SWITCHaai News

SWITCH

SWITCHaai
aai@switch.ch
20. May 2020

SWITCHaai News Overview

- Phasing out TLS 1.0 & TLS 1.1
- Not forgotten: Metadata Query (MDQ)
- Shibboleth IdPv4: New default XML encryption algorithm
- The Attribute Release Inspector in the Resource Registry
  It’s your friend!

Phasing out TLS 1.0 & TLS 1.1

- These protocols are obsolete: Grade capped to **B** 

- Attribute Viewer, RR & WAYF-Test require TLS 1.2: Grade **A+**
- Most IdP Hosting IdPs warn users on login page
  referral to http://browsertest.aai.switch.ch
- Require TLS 1.2, block TLS 1.0 & TLS 1.1:
  - On **Thu 2. July 2020** for these IdPs:
    SWITCH eduID, adopted organizations & IdP Hosting customers
  - On **Wed 5. August 2020** for WAYF
- Check your own web server configurations, consult the
  Mozilla SSL Configuration Generator: https://ssl-config.mozilla.org

Not forgotten: Metadata Query (MDQ)

- Growing number of SAML entities ➔ Metadata file size increases

- This mainly affects the interfederation enabled IdPs & SPs
  - Consider to increase the RAM and Tomcat's heap allocation!
- Not affected are the vast majority of SPs registered in SWITCHaai

- If the SWITCHaai federation would support the Metadata Query Protocol, IdPs and SPs could load metadata only on request, when needed.
- Some international federations started to support it.
- We see no urgent need yet, it's on our watch list.

Shibboleth IdPv4: New default XML encryption algorithm

- Be careful in case you plan to update to IdPv4 or install a new IdPv4 IdP:
  - The default XML encryption algorithm changed
    Now it is `AES128-GCM`, up-to-now it was `AES128-CBC`
  - Old Shibboleth SPs and most other SP implementations will **not** interoperate with the new default.
- Check out the details in the IdPv4 Release Notes:
  https://wiki.shibboleth.net/confluence/display/IDP4/ReleaseNotes
- We intend to enhance the Resource Registry, so that SPs will be able declare the encryption algorithms supported.
  Modern IdPs will know when to apply the safer XML encryption algorithm.