• Feedback on user agent • IdB configured in user agent	Feedback on user agent
IdP • Single point of failure • High-value attack target	• Multiple IdBs (generic task) • User can select IdB • IdB stores no data	n/a (many issuers)
Interoperability	• SP protocol unchanged • Harness claim-based credentials	• Credential use across services
	• SP: broader user base at little cost • User: more services with same credentials	

Evaluation

IdP:	identity provider
IdB:	identity broker
SP:	service provider

	Compared to network-based IdM	**Compared to claim-based IdM**
User consent	User consent on user agent for each transaction	
Transaction monitoring, linking, profiling	• Multiple IdBs • Leveraging: • Selective disclosure • Pseudonymity • Anonymity	Additional user trust needed in IdB

Future work: prototype

- Out-of-band session transfer
  - Bluetooth
  - NFC
  - …
- Trust enforcement
  - Middleware
  - Browser hardening
- Other claim technologies
- Other authentication & assertion protocols

Future work: new concepts

- Tamperproof module in identity broker
  - For less privacy-friendly technologies
  - Enforce selective disclosure
- Identity broker entirely on smartphone
  - Trust enforcement is paramount!
  - Research mobile tamperproof modules
- Trust establishment strategies
  - Without breaking standards?

Questions?