

SURF

# SURFconext

REFEDS and eduGAIN webinars  
on H&S federations



# Agenda

**01**

Introduction

**02**

Hub & spoke

**04**

IdP perspective

**06**

Providers perspective

**03**

User  
perspective

4 demos

**05**

SP perspective

**07**

OpenConext

**08**

What do you need?

# Team Trust & Identity @SURF

## Team trust & identity development

- Exploring and building new solutions and services

## Team trust & identity operations

- Operations of trust & identity services

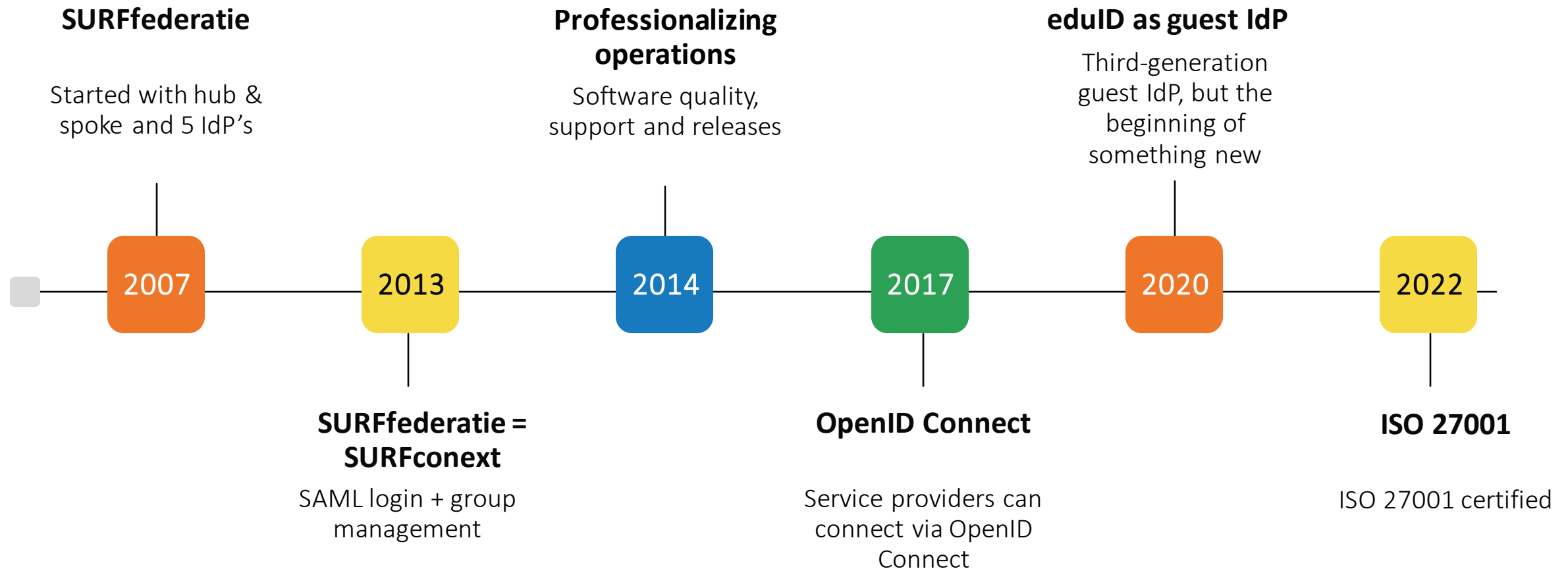
## Our services

- SURFconext
- SURFsecureID
- SURFresearch access management
- eduID

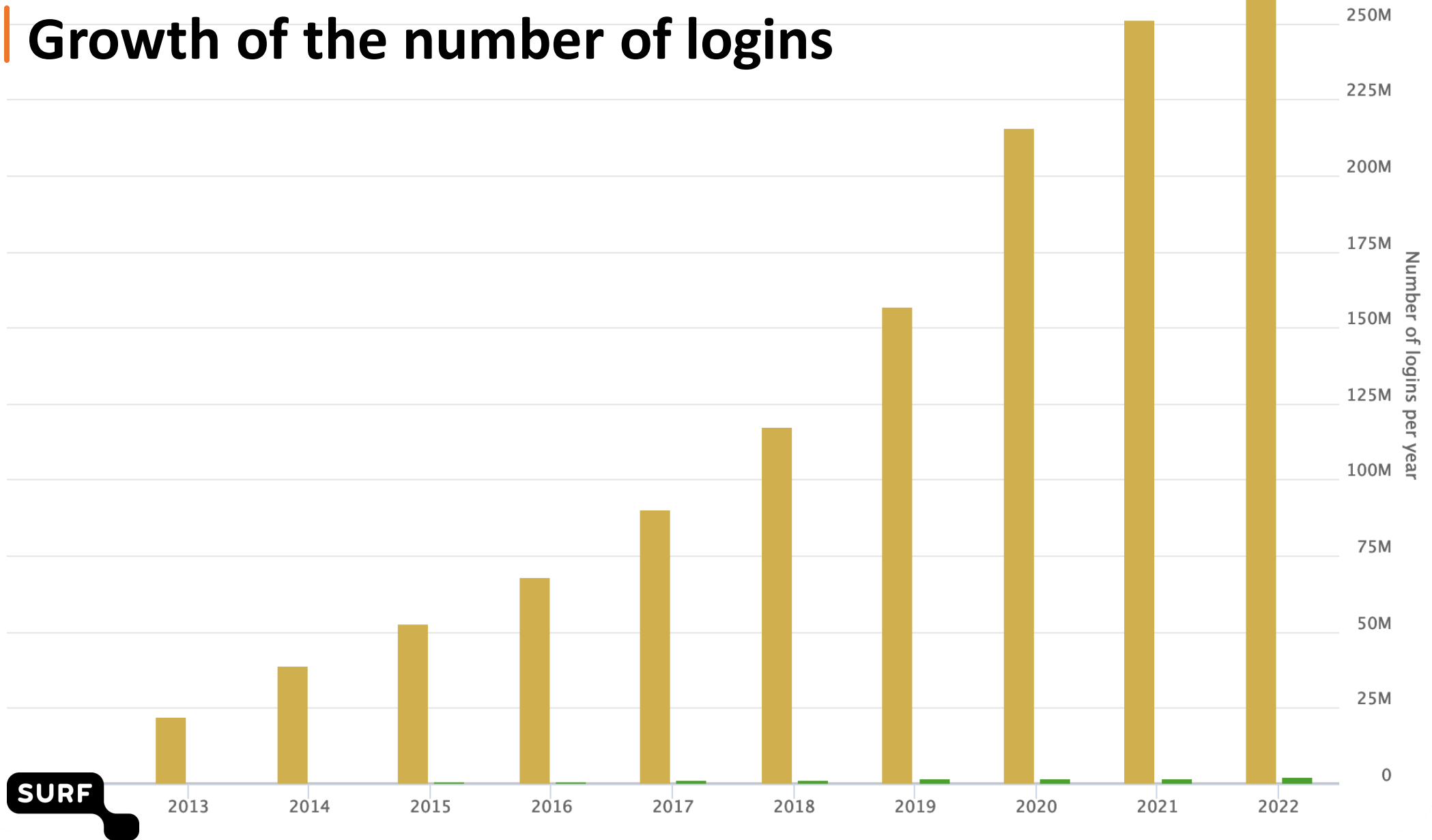
**SURF**



# A brief history lesson

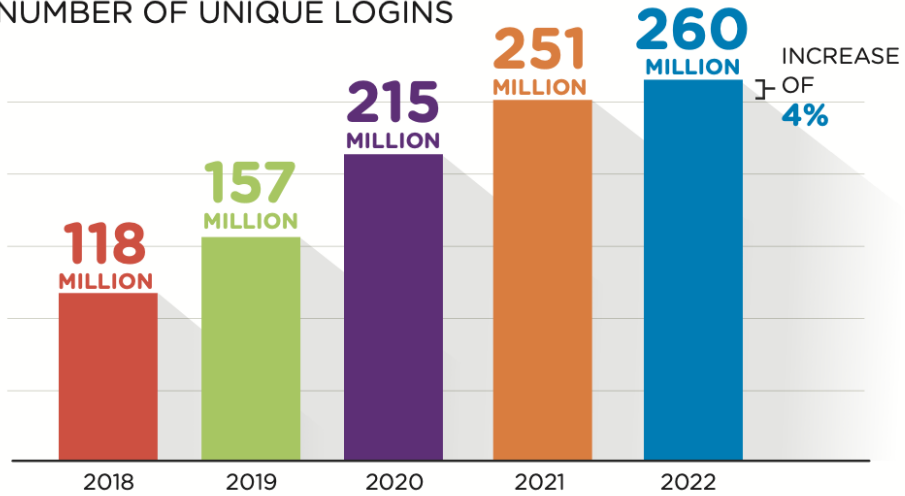


# Growth of the number of logins

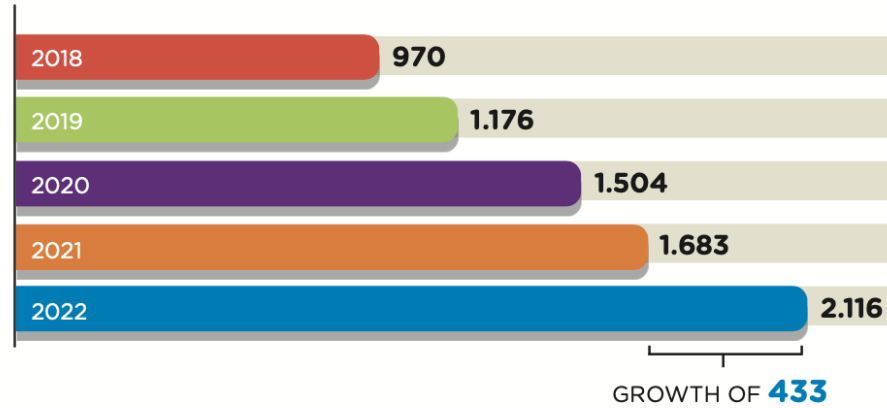


# MORE THAN 260 MILLION LOGINS WITH SURFCONEXT IN 2022

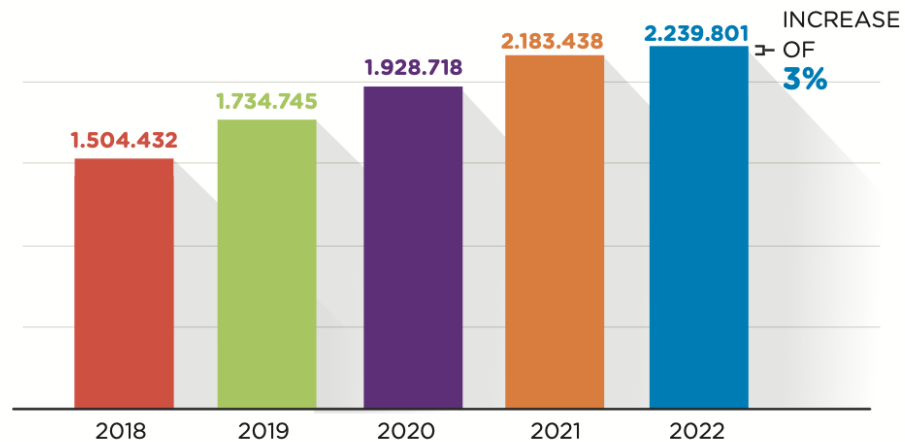
NUMBER OF UNIQUE LOGINS



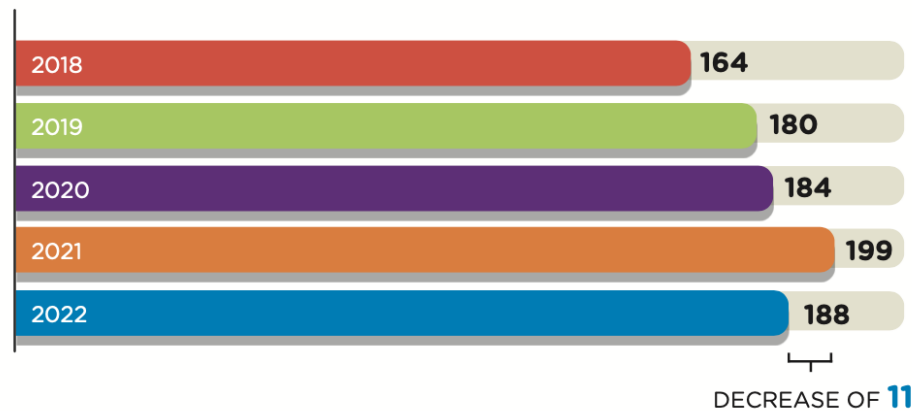
NUMBER OF SERVICE PROVIDERS



NUMBER OF UNIQUE USERS



NUMBER OF IDENTITY PROVIDERS



# | Why hub & spoke?

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



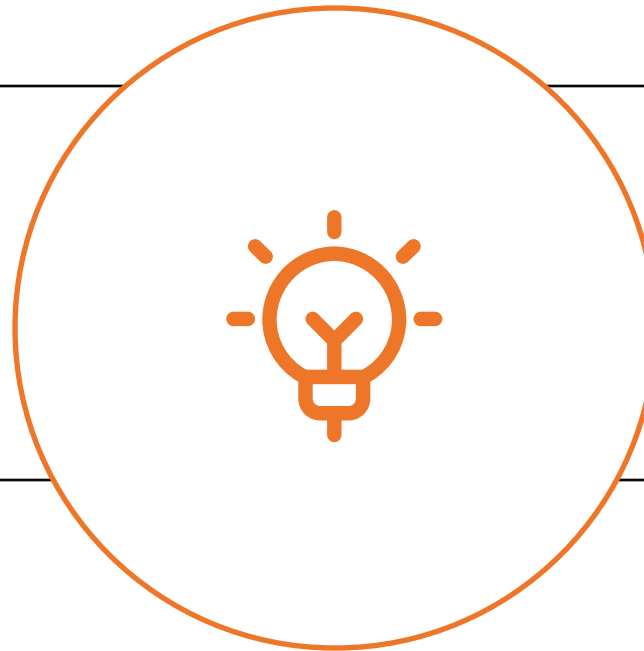
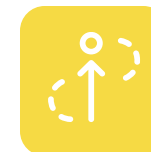
**Flexibility**  
Allows fast development and supports institution's choices (e.g., Microsoft) centrally, streamlining new developments like eduID.



**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

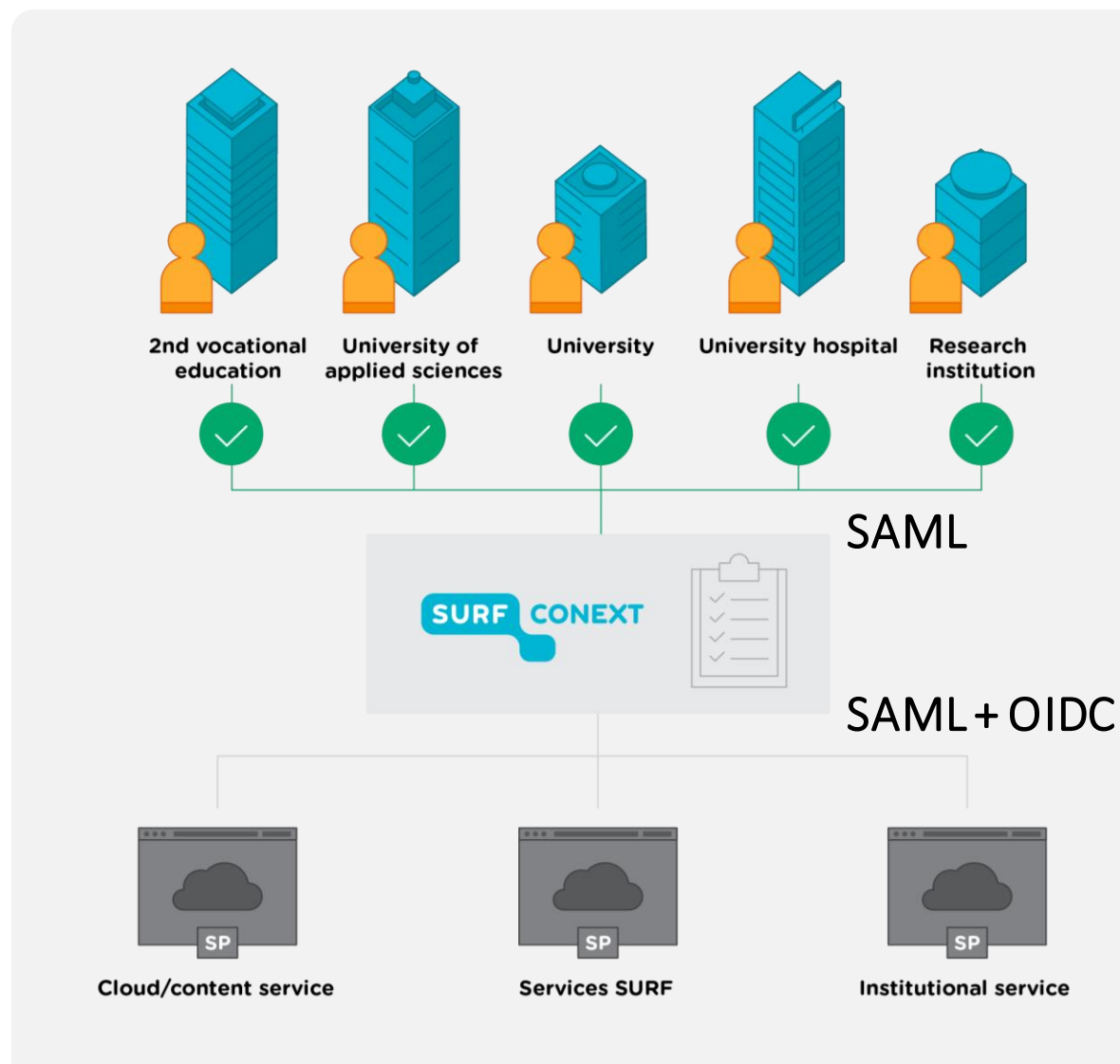


# Hub & spoke

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

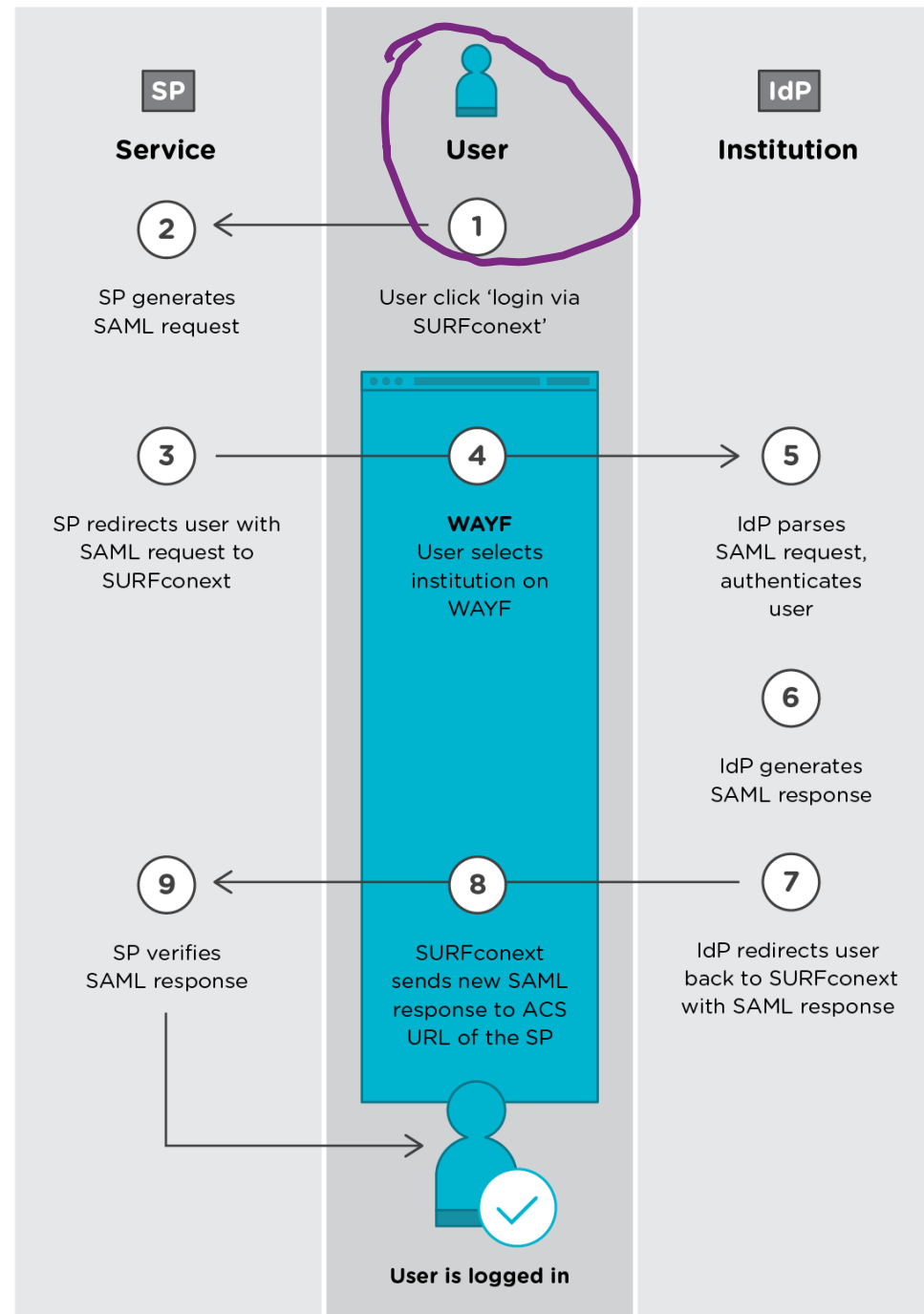
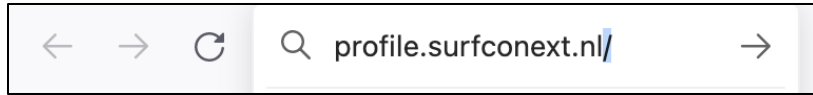
## Only one connection

- Trust is organized centrally
- Extra features: stats, dashboards, strong authentication etc.

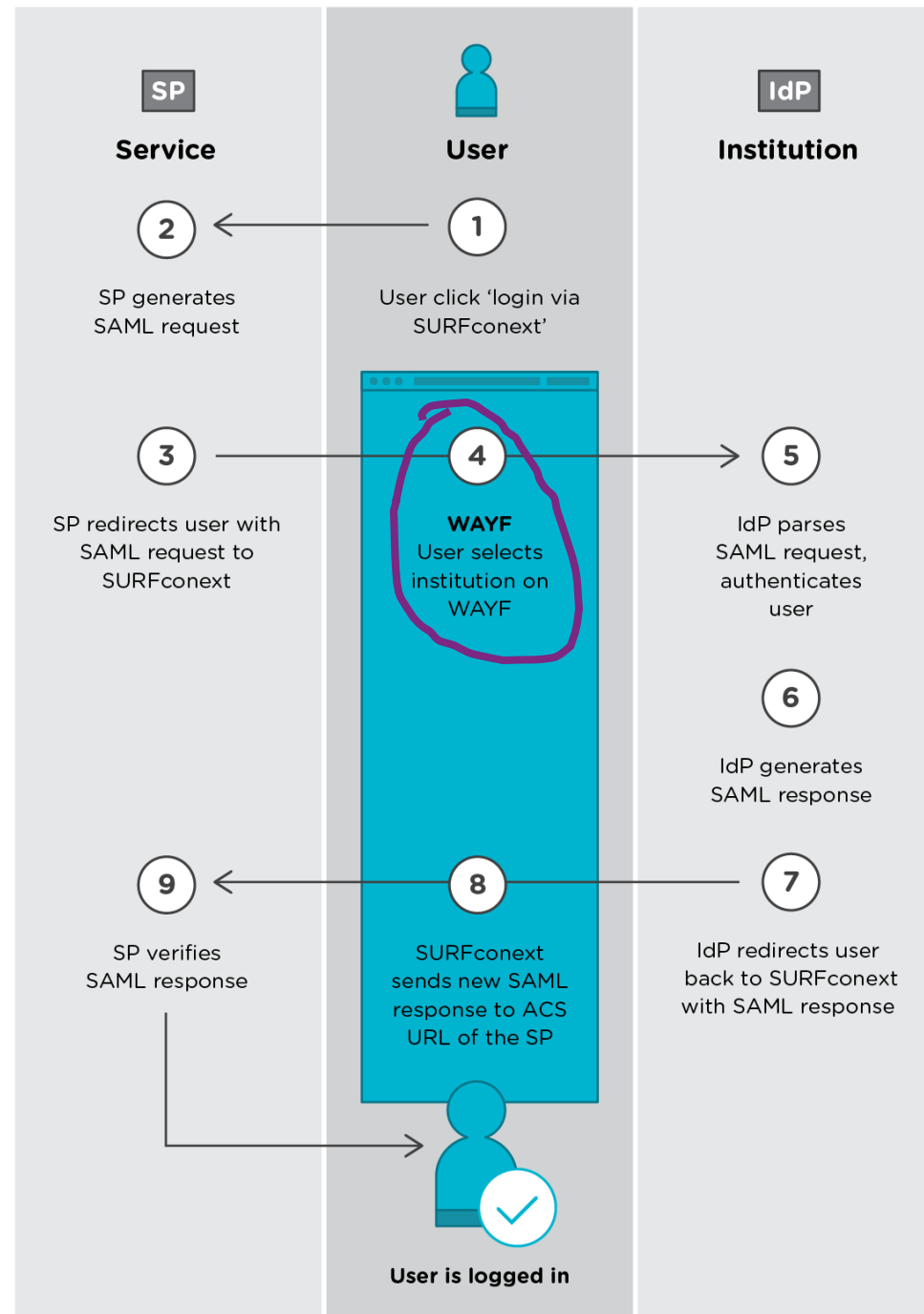
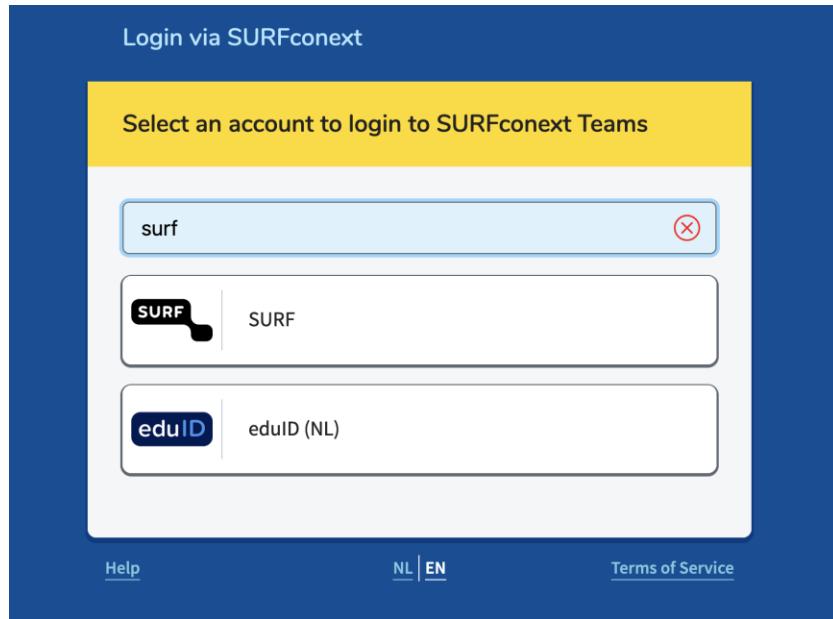




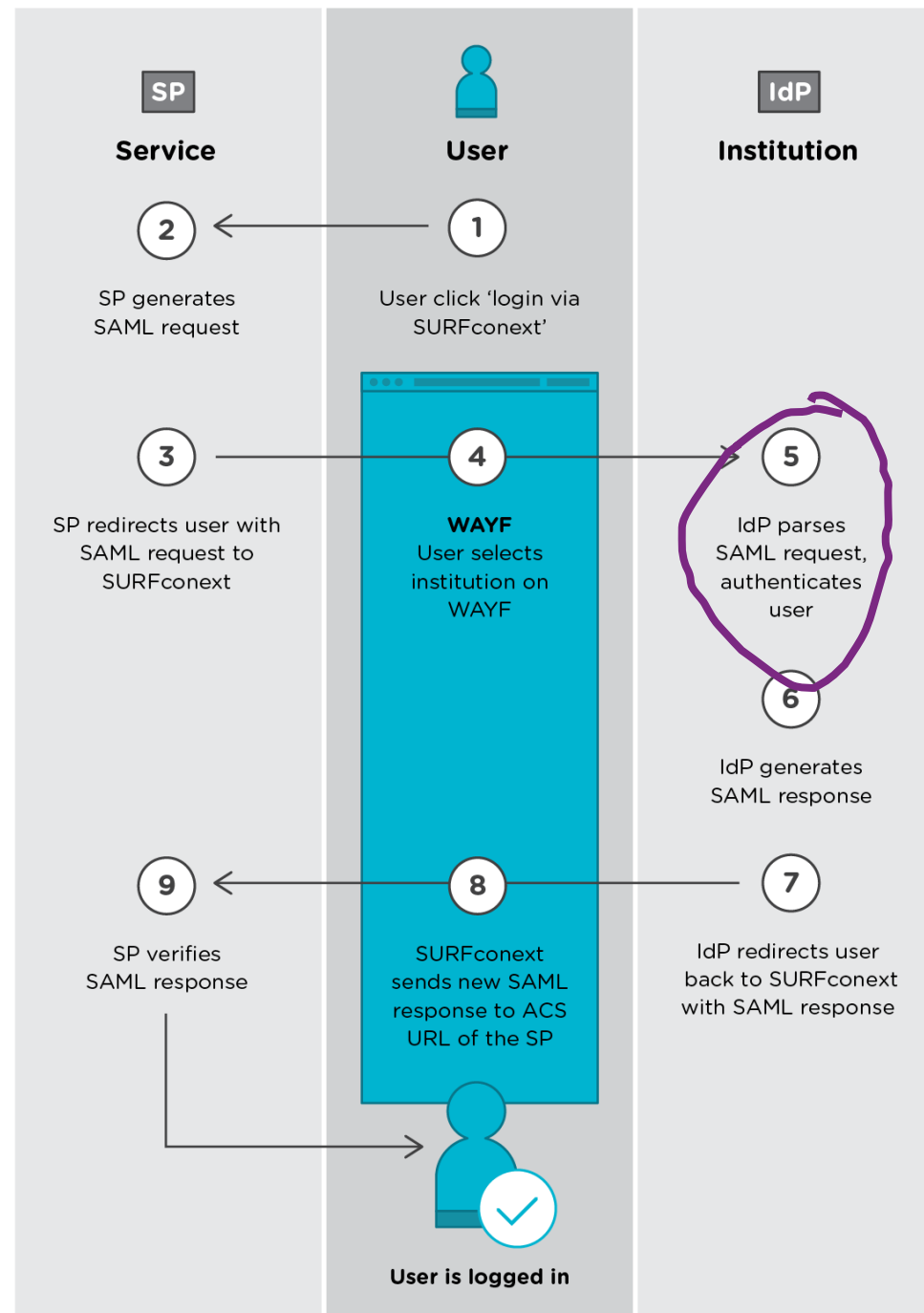
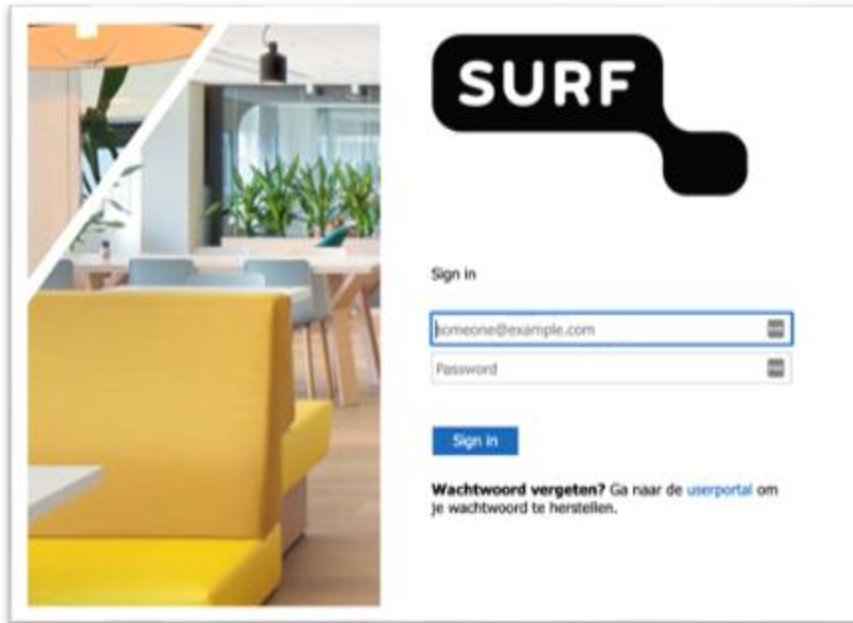
# Authentication flow SURFconext (SAML)



# Authentication flow SURFconext (SAML)



# Authentication flow SURFconext (SAML)



# Authentication flow SURFconext (SAML)


Login via SURFconext TEST

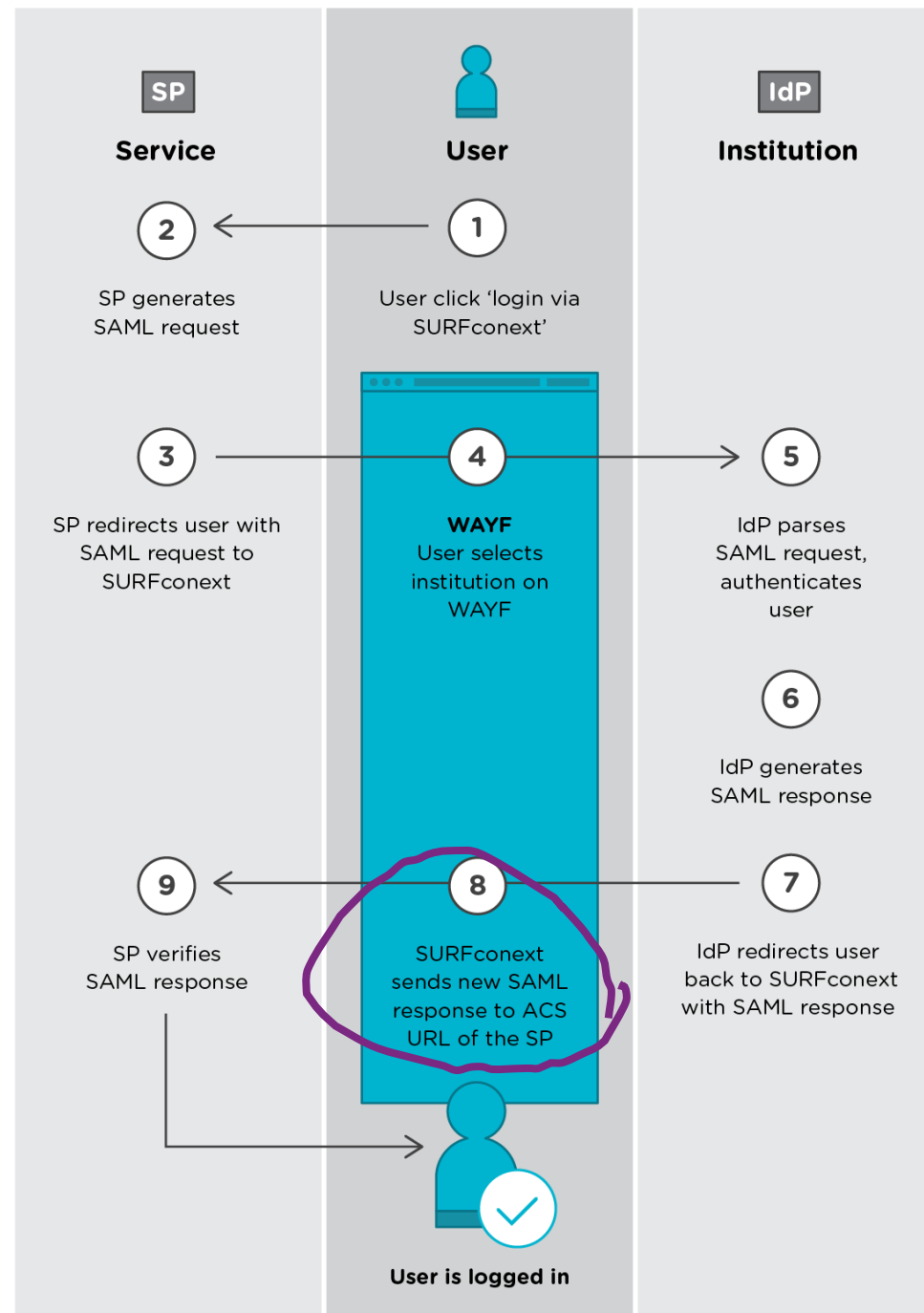
Review your information that will be shared.

**SURFconext Profile will receive**

Display Name	Femke Morsch
Full Name	Femke Morsch
First name	Femke
Surname	Morsch
Email address	femke.morsch@surf.nl

[Show more information](#) ▾

 provided by SURF (New) [Something incorrect?](#)



# | Demo Profile

SURF

# | 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

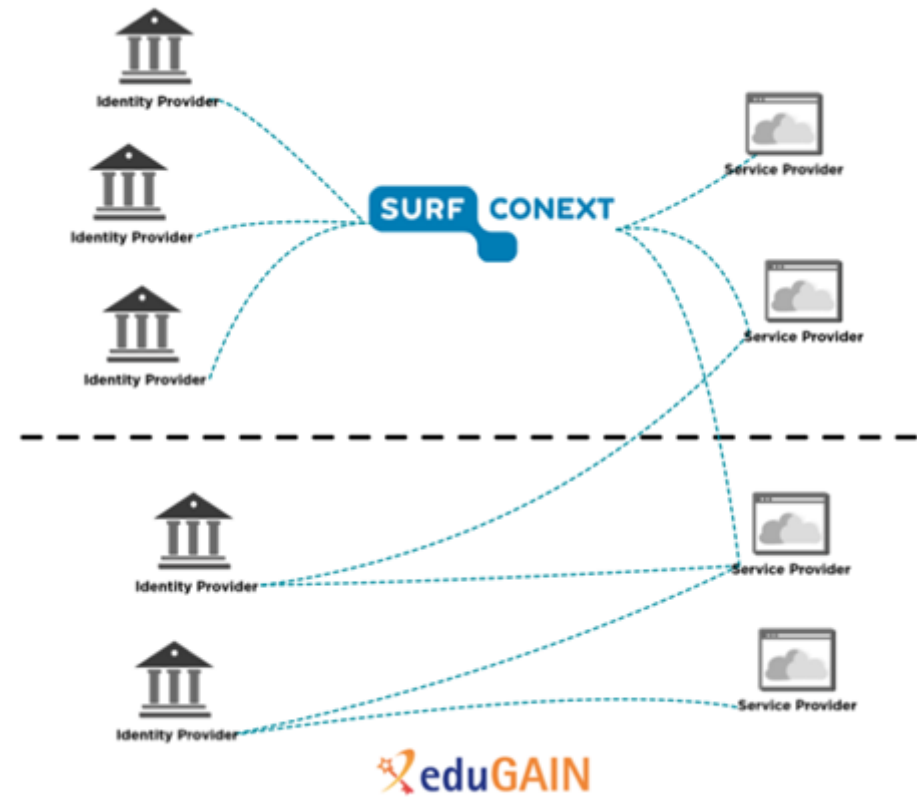
#	%	Product
101	46%	MS ADFS
86	39%	MS Azure AD
20	9%	SimpleSAMLphp
5	2%	NetIQ AM
3	1%	Shibboleth
2	1%	Google Workspace
1	0%	eduID
1	0%	OpenSSO / Oracle AM / OpenAM
1	0%	VMware Identity Manager

# | 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:20230503/583ece5a5636f8ee068742c66dfc1cd5>



# | 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.

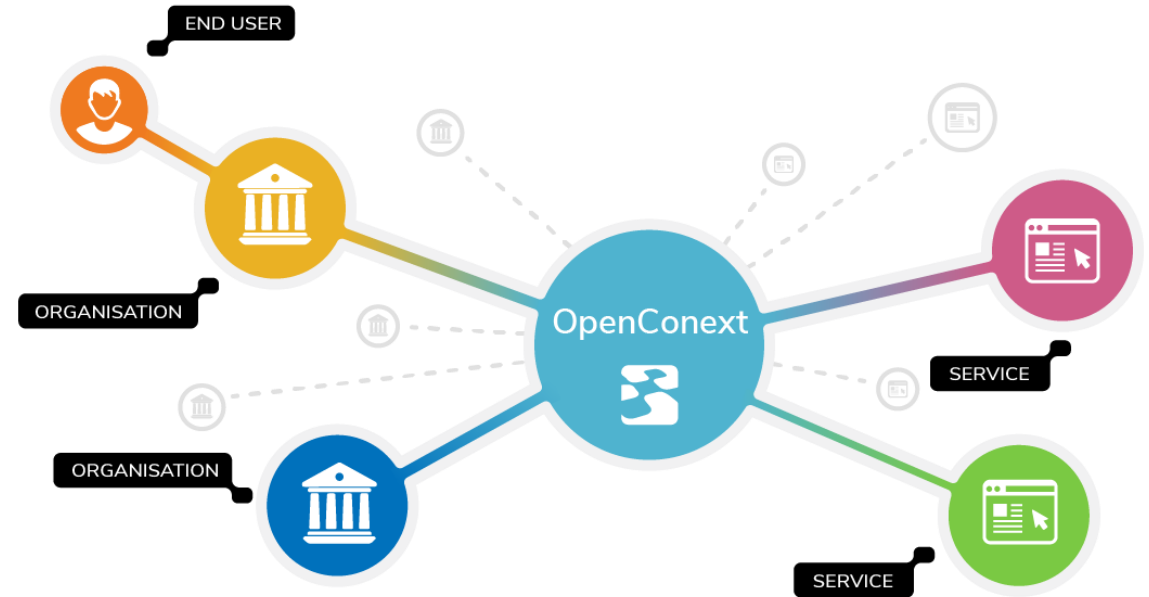


# | Demo Manage

SURF

# | 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



# OpenConext

OpenConext

Search: Type ↵ to search

Overview Repositories 54 Projects 1 Packages Teams 4 People 27 Settings

Find a repository... Type Language Sort New repository

- Openconext-Access** Public  
Java Apache-2.0 0 stars 0 forks 0 issues Updated 30 minutes ago
- Stepup-API** Public  
Application Programming Interface for OpenConext-Stepup  
PHP Apache-2.0 0 stars 2 forks 2 issues Updated 1 hour ago
- OpenConext-devconf** Public  
Contains configuration file to get an development environment up and running  
Shell Apache-2.0 0 stars 0 forks 2 issues Updated 1 hour ago
- OpenConext-attribute-aggregation** Public  
OpenConext attribute aggregation  
Java Apache-2.0 1 star 2 forks 3 issues Updated 2 hours ago
- OpenConext-deploy** Public  
Ansible-based deployment automation for the OpenConext platform  
tags: `deploy` `openconext` `ansible`





# OpenConnext



Rijksoverheid



# ENTREE federatie





OpenConext.org

SURF

# | 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

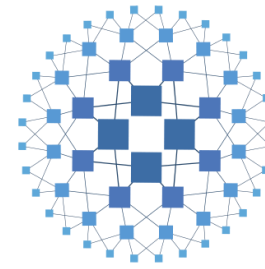
## We need:

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



# | Technologies used

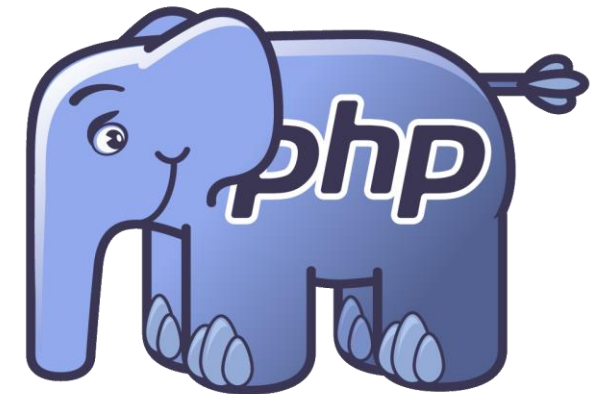
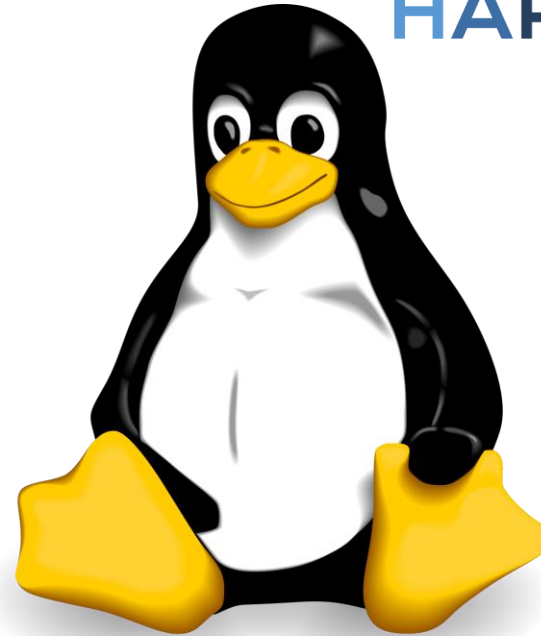
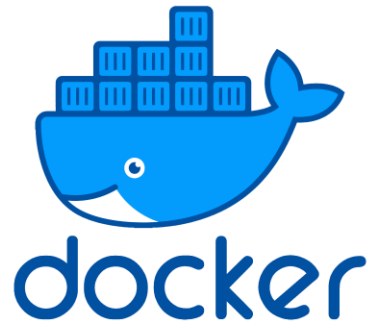
- PHP
- Java
- MariaDB
- MongoDB
- Haproxy
- Docker



HAPROXY



mongoDB



# | 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



The screenshot shows the 'eduID' user interface. At the top left is the 'eduID' logo, and at the top right is a 'Logout' button. A left-hand navigation menu includes 'Home', 'Personal info', 'Data & activity', 'Security' (highlighted in green), and 'Account'. The main content area is titled 'Security settings' and contains the following sections:

- Security settings:** A heading followed by the text 'We provide different methods to sign in to your eduID account.' Below this is a promotional card for the 'eduID app' with the text 'Want to sign in quicker and more secure next time?' and 'Get the eduID app and securely sign in without passwords or accessing your email.' A blue 'Get it now' button is at the bottom of the card. An illustration of a smartphone and a person is on the right.
- Other sign-in methods:** A list of methods with edit icons:
  - Send magic link to: femkemorsch@ [redacted]
  - Password: [redacted]
  - Security key 1: Iphone nieuw (with a 'Test' button)
- Add security key:** A blue button with the text 'Add security key'. Below it is explanatory text: 'You can add security keys to your eduID account which can be used to login. You can use, for example, the built-in sensor of your device (TouchID, FaceID) or a separate hardware key (YubiKey).'
- Sign-in settings:** A section with a checked checkbox for 'Stay logged in' and the text 'Your device is currently remembered. You will be automatically logged in to eduID.' A blue 'Forget me' button is on the right.

| ?????

**SURF**

[surfconext.nl](https://surfconext.nl)  
[openconext.org](https://openconext.org)