SAML & eduVPN

NORDUnet Technical Workshop

Tuesday, 24 September 2019

Authentication

- User & Pass
  - SQL database
- LDAP
  - OpenLDAP
  - 389 Directory Server (Red Hat DS)
  - Active Directory
- RADIUS
- **SAML…**

SAML...

- The most interesting challenge when configuring eduVPN...
  - Running the `deploy_${DIST}.sh` script is easy...
  - Setting up some additional profiles requires reading some docs, but not *that* difficult...
  - Configuring SAML requires Apache configuration changes...

SAML != SAML != SAML

- There are many SP implementations available with varying quality, feature completeness, maturity, stability, support...

Supported SAML SPs

- **Shibboleth SP**
  - The *go to* SAML SP
- **mod_auth_mellon**
  - SP implementation for Apache
- **php-saml-sp** (experimental)
  - Simple SP written in PHP (~ 1500 SLoC)

Comparison

Implementation	Easy to setup	Standards Compliance	ePTID	Popularity
Shibboleth SP	-	++	++	++
mod_auth_mellon	-	+	--	+
php-saml-sp	+	-	++	--

Problems

- **Shibboleth SP** is difficult to setup
  - except on Debian, official packages available
- **mod_auth_mellon** has no support to properly “serialize” ePTID
- **php-saml-sp** does not support `EncryptedAssertion` (on purpose) and did not have an extensive (protocol implementation) audit

@SURF

- SURF uses **php-saml-sp** in production
  - `EncryptedAssertion` is not used at all in their federation (SURFconext)
  - Required for smooth MFA integration with “SURFsecureID”
    - requests LoA based on user’s entitlement / affiliation attribute(s)
      - Maybe this could be done also with other SPs?

@Other NRENs

- Some federations require `EncryptedAssertion`, even though it is known broken …
  - Federations don’t allow disabling encryption, or even specifying supported algorithms through metadata to their IdPs → requires supporting AES-CBC
- Some **require** the use of Shibboleth SP proper

Recommendations

- Use **Shibboleth SP** when part of “mesh” federation
- Use **mod_auth_mellon *only*** when you connect to one IdP or a “hub & spoke” federation
- Don’t use **php-saml-sp** (yet)
- Use OS distribution packages if at all possible!

Dreaming out loud...

- Push for modern cryptography in SAML (Ed25519, X25519)
  - ...even AES-256-GCM is barely supported...and *still* not secure (IV-reuse)
- Audit for **php-saml-sp**
  - But some federations *require* `EncryptedAssertion`...
  - ...or just give up on php-saml-sp and standardize on Shibboleth SP?!

Questions?

- Contact
  - eduvpn-support@lists.geant.org
- Twitter
  - https://twitter.com/eduvpn_org
- Web
  - https://www.eduvpn.org/