SURFconext

REFEDS and eduGAIN webinars on H&S federations
Agenda

01 Introduction
02 Hub & spoke
03 User perspective
04 IdP perspective
05 SP perspective
06 Operations perspective
07 OpenConext
08 What do you need?

4 demos
Team Trust & Identity @SURF

Team trust & identity development
- Exploring and building new solutions and services

Team trust & identity operations
- Operations of trust & identity services

Our services
- SURFconext
- SURFsecureID
- SURFresearch access management
- eduID
**A brief history lesson**

**2007**
SURFfederatie

- Started with hub & spoke and 5 IdP’s

**2013**

- SURFfederatie = SURFconext
  - SAML login + group management

**2014**

- Professionalizing operations
  - Software quality, support and releases

**2017**

- OpenID Connect
  - Service providers can connect via OpenID Connect

**2020**

- eduID as guest IdP
  - Third-generation guest IdP, but the beginning of something new

**2022**

- ISO 27001
  - ISO 27001 certified
Growth of the number of logins
MORE THAN 260 MILLION LOGINS WITH SURFCONEXT IN 2022

NUMBER OF UNIQUE LOGINS

- 2018: 118 million
- 2019: 157 million
- 2020: 215 million
- 2021: 251 million
- 2022: 260 million (increase of 4%)

NUMBER OF SERVICE PROVIDERS

- 2018: 970
- 2019: 1,176
- 2020: 1,504
- 2021: 1,683
- 2022: 2,116 (growth of 433)

NUMBER OF UNIQUE USERS

- 2018: 1,504,432
- 2019: 1,734,745
- 2020: 1,928,718
- 2021: 2,183,438
- 2022: 2,239,801 (increase of 3%)

NUMBER OF IDENTITY PROVIDERS

- 2018: 164
- 2019: 180
- 2020: 184
- 2021: 199
- 2022: 188 (decrease of 11)
Why hub & spoke?

**Multi-Protocol support**
Easy integration of protocols like OIDC and simplifying the introduction of new authentication mechanisms.

**Flexibility**
Allows fast development and supports institution’s choices (e.g., Microsoft) centrally, streamlining new developments like eduID.

**Expertise optimization**
Efficiently leverages specialized knowledge at SURF, reducing duplication and improving resource allocation.

**Single Connection**
Institutions and service providers only need to establish and maintain one connection.
Hub & spoke

- The user authenticates at the home institution (identity provider)
- Attributes can be shared with the service (service provider)
- Single sign on

Only one connection

- Trust is organized centrally
- Extra features: stats, dashboards, strong authentication etc.
Authentication flow
SURFconext (SAML)

SP Service

1. User click 'login via SURFconext'

2. SP generates SAML request

3. SP redirects user with SAML request to SURFconext

4. WAYF User selects institution on WAYF

5. IdP parses SAML request, authenticates user

6. IdP generates SAML response

7. SP verifies SAML response

8. SURFconext sends new SAML response to ACS URL of the SP

9. IdP redirects user back to SURFconext with SAML response

User is logged in

profile.surfconext.nl
Authentication flow
SURFconext (SAML)
Authentication flow
SURFconext (SAML)

1. User clicks 'login via SURFconext'
2. SP generates SAML request
3. SP redirects user with SAML request to SURFconext
4. User selects institution on WAYF
5. IdP parses SAML request, authenticates user
6. IdP generates SAML response
7. IdP redirects user back to SURFconext with SAML response
8. SURFconext sends new SAML response to ACS URL of the SP
9. SP verifies SAML response

User is logged in
Authentication flow
SURFconext (SAML)

1. User clicks 'login via SURFconext'.
2. SP generates SAML request.
3. SP redirects user with SAML request to SURFconext.
4. User selects institution on WAYF.
5. IdP parses SAML request, authenticates user.
6. IdP generates SAML response.
7. IdP redirects user back to SURFconext with SAML response.
8. SURFconext sends new SAML response to ACS URL of the SP.
9. SP verifies SAML response.
10. User is logged in.
Demo Profile
SURFconext: The IdP perspective

- One technical connection
- IdP dashboard provides insight in all connection related information (statistics, privacy information available service providers)
- Technical expertise provided by the SURFconext team
## IdP software products distribution

<table>
<thead>
<tr>
<th>#</th>
<th>%</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>46%</td>
<td>MS ADFS</td>
</tr>
<tr>
<td>86</td>
<td>39%</td>
<td>MS Azure AD</td>
</tr>
<tr>
<td>20</td>
<td>9%</td>
<td>SimpleSAMLphp</td>
</tr>
<tr>
<td>5</td>
<td>2%</td>
<td>NetIQ AM</td>
</tr>
<tr>
<td>3</td>
<td>1%</td>
<td>Shibboleth</td>
</tr>
<tr>
<td>2</td>
<td>1%</td>
<td>Google Workspace</td>
</tr>
<tr>
<td>1</td>
<td>0%</td>
<td>eduID</td>
</tr>
<tr>
<td>1</td>
<td>0%</td>
<td>OpenSSO / Oracle AM / OpenAM</td>
</tr>
<tr>
<td>1</td>
<td>0%</td>
<td>VMware Identity Manager</td>
</tr>
</tbody>
</table>
Demo IdP Dashboard
Wait, how about eduGAIN?

SURFconext is a true proxy

We publish a unique SSO endpoint for every IdP:

https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20230503/613fe2325e027d8b02ff49c9d10521d7

https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20230503/583ece5a5636f8ee06b742c66d8c1d5
**SURFconext: The SP perspective**

- Single connection to potential 200 IdP's
- Choice between OpenID connect and SAML
- Connect APIs with SURFconext API security
- Self service dashboard to manage connections
Demo SP Dashboard
SURFconext: The operator perspective

- Manage is the application for administrators to configure SURFconext. SP and IdP configuration, ACL’s, ARP, consent and more.
- One central database (Mongo) used by Engine, IdP and SP dashboard and Manage.
Demo Manage
OpenConext

- Everything developed in the open on GitHub, free to use and contribute
- Modular system: start small and add components when you need them
- Used by several federations, with a community of users and contributors
<table>
<thead>
<tr>
<th>Repository Name</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenConext-Access</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Stepup-API</td>
<td>Public</td>
<td>Application Programming Interface for OpenConext-Stepup</td>
</tr>
<tr>
<td>OpenConext-devconf</td>
<td>Public</td>
<td>Contains configuration file to get an development environment up and running</td>
</tr>
<tr>
<td>OpenConext-attribute-aggregation</td>
<td>Public</td>
<td>OpenConext attribute aggregation</td>
</tr>
<tr>
<td>OpenConext-deploy</td>
<td>Public</td>
<td>Ansible-based deployment automation for the OpenConext platform</td>
</tr>
</tbody>
</table>

*Images of repository icons and activity graphs are present.*
What do you need to run a hub & spoke federation?

In order to facilitate:

• 3000 logins per minute / 200 IdPs / 2000 SPs
• Run & develop OpenConext
• Hold webinars for the R&E community

We need:

• 25 VM's for production (87 in total, including test and staging, management VMs etc)
• 5 employees
Technologies used

- PHP
- Java
- MariaDB
- MongoDB
- Haproxy
- Docker
No worries!

- OpenConext runs on one VM
- Start small
- If you use OpenConext, we provide helpful support via our Slack workspace
- We are transitioning to Docker, ensuring OS independence
**SURFconext: the future**

**eduID**
- Now: guest IdP
- Future: account for education and research in the Netherlands

**SURFconext**
- SP proxy for eduID
- Enhanced integration options for SPs and IdPs
- Authorisation

**SURFconext is the enabler for the transition to eduID and wallets**