

# Calculating metadata propagation time within eduGAIN

Research Project: 2  
Supervisor: Brook Schofield  
GÉANT

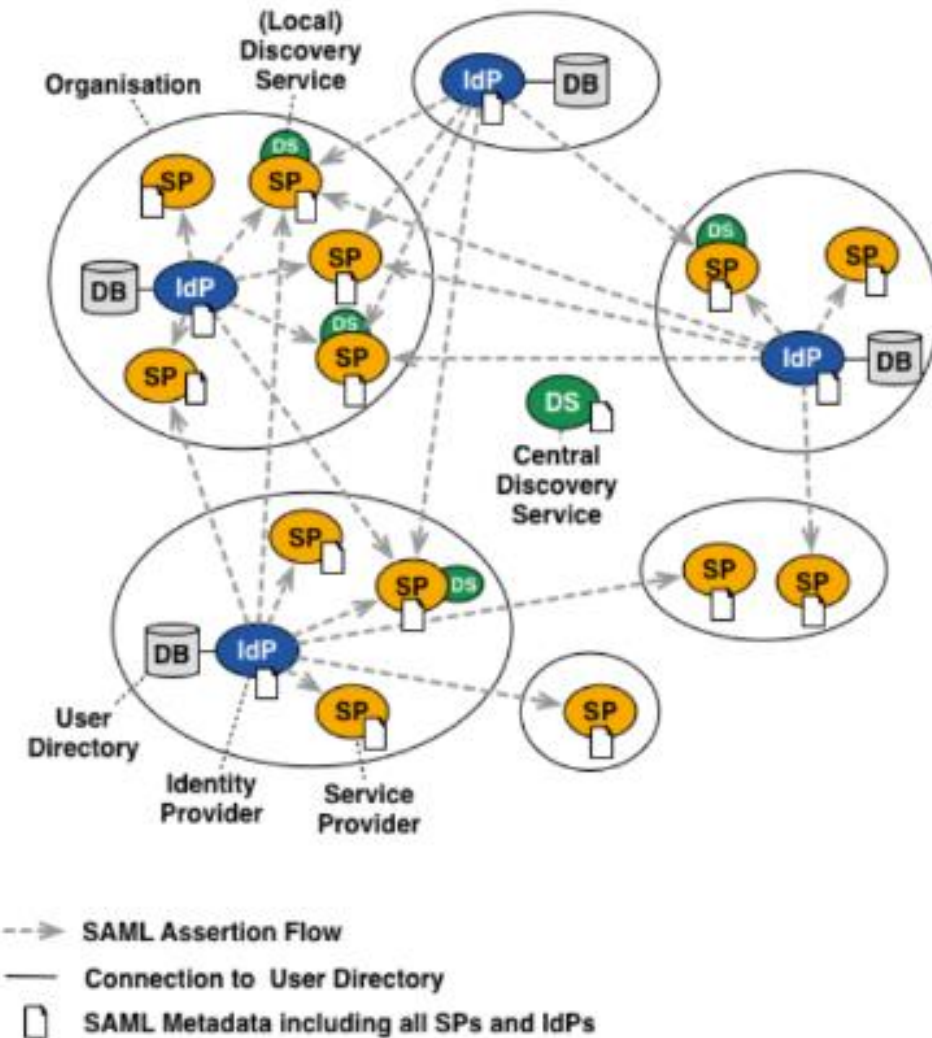
**Marcel den Reijer**

Thursday July 4, 2019

UvA – System & Network Engineering

# Introduction

- eduGAIN
- “Identity” Federation
  - Full Mesh
  - 3 types of metadata files
- Security Assertion Markup Language (SAML)
  - Identity Provider (IdP)
  - Service Provider (SP)



# Motivation

- SAML XML metadata file
  - Security threats
  - Key rollover
  - Updates to service configuration
  - Attribute release information

# Research question

- What is the propagation time of metadata throughout SAML identity federations?
  - *Can manual vs automatic metadata updates be detected by looking at metadata propagation times?*
  - *What levels of cohesion are there within federation?*

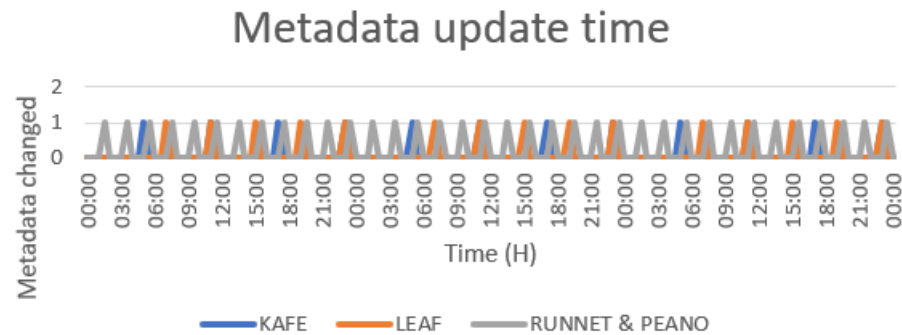
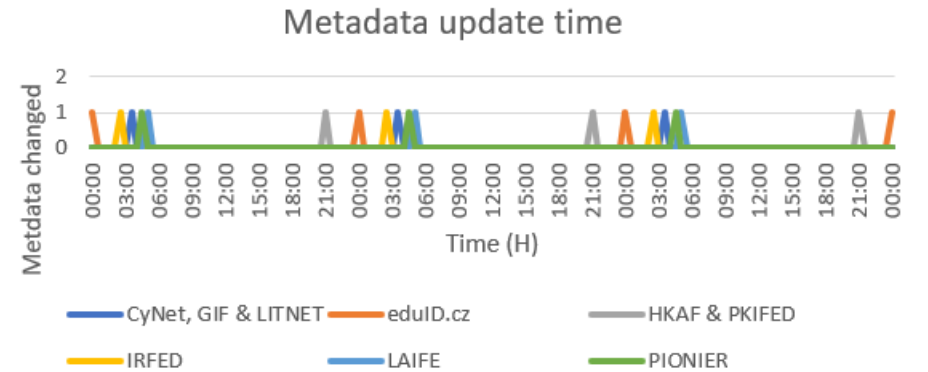
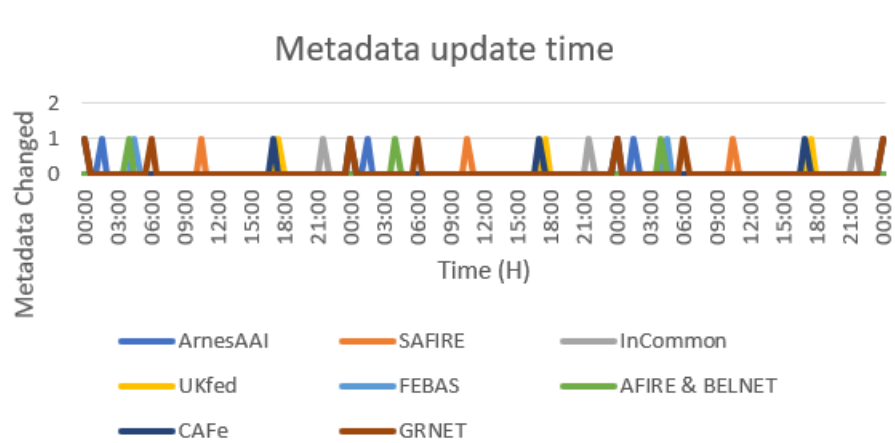
# Related work

- Alex Stuart (2018) has measured the propagation time in the UK Federation. Stuart proposed a method for measuring the propagation time from the metadata of SPs to IdPs using SAML2.0 "AuthnRequest" messages.

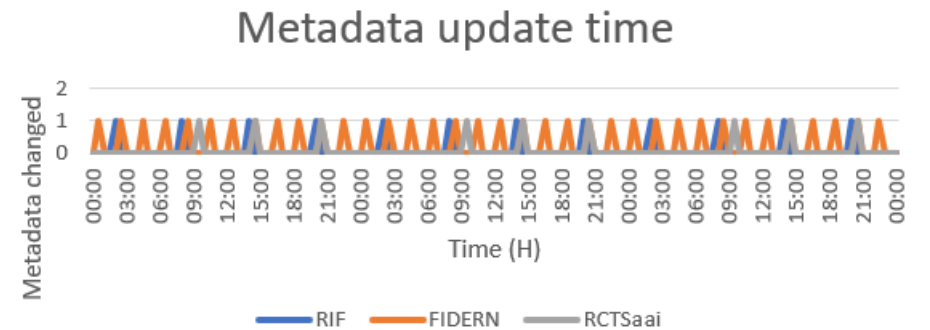
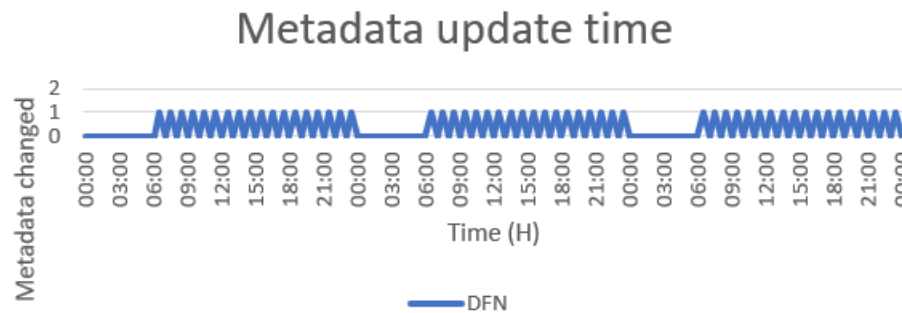
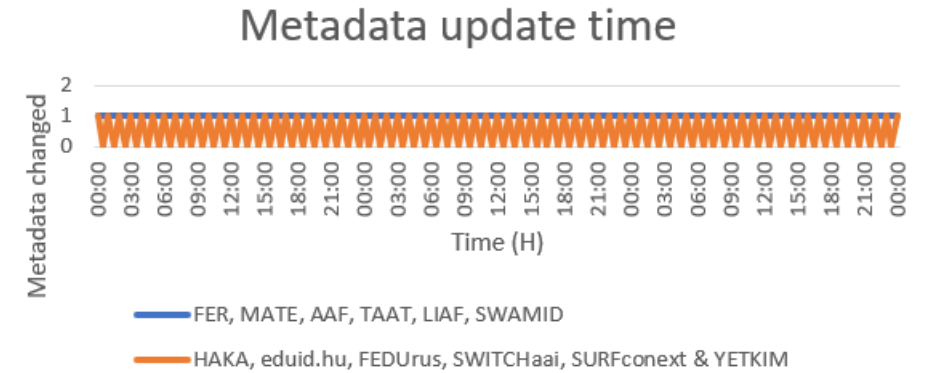
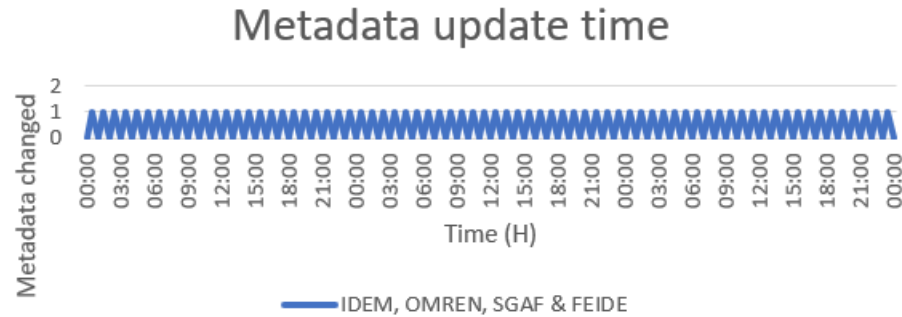
# Approach

- Run script every 30 minutes with Cron
  - Download local, published and eduGAIN metadata files
  - Create MD5 hashes of every metadata file and detect changes to it based on the creation time stamp.
  - Changes in the hash is equal to changes in the metadata file
- XML attributes
  - <md:SPSSODescriptor>
  - <md:IDPSSODescriptor>
- Using regular expressions in order to count the IdPs and SPs of the local, published and eduGAIN XML metadata files

# Results – automatic update detection

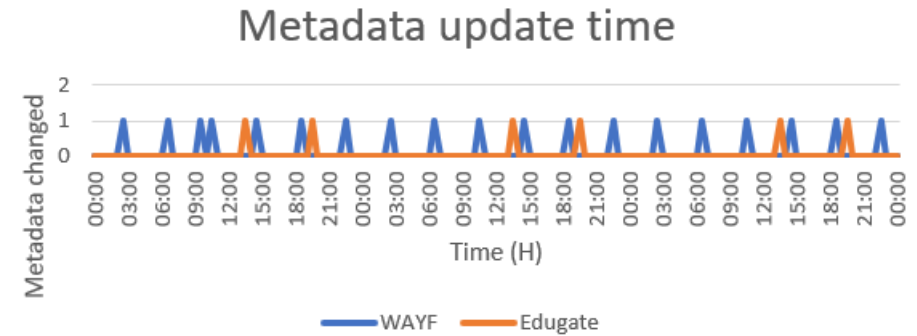
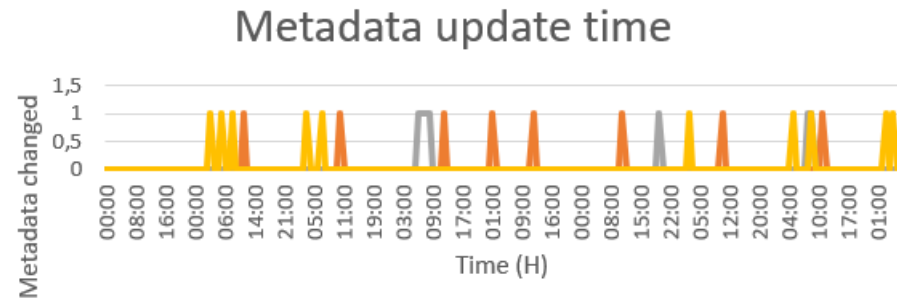


# Results – automatic update detection

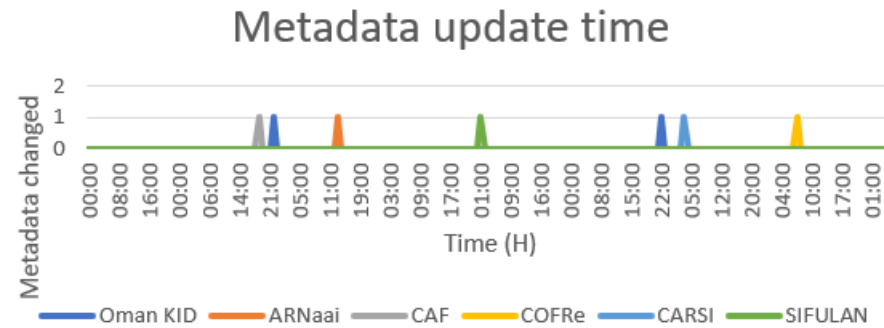




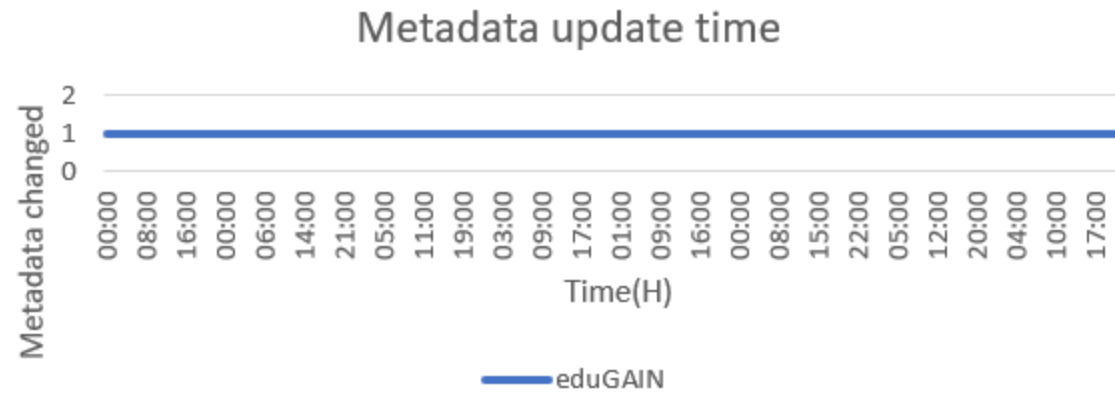
# Results – Manual update detection



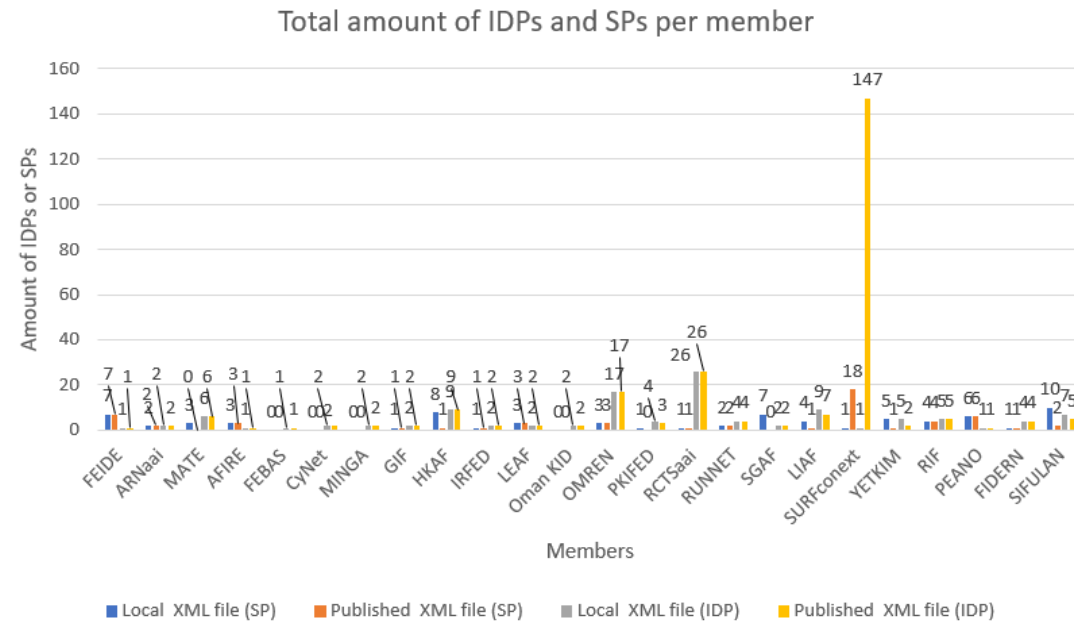
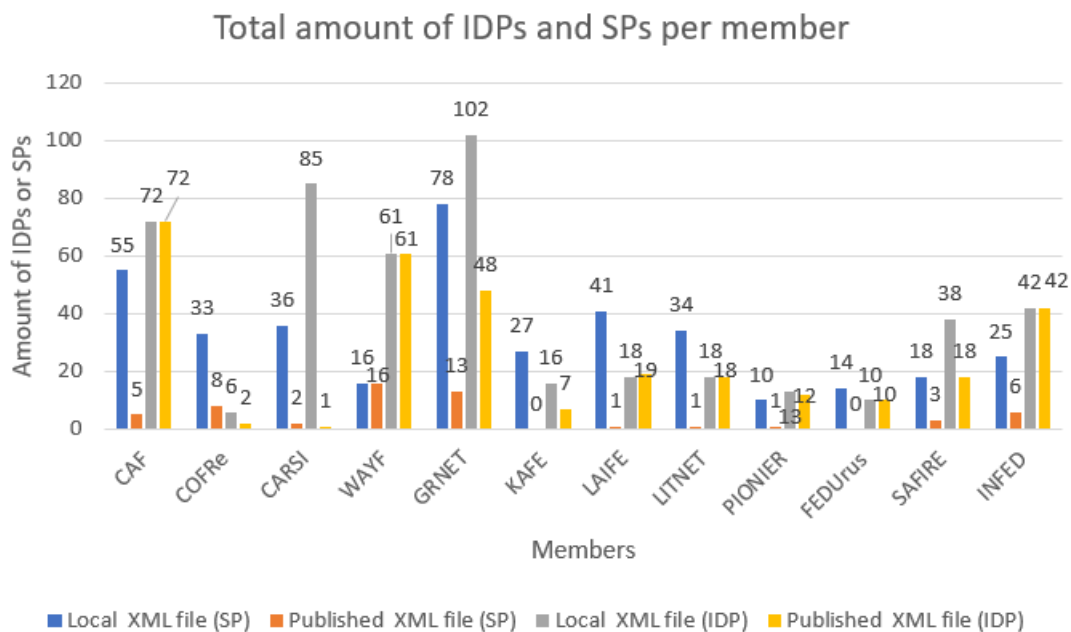
# Results – update detection Unknown



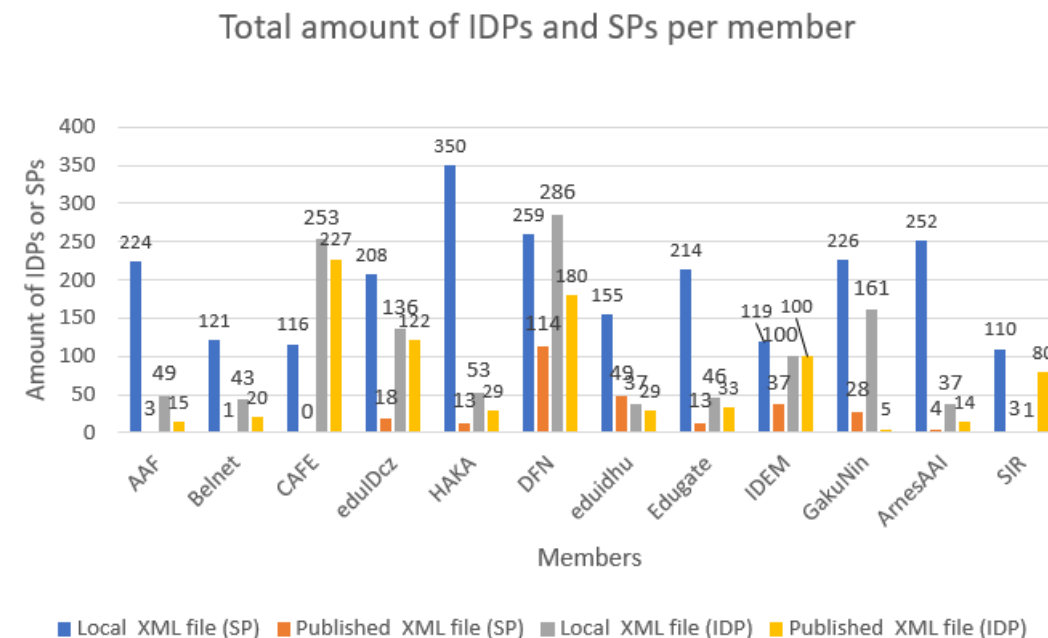
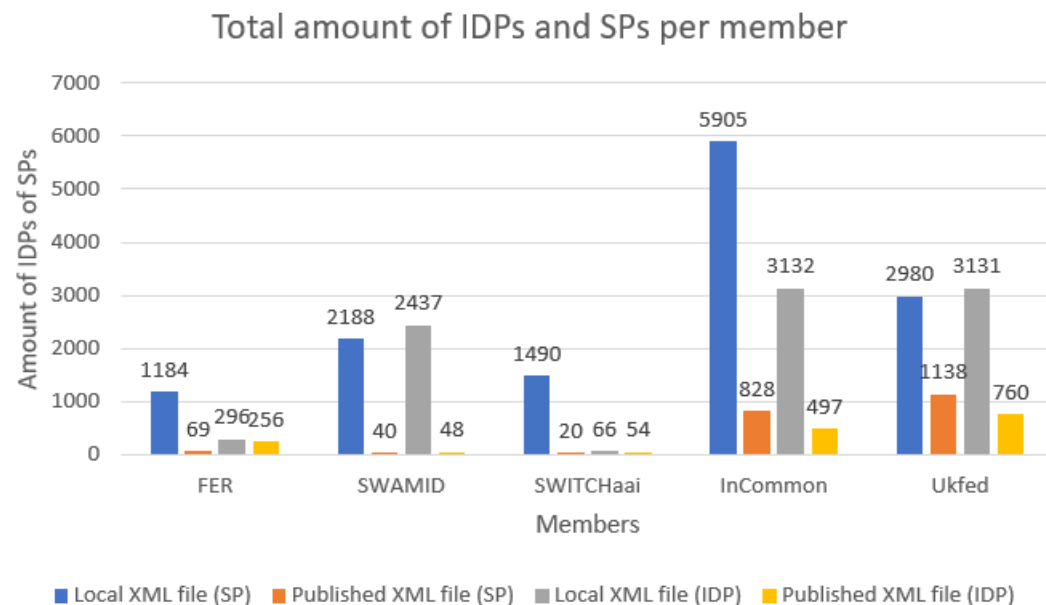
# Results – update time eduGAIN



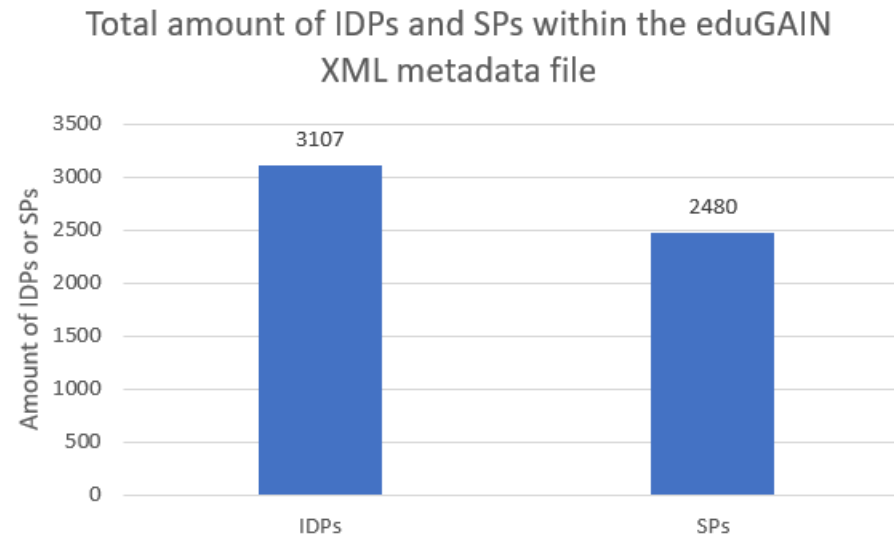
# Results – Cohesion of IdPs and SPs



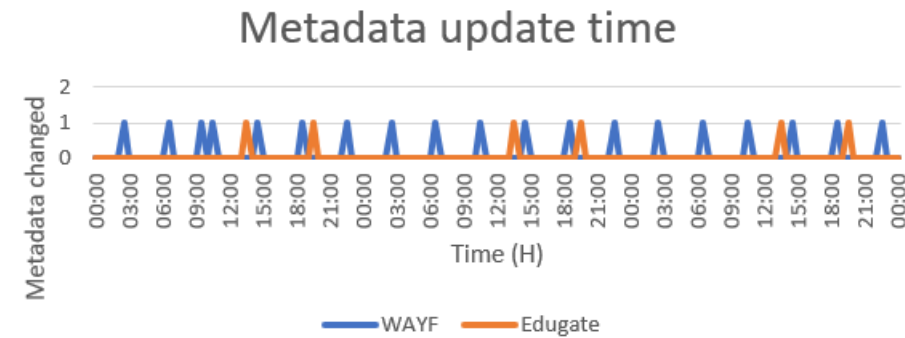
# Results – Cohesion of IdPs and SPs



# Results – Cohesion of IdPs and SPs



# Conclusion part 1.



- *Can manual vs automatic metadata updates be detected?*
  - Yes, eduGAIN member WAYF has a different pattern
- *What levels of cohesion are there within federations?*
  - eduGAIN knows 15,0% of all SPs (2491/16561 local SPs published)
  - eduGAIN knows 27,9% of all IdPs (3034/10862 local IdPs published)
  - eduGAIN aggregate 99, 6% of all SPs (2480 SPs)
  - eduGAIN aggregate 2,4% more IdPs (3107 IdPs)

# Conclusion part 2.

- What is the propagation time of metadata throughout SAML identity federations?
  - EduGAIN updates its metadata file every 60 minutes at 1:00 am, 2:00 am, 3.00 am etc.
  - Max 60 minutes)



# Discussion

- The script in this research runs every 30 minutes at 00:00, 00:30, 01:00 and so on, therefore is it unknown exactly when the changes to the XML metadata files happened
- Time limitations
  - SIR, ACOnet, IUCCIF, eduid.mk, eduidm.ma and AAledu.HR have not updated their metadata files
    - Manually or automatically detection is very hard
  - Oman KID, ARNaai, CAF, COFRe, Carsi & SIFULAN have updated their metadata files once
    - Manually or automatically detection is very hard

# Future work

- First, research via external assessment of metadata exchange, caching different versions of metadata
- Second, calculating the propagation time in a environment where every party has implemented the Metadata Query Protocol (MDQ)
- last subject may be researching if and what bilateral agreement may be exposed by looking at metadata exchange

# Questions

