INTEGRATION OF DYNAMIC AUTOMATED METADATA EXCHANGE INTO SAML 2.0 WEB BROWSER SSO PROFILE

DANIELA PÖHN, STEFAN METZGER, WOLFGANG HOMMEL
LEIBNIZ SUPERCOMPUTING CENTRE

IETF 90, Toronto
July 2014

BACKGROUND
FEDERATED IDENTITY MANAGEMENT (FIM)

Characteristics of FIM-based scenarios for collaboration

- Trust boundaries through contractual agreements
- Commonly used technology (e.g. SAML, OpenID)
- Technical trust relationship:
  - **Exchange of aggregated „Metadata“**
  - Common syntax & semantics of user information (attributes)

FOCUS OF OUR APPROACH

- Project-related / dynamic collaborations (non-federation members, project partners)

- Including …

✓ On-demand, fully-automated **initial** exchange of metadata!

✓ Required metadata only!

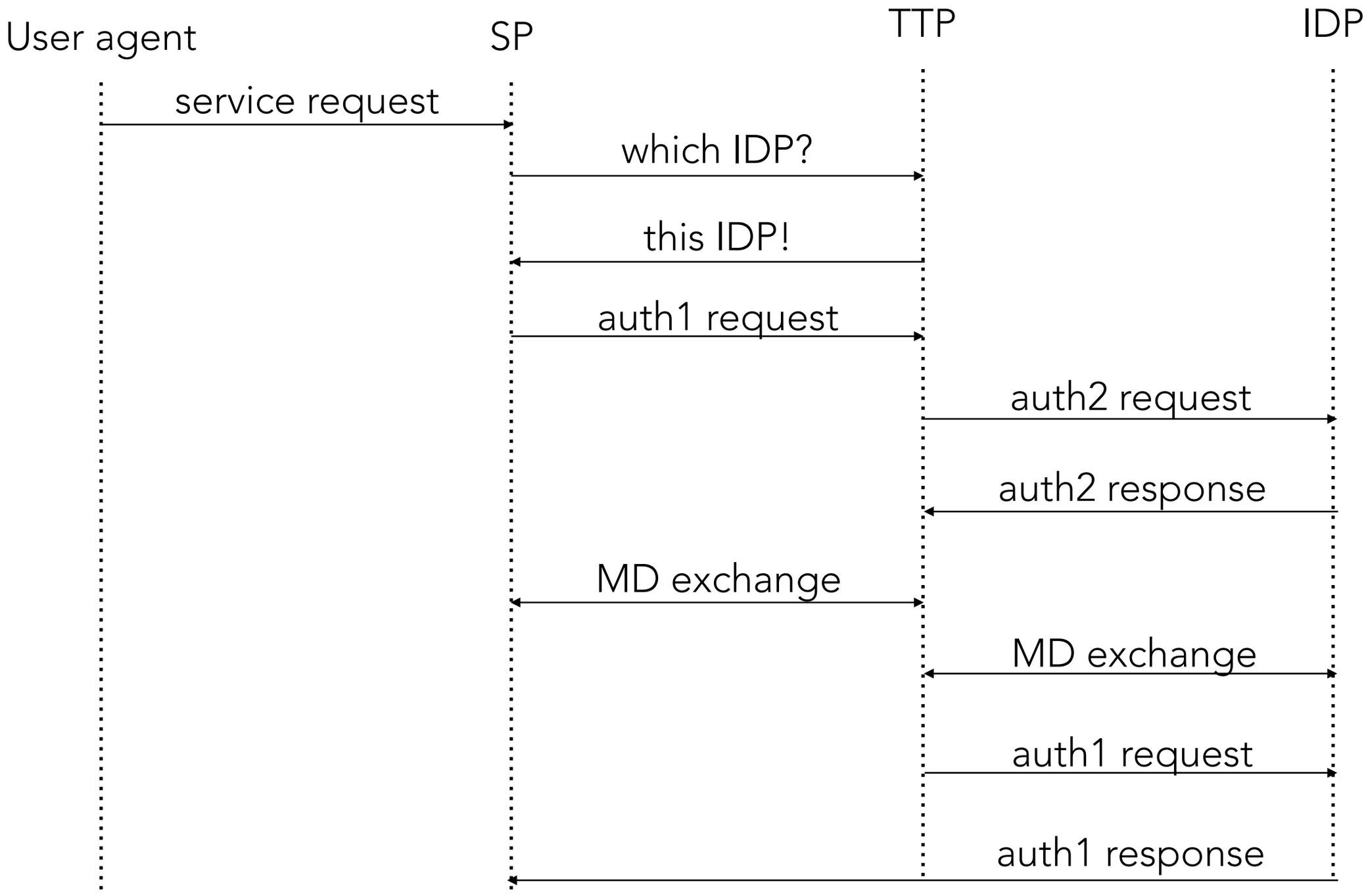
✓ Seamless integration in SAML 2.0 deployments!

DYNAMIC AUTOMATED METADATA EXCHANGE (DAME)

- Metadata register at a trusted third party (TTP)
- Enhanced SAML Authentication Request Protocol through TTP provides …
  - Integrated Identity Provider Discovery[4]
  - Triggering automated initial metadata exchange for bi-directional provider pairing
  - User authentication and transferring attributes to SP only

[4] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf

DAME - IN MORE DETAIL



CONTACT

geant-trustbroker@lists.lrz.de

https://datatracker.ietf.org/doc/draft-poehn-dame/