Maarten Kremers, SURF
REFEDS #47, Stockholm,
11 October 2023
Team Trust & Identity @SURF

Team trust & identity
- Operations of trust & identity services
- Exploring and building new solutions and services

Our services
- SURFconext
- SURFsecureID
- SURFresearch access management
- eduID
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
VERTAALDIAGONAAL

**SURFconext Invite**

SURF is improving access control for our institutes with SURFconext invite.

- An inviter adds roles to specific individuals (also in batches) to determine which applications a user can access.
- Adds end dates for automated removal of roles and user information.
- The institute determines role names, period of validity, etc. Themselves.
- Provisioning to institutional applications based on SCIM protocol.
- Reduces security and privacy risks.
- Invite merges with one of our previous access services to avoid increase in complexity.
SURFsecureID

- Added SSO on 2nd factor. Momentarily with session duration of 24 hours. SSO can be enabled per application.
- Added self asserted tokens with a new Level-of-Assurance. Users can now self-register a 2nd factor instead of registering one at a servicedesk with ID verification. During registration, adding a recovery method like SMS or recoverycode is required.
- Updated tiqr mobile apps.
### SURFsecureID levels-of-assurance

1. **Basic – with MFA**
   - Level: 0
   - Description: Institution username and password is 1st factor

2. **Basic**
   - Level: 1.5
   - Description: Basic plus a self-registered 2nd factor. Suitable to prevent abuse.

3. **Medium – with MFA and ID verification**
   - Level: 2
   - Description: The institution checks the identity of the user before the 2nd factor can be used. Suitable when more certainty of identity is required.

4. **High – with hardware 2nd factor and ID verification**
   - Level: 3
   - Description: Identity check and extra secure 2nd factor (USB keys). Highest level of reliability and protection against misuse.

The institution checks the identity of the user before the 2nd factor can be used. Suitable when more certainty of identity is required.
**eduID**

- Added passwordless login with eduID mobile app. Developed based on the existing tiqr app.
- Updated eduID mobile app with all profile management functions.
- Growth of 20K users in 2022 to 50K now. 150K logins ytd 2023. 150 apps connected to eduID IDP.
- Expanded eduXchange.nl student mobility project to 6 universities. Now has 11K eduID users.
- Many discussions with Microsoft about eduID access to MS365 apps. No green light yet.
- Researched ID verification options. Going for Dutch bank ID (iDIN) and eIDAS.
Future plans for SRAM

Some ideas from our roadmap

• Containerise SRAM (follow SURFconext)
• Enhance automatic testing
• Wanted: better support for MFA in eduGAIN
• Offer SBS to other NREN’s/communities?
• AARC TREE
• Token based access/authorisation
• Offer (basic) collaboration tools?

Towards an integrated service

• SURF members confused about differences with SURFconext
• Overlap with SURFconext (invite tool, SURFconext Teams, Authorisation Rules)

Also: 1 researcher identity?

• eduID?
What’s next?

Self Sovereign Identity (SSI)
- Participate in DC4EU (Large Scale Pilot)
- Explore emerging standards (OpenID4VCI / OpenID4VCP)
- Experiment with Wallet technology to gather sector requirements

Higher Education Sector Architecture (HOSA)
- Three parts: Flexible Education / Research Data / Identity & Access
- Identity & Access: mostly based on SSI-principles. Q: How to transform the sector?
- NPULS programme: Collaborating to improve the quality and the agility of education system, and to enhance the digital skills of lecturers and learners.

Support European University Alliances
- Complicated. AuthN via eduGAIN not enough, more complex services needed (including authZ and provisioning). Preferably ‘as a service’ and at ‘international scale’
eduID
An eduID is an account for users within Dutch education and research. It belongs to you and exists independently of an educational institution.

SURFconext + research access + secureID
Ensuring that institutions, research groups and services can provide easy and reliable access to students, staff and anyone who needs access.

- SP proxy for eduID
- Enhanced integration options for SPs and IdPs
- Authorisation
- SURFconext is the enabler for the transition to eduID and wallets