What is a SAML Proxy?

Thomas Lenggenhager
thomas.lenggenhager@switch.ch
TRID WG Meeting, 26.5.2021
SAML Proxy Overview

SAML Flow

1. credentials
2. assertion
3. authn request
4. assertion
5. credentials
6. authn request
7. assertion
8. assertion

SAML Trust

See a SAML Proxy in action at https://engines.switch.ch/
Use the SAML-tracer browser add-on for details

For SAML flow details see
https://www.switch.ch/edu-id/docs/services/specialsp/proxy/
Two of a kind

• SAML authentication built into IdPv4
  – SWITCH deployed it as Azure AD Proxy
    https://www.switch.ch/edu-id/docs/unis/tech/aad/

• User authentication of a Shibboleth IdPv3 delegated to a Shibboleth SP
  – SWITCH deployed it for
    • SWITCHhub for login to e.g. Adobe, LinkedIn Learning
    • SWITCH edu-ID for login to e.g. Box, Engines, Gartner, Symfact
  – It requires the MPASSid- IdP module
    https://github.com/mpassid/shibboleth-idp-authn-shibsp
  – It allows some user interaction before handing over to the IdP,
    e.g. user select the preferred email address within a PHP script