Solutions to Sharing Institutional Resources for Collaborations

Science Collaboration Zone

Gerben Venekamp
SURFsara

June 12, 2018
TNC'18 – Trondheim

Dutch Federation: SURFconext

- Hub and Spoke and it Works right?
- After all, institutes can offer services to large groups without too much trouble.
- A SURFconext representative takes care of the hard work, e.g. allowing the attributes to flow.
- It works for groups. 😄
- ...how about individual users?

Dutch Federation: SURFconext

An Individual Researcher Would Like to Use an External Service Provider

An individual researcher needs to:

- Find the SURFconext representative.
- Explain why the external service is necessary, what it does, etc.
- Convince the SURFconext representative and security officer that it is okay to send to the SP attributes.
- There are a lot of individual Researchers (long tail).
- SURFconext representative has a lot of other responsibilities too.

Science Collaboration Zone

What is it About?

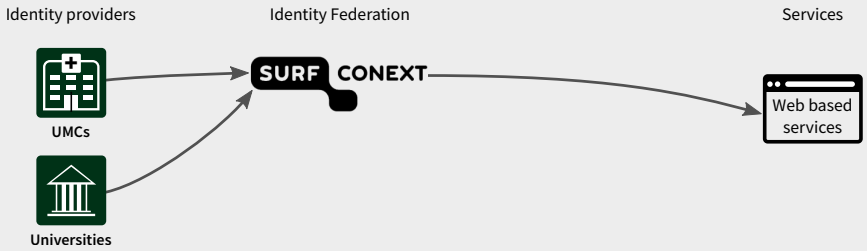
- Policies: creating trust for IdP, e.g. only allow SPs that meet minimum requirements.
- IdP Attributes are not transparently released to SPs.
- Easy management of Collaborative Organisations.
- Make it easy for individuals to enroll into a Collaborative Organisation.
- Platform GDPR compliant and put responsibilities at the proper party.[1]

[1] https://wiki.surfnet.nl/display/SCZ/Getting+IdP's+to+connect+to+the+SCZ+proxy

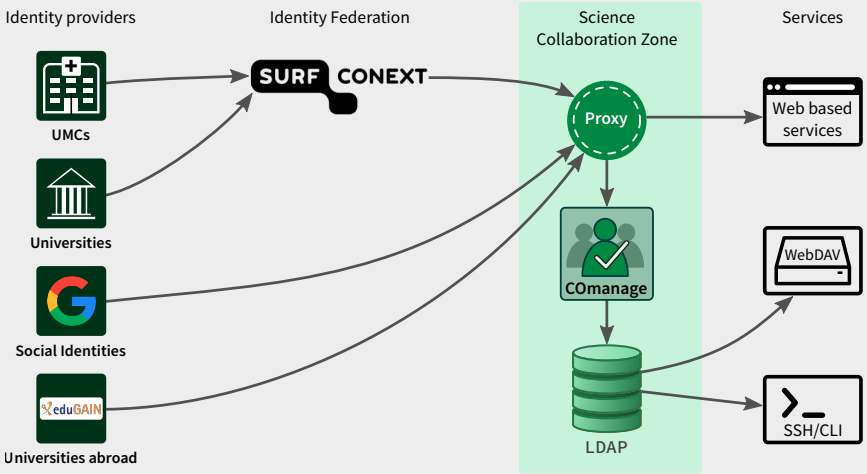
Then non-web use case is supported by:

- LDAP (Application Specific Passwords, tokens)
- OIDC (oAuth2)

SURFconext


Identity providers
Identity Federation
Services
UMCs
Universities
SURF CONEXT
Web based services

Science Collaboration Zone



Science Collaboration Zone

Major Components

Within the Science Collaboration Zone a number of components have been integrated. The major ones are:

- COmanage (*enrollment, provisioning, delegation, attribute management*)
- SATOSA (*SAML to SAML proxy, OIDC, attribute release*)
- pyFF (*metadata management, discovery*)

COmanage

Enrollment, Provisioning, Delegation, Attribute Management

- Provides a portal for management of Collaborations.
- Special SP within the SCZ context.
- Attribute store for all attributes.

SATOSA

SAML to SAML Proxy, OIDC, Attribute Release

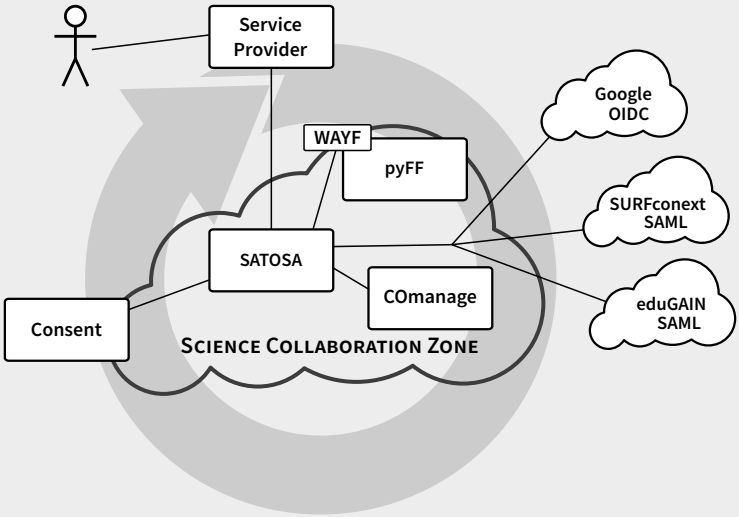
- Collects attributes from COmanage.
- Connect SAML IdP from eduGAIN.
- Connect services via SAML or OIDC.
- Inform/Consent.
- Authorization enforcement.

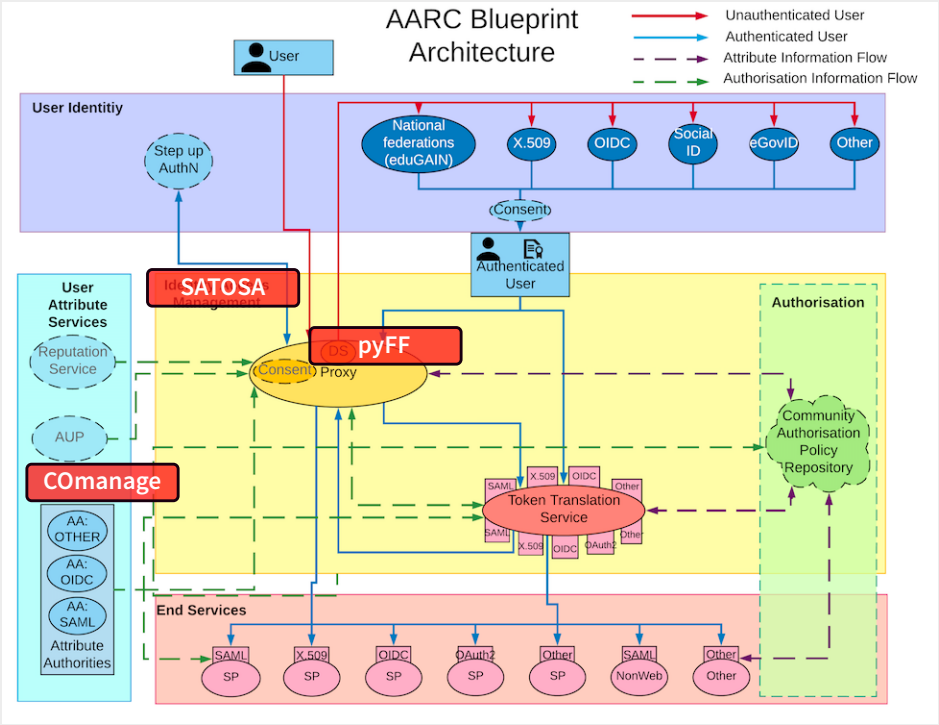
pyFF

Metadata Management, Discovery

- Handles meta data from different sources:
  - SURFconext
  - eduGAIN
  - Social (Google)
- Handles discovery.

Architecture




AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Attribute Information Flow
Authorisation Information Flow
User
User Identitiy
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGovID
Other
Consent
Authenticated User
SATOSA
pyFF
DS
Consent
Proxy
User Attribute Services
Reputation Service
AUP
COmanage
AA: OTHER
AA: OIDC
AA: SAML
Attribute Authorities
Authorisation
Community Authorisation Policy Repository
SAML
X.509
OIDC
Other
Token Translation Service
OAuth2
End Services
SP
NonWeb

Pilot 1: Use Case

BBMRI

Use-case

User must be able to SSH into a Virtual Machine

Description

Letting users from a Collaborative Organisation access a VM by means of their public SSH. The public SSH key is uploaded to and provisioned by the SCZ portal.

Results

- Based on their uploaded public SSH users gain access to the VM.
- Users are provisioned within COmanage.
- On the VM: just in time creation of the user's environment through the PAM stack.

Pilot 2: Use Case

U2CONNECT / UTRECHT UNIVERSITY

Use-case

Allow data sharing between an institute and outside world.

Description

Utrecht University used iRODS for data storing and sharing. To this end a portal has been built to easily manage local users (YODA). The concept of Federative Authentication is foreign to both the YODA and iRODS. SCZ is used to add the missing functionality.

Status

- When new people are added to the YODA portal, those people are also provisioned to SCZ.
- In SCZ users can generate a shared secret to do TOTP.
- iRODS learns the share secret and authenticate users based on tokens.
- WebDAV access to iRODS also works with TOTP by shortly allowing reuse of the last TOTP token.
- Current solution is planned to go live in Q3.

Pilot 3: Use Case

University of Amsterdam / Amsterdam University of Applies Sciences

Use-case

Sharing local services with users outside the UvA/HvA domain.

Description

The UvA/HvA must be in control of the creation of Collaborative Organizations. The CO is administered by UvA/HvA. The CO manager creates new research groups by creating COUs.

Status

- Setting up LDAP on receiving end.
- Discussion on user experience when interacting with SCZ.

Pilot 4: Status

VUmc/AMC

Use-case

Providing access to services by external users in an Azure Active Directory environment.

Description

VUmc/AMC use Azure AD for their identity management. SCZ needs to connect to Azure in order to enable provisioning of external users.

Status

- Leverage LDAP Synchonization Connector (LSC) for provisioning Auze AD.

Questions?

INFO: https://wiki.surfnet.nl/display/SCZ/

SURFNET: *Niels van Dijk* • Bas Zoetekouw • Martin van Es • Michiel Uitdehaag • Raoul Teeuwen
SURFSARA: *Gerben Venekamp* • Harry Kodden