AAI - Tokens

CLARIN Centre Meeting

9-10 June 2021

Willem Elbers

willem@clarin.eu

CLARIN

API Security

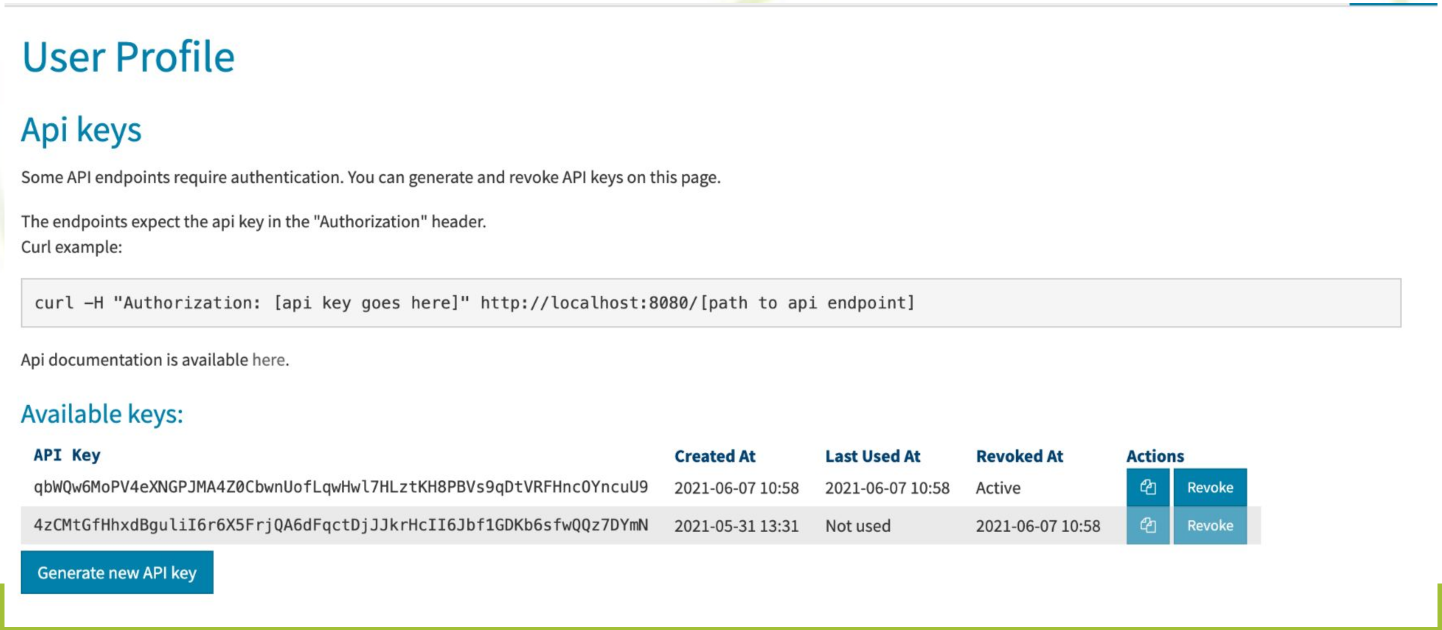
- API key vs Authentication key
  - API Key used to identify the calling project
  - Authentication key to identify a person

- Token types:
  - JSON web token
    - Token is signed, can be validated and used with access to an external service
    - Cannot be revoked, therefore short TTL is recommended
  - Custom
    - Token must be validated with issuer
    - Easy to revoke a token
  - OAuth 2.0
    - More complex, but more flexible and standard, implementation
    - Requires access to an OAuth2 authorization server (AS)
    - Tokens must be validated with the AS
    - Easy to revoke a token

API Security

- Transport
  - How to get the token from the client to the server?
  - Use TLS
  - HTTP Bearer Authentication
    - RFC-6750
    - “Authorization: Bearer <token>”

- Example from the VCR:



User Profile

Api keys

Some API endpoints require authentication. You can generate and revoke API keys on this page.

The endpoints expect the api key in the "Authorization" header.
Curl example:

```
curl -H "Authorization: [api key goes here]" http://localhost:8080/[path to api endpoint]
```

Api documentation is available here.

Available keys:

API Key	Created At	Last Used At	Revoked At	Actions
qbWQw6MoPV4eXNGPJMA4Z0CbwnUofLqwHwl7HLztKH8PBVs9qDtVRFHncOYncuU9	2021-06-07 10:58	2021-06-07 10:58	Active	Revoke
4zCMtGfHhxdBguliI6r6X5FrjQA6dFqctDjJJkrHcII6Jbf1GDKb6sfwQQz7DYmN	2021-05-31 13:31	Not used	2021-06-07 10:58	Revoke

AAI - AAggregator

CLARIN Centre Meeting

9-10 June 2021

Willem Elbers

willem@clarin.eu

Statistics

- https://lindat.mff.cuni.cz/services/aaggreg/
- Besides giving insight into attribute release we can also use the AAggregator to generate useful statistics
- Example:
  - Based on 7 SPs (out of 51) with AAggregator integration enabled,
  - During the period between 2020-01-20 en 2021-05-25
  - We got:
    - TotalLogins: 9999,
    - OtherLogins: 9339
    - ClarinIdpLogins: 660
    - Using a total of 307 distinct IdPs

Statistics

- Example:
  - Logins per SP:

SP	CLARIN IdP	Own IdP	Other IdP	Total
https://ufal-point.mff.cuni.cz/shibboleth/eduid/sp	168	1172	591	1931
https://sp.www.kielipankki.fi	3	319	1139	1461
https://sp.korp.csc.fi/	40	205	3980	4255
http://sp.lat.csc.fi	6	10	139	155
http://sp.vs1.corpora.uni-hamburg.de	300	337	1258	1895
https://sp.catalog.clarin.eu	105		111	216
https://sp.vcr.clarin.eu	38		39	77

  - Rough login distribution: 6.7% via CLARIN IdP, 20.5% via own IdP and 72.9% via other IdPs (eduGain)

- Any suggestions for other statistics?

Uptake

- With 8 out of 50+ SPs there is much room to improve the uptake
  - Idea: make AAggregator integration required in the certification guidelines?
  - Any other ideas?

AAI - Proxy

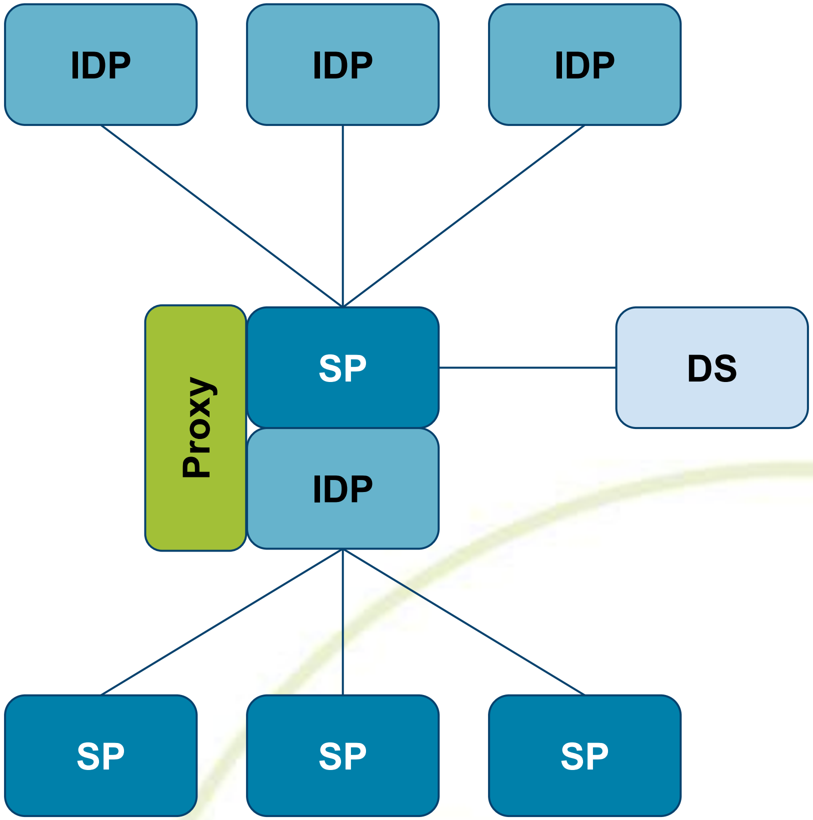
CLARIN Centre Meeting

9-10 June 2021

Willem Elbers

willem@clarin.eu

Architecture - Proxy Setup



- Centralised metadata management → Less Administrative overhead for CLARIN ERIC, only one SP entityID to manage across federations (and one IDP entityID for within the SPF)
- Centralised communication through proxy.

Advantages / Disadvantages / Discussion

- Centralised control
  - For us only one entityID to manage across federations, including eduGain
  - If CLARIN ERIC only supports the proxy, centre SP metadata is not propagated to eduGain / NRENs.
  - For SP only one IDP entityID to trust / manage
  - For IDP only one SP entityID to trust / manage
  - Technical setup matches organisational setup
- Single point of failure
  - Can we properly mitigate this?
    - Providing a redundant setup will require some investigation and work from our (CLARIN ERIC) side
  - Is it a blocker for SPs to accept this approach?
- Allows for credential translation (nice to have)
  - Also support OAuth2 to connect SPs
  - Also support OpenID connect IDPs (social IDPs)

Advantages / Disadvantages / Discussion

- Extend attribute set if needed
  - Allows to request additional attributes from the user and augment the session with any information not released by the original IdP
  - Potentially also normalize attributes released from upstream IdPs
- Potential issue with discovery → discovery → … flow for the end user.
  - User might have to select IdP multiple times while being redirected through several discovery services.
    - Example:
      - user tries to login with a CLARIN SP
      - the CLARIN proxy shows a DS and the user selects B2ACCESS
      - B2ACCESS also show a DS and the user selects …
      - ...
  - Potential solutions are under discussion:
    - A specification for IdP hinting: https://zenodo.org/record/4596667/