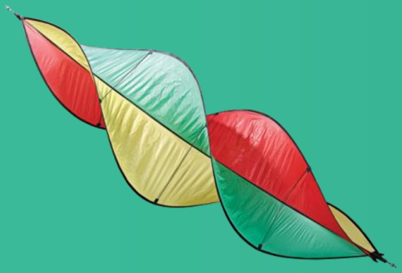


Making OpenID mobile and privacy-friendly

ECUMICT
Ghent, March 27th 2014

Faysal Boukayoua
MSEC, KU Leuven

Overview

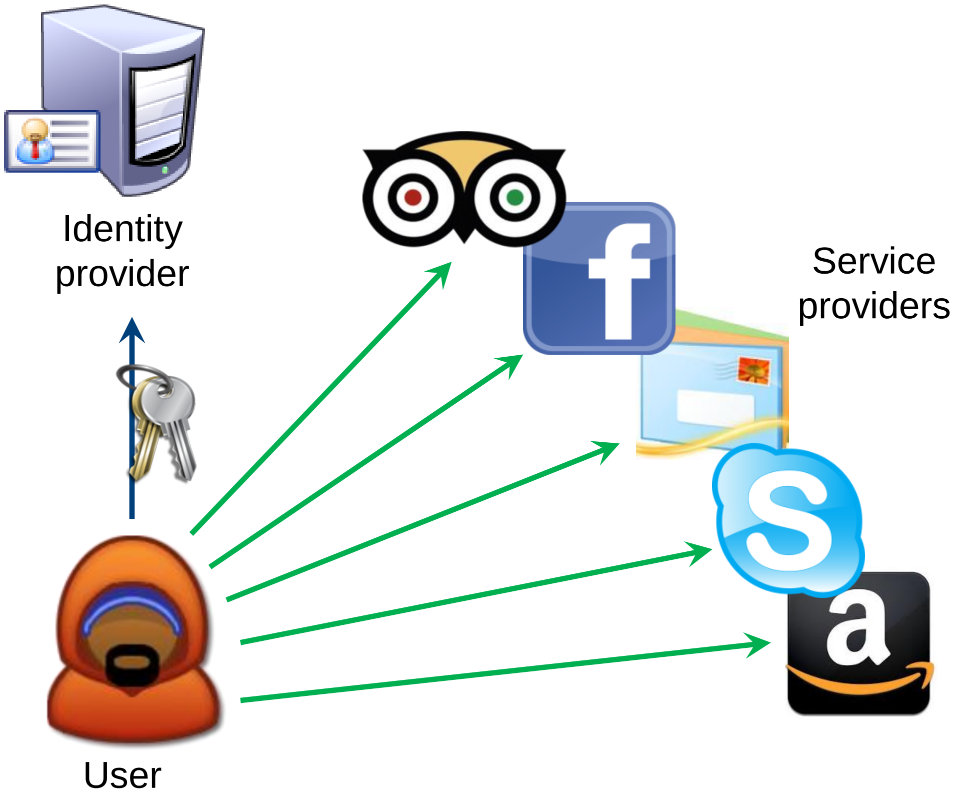
- Introduction
- OpenID
  - What is it?
  - How does it work?
- MSEC’s IdM architecture
- OpenID shortcomings
- Approach
- Implementation
- Evaluation

The advent of today’s Web

- A myriad of services
- Countless logins

- Unreliable user information

The emergence of Web single sign-on

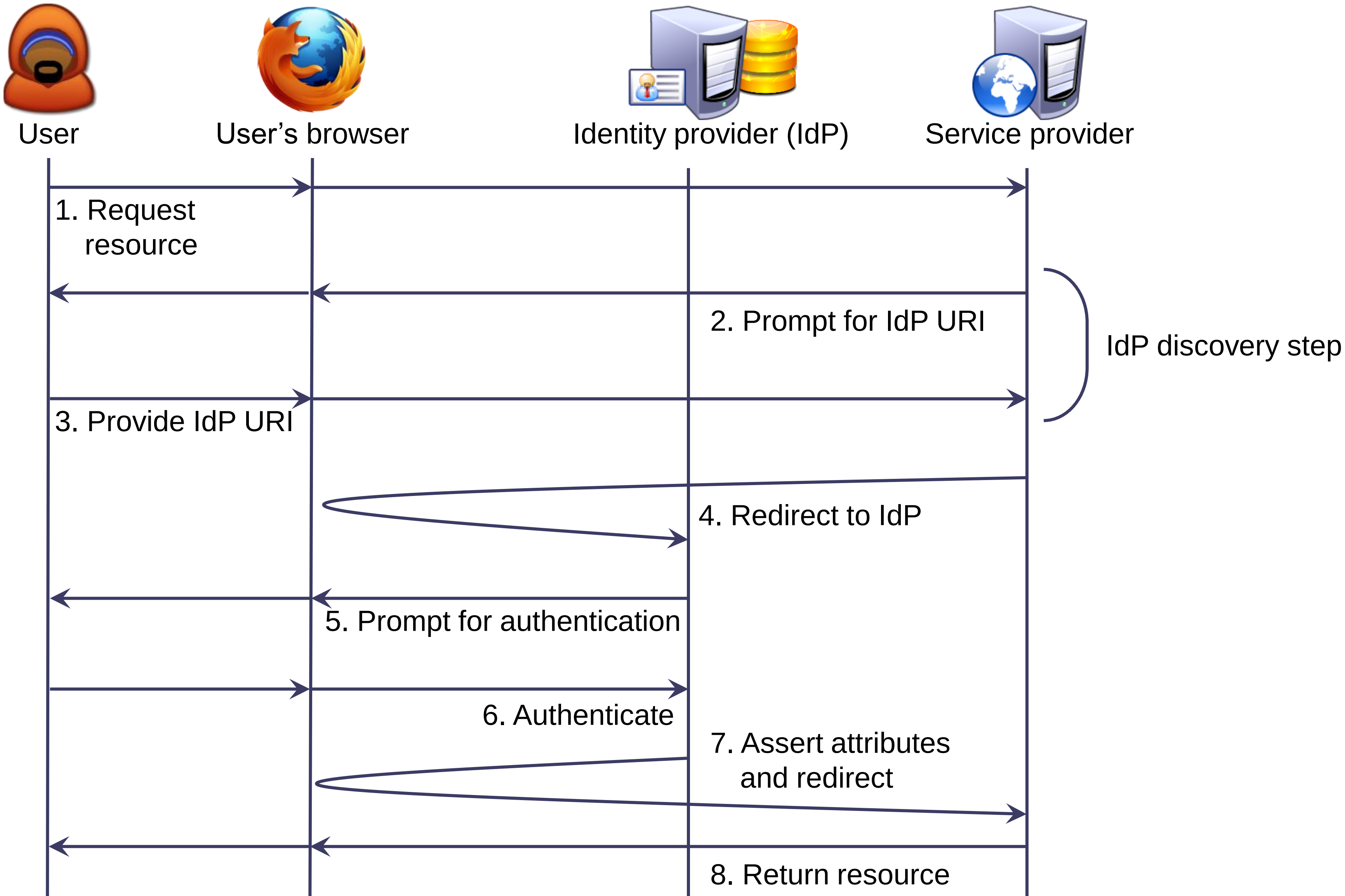


- OpenID
- SAML-based setups
  - Shibboleth
  - Belgian eGov Login
- Proprietary infrastructures
  - Google
  - Facebook
  - Twitter

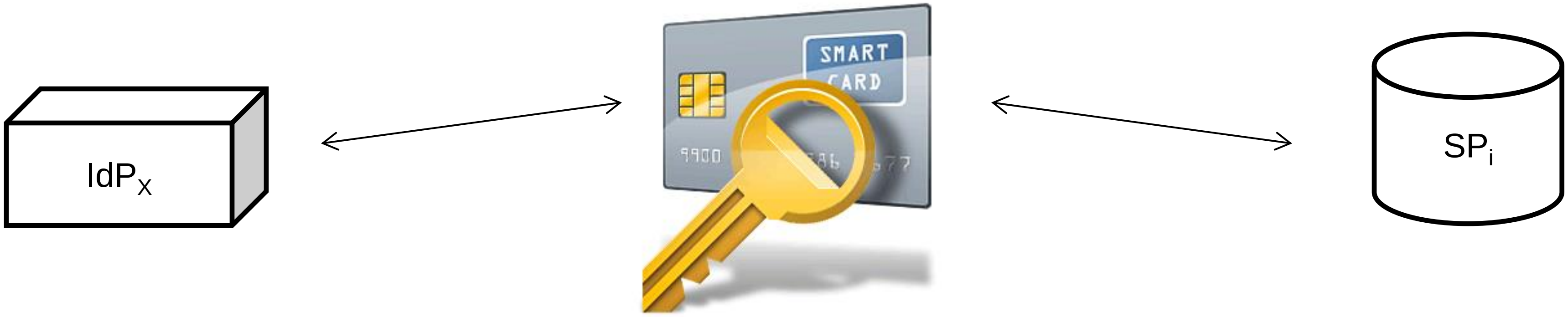
OpenID: what is it?

- Single sign-on standard
- Origins: blogosphere, 2005
- 2007: version 2.0
- 2009: > 1 billion OpenID-enabled accounts
- Many identity providers: Google, Yahoo, Paypal, AOL, Wordpress,…

OpenID: how does it work?



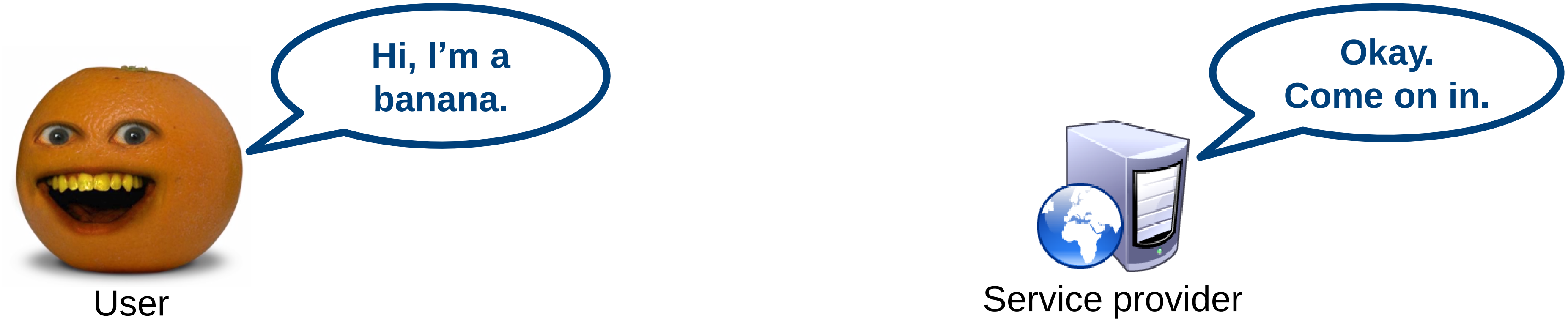
MSEC’s IdM architecture



- Tamper-resistant module is mediator between
  - identity providers
  - service providers
- Access to attributes controlled by
  - external authorities: certificates
  - user: personalized policies on the card

OpenID shortcomings: trust

Before OpenID



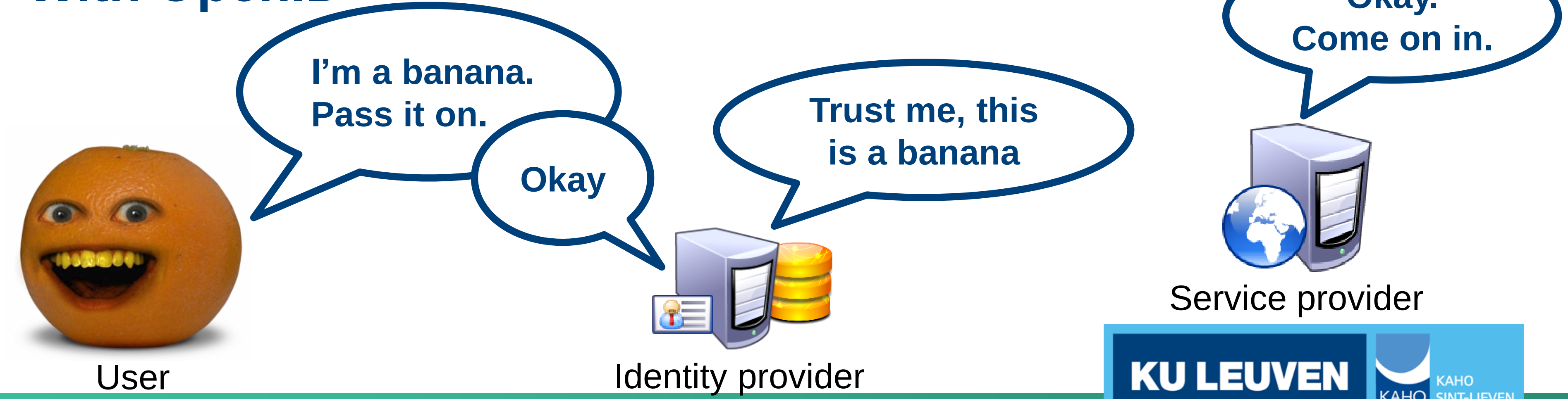
Hi, I’m a banana.

Okay. Come on in.

User

Service provider

With OpenID



I’m a banana. Pass it on.

Okay

Trust me, this is a banana

Okay. Come on in.

User

Identity provider

Service provider

OpenID vs. IdM architecture

		OpenID	IdM architecture
Interoperability	*Must modify workstation?*	Typically not	Yes
	Based on a standard?	Yes	No
Security	*Credentials*	Passwords: weak	ECDH: strong
		Prone to theft by malware	Protected by tamper-resistant card
		Prone to phishing by SP	• Feedback about URI • Certificate checks
	Communication security	Data authentication not required (MITM attacks)	Secure, authenticated channels
	Identity provider	Centralised: high-value attack target	Decentralised
Privacy		Transaction monitoring, linking, profiling	Mediation by card
		Can impersonate user	Mediation by card
	Anonimity level towards service provider	Global user ID (URI)	• Identifiabile • Pseudonymous • (Accountably) anonymous
	Selective attribute disclosure?	Typically not	Yes
	User consent?	Typically not	Yes

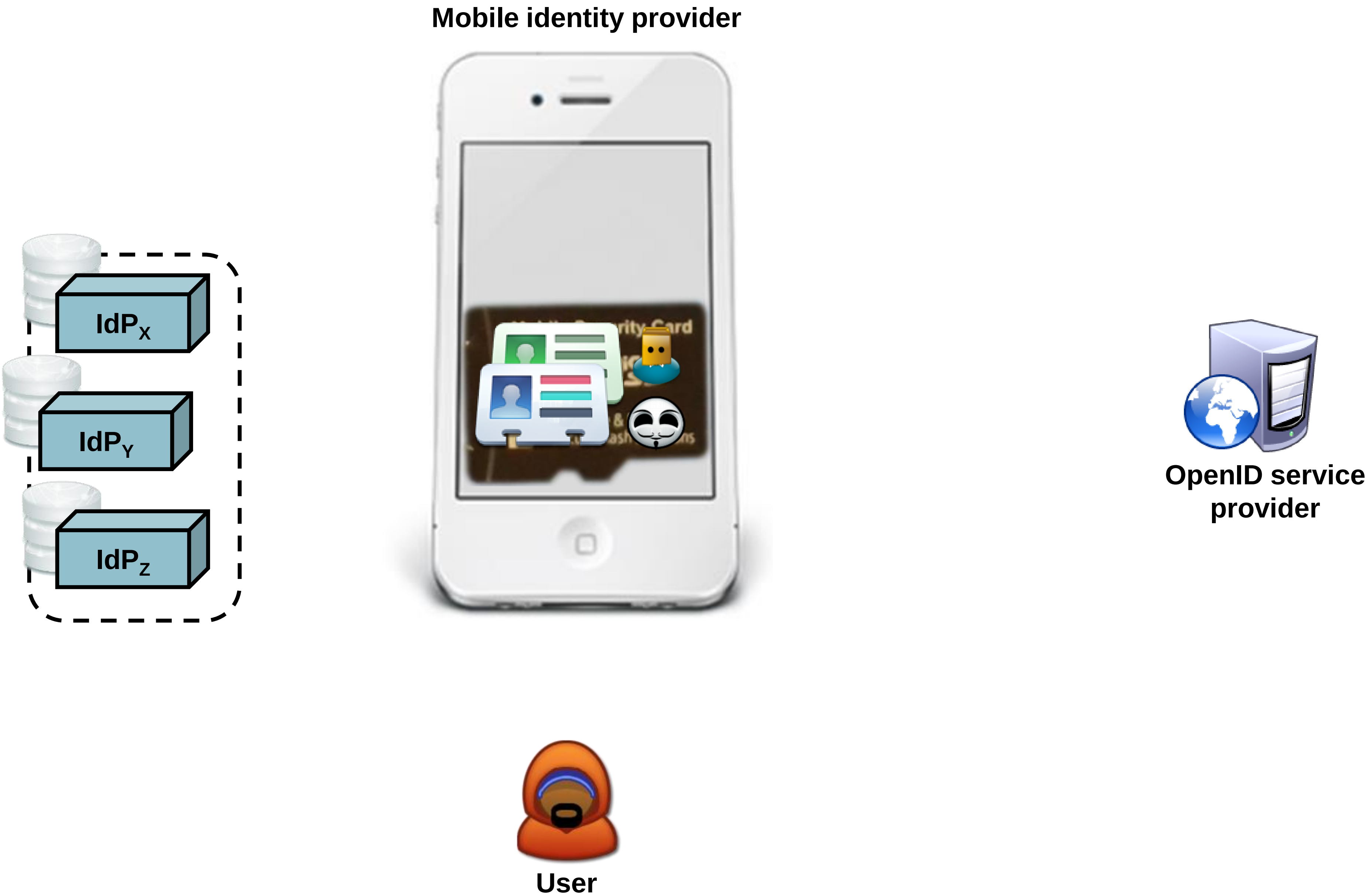
Approach: current trends and opportunities

More mobility &
more computers

Smartphones
omnipresent

Mobile Internet
adoption

Approach: a mobile identity provider



Mobile identity provider

IdP_X

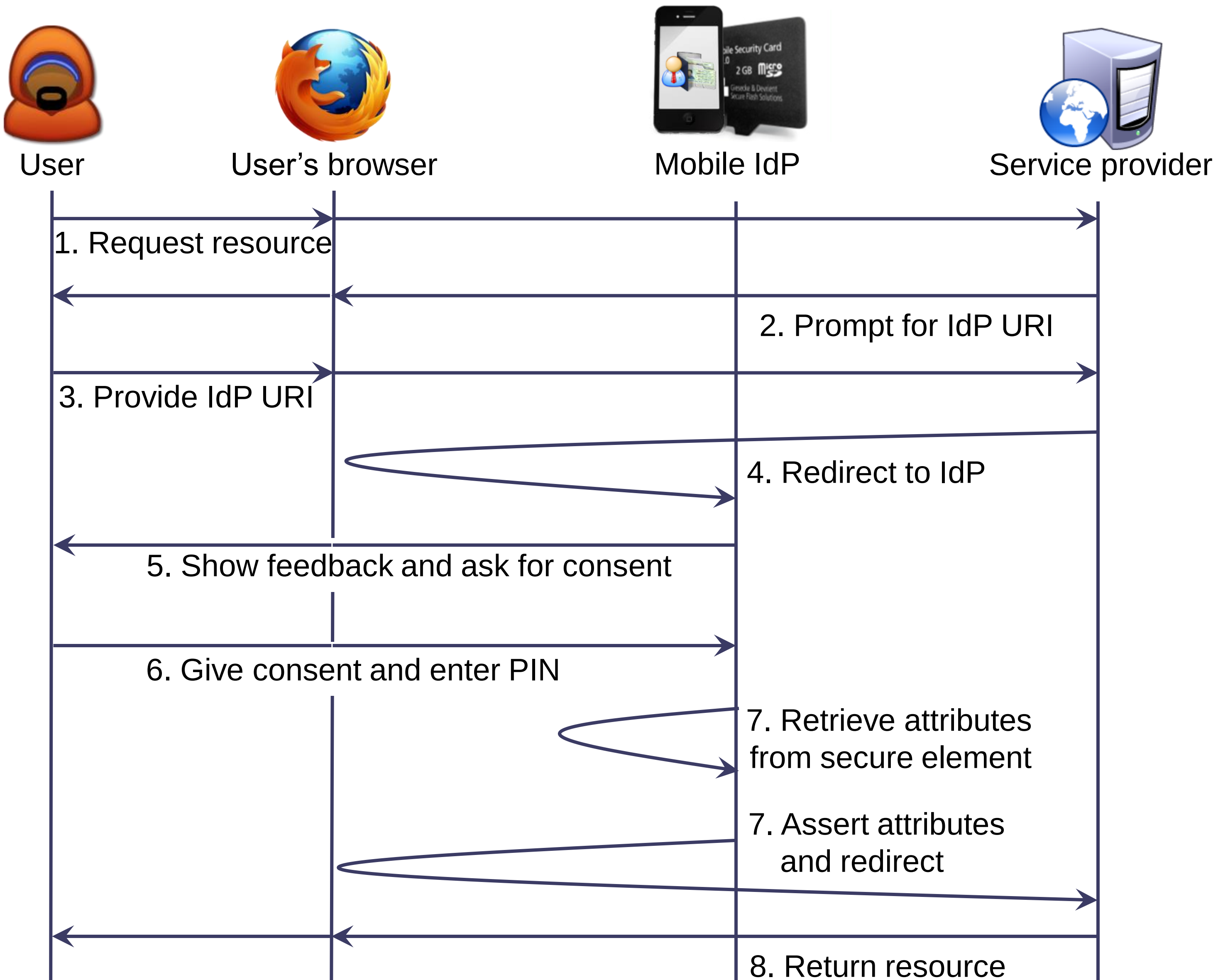
IdP_Y

IdP_Z

OpenID service provider

User

Approach: protocol flow



User

User’s browser

Mobile IdP

Service provider

1. Request resource

2. Prompt for IdP URI

3. Provide IdP URI

4. Redirect to IdP

5. Show feedback and ask for consent

6. Give consent and enter PIN

7. Retrieve attributes from secure element

7. Assert attributes and redirect

8. Return resource

Implementation

Mobile device

- Acer Liquid Glow E330
- Android 4.0.4
- I-Jetty webserver
- Secure element middleware

Secure element

- Giesecke & Devrient Mobile Security Card 1.0
- Java Card 2.2.2
- MSEC’s IdM architecture

Service provider

stackoverflow

Evaluation

- Better privacy
- Better security
- Better interoperability
- Mobile IdP is *personal* server…
  - ○ Network anonymity important!
  - ○ Tor
    - Hidden service (**.onion* pseudo top-level domain)
    - Tor2web proxy to get a non-Tor URI

Q&A