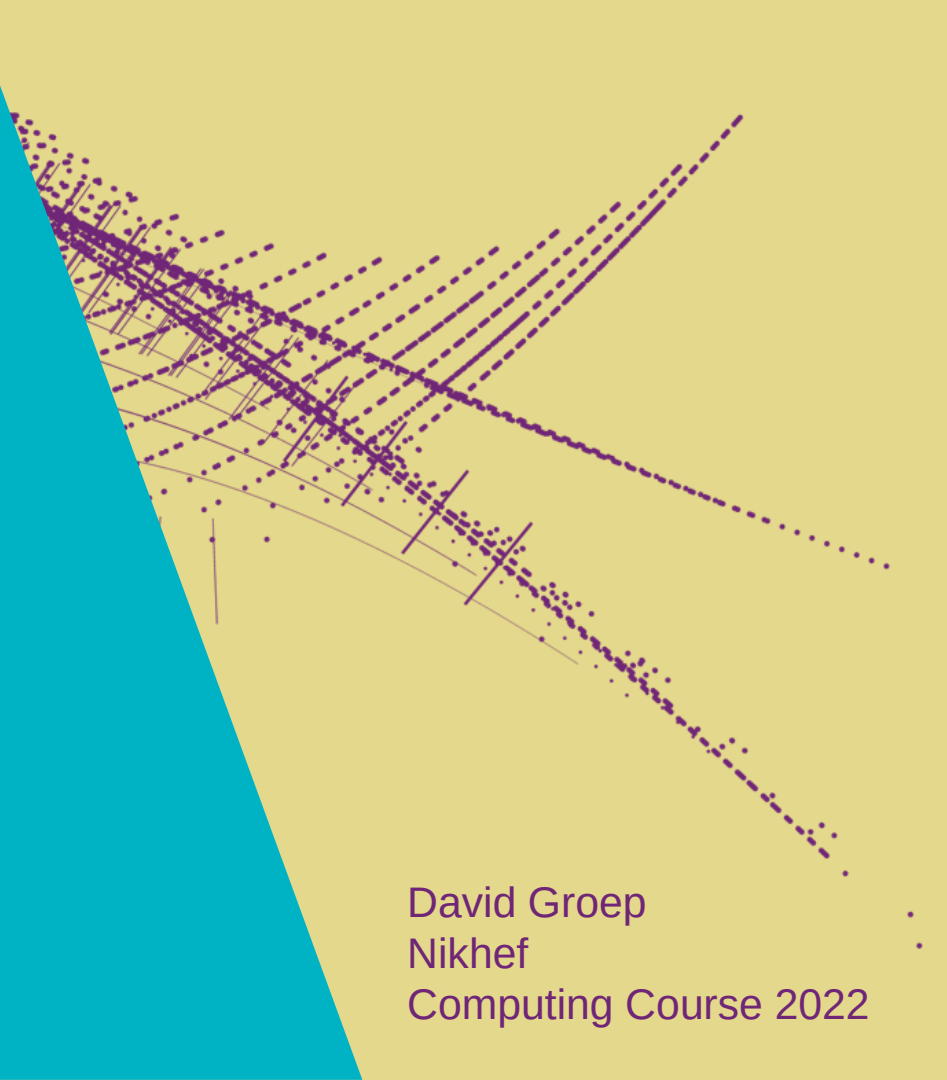
Nikhef

Maastricht University

how to work together

You, your laptop, and somebody else

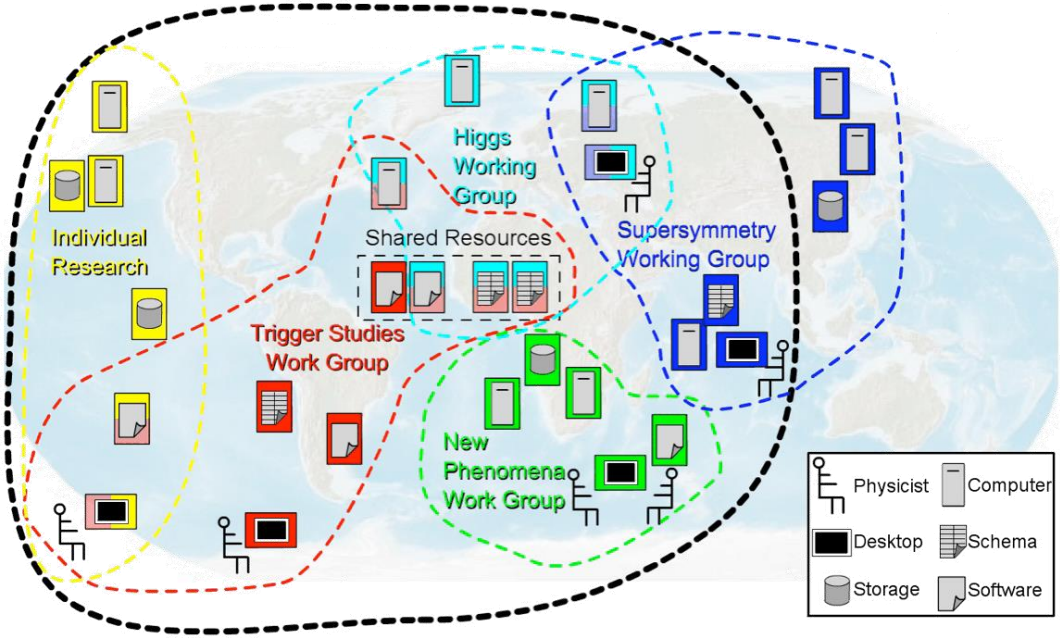


David Groep
Nikhef
Computing Course 2022

Objectives for this session

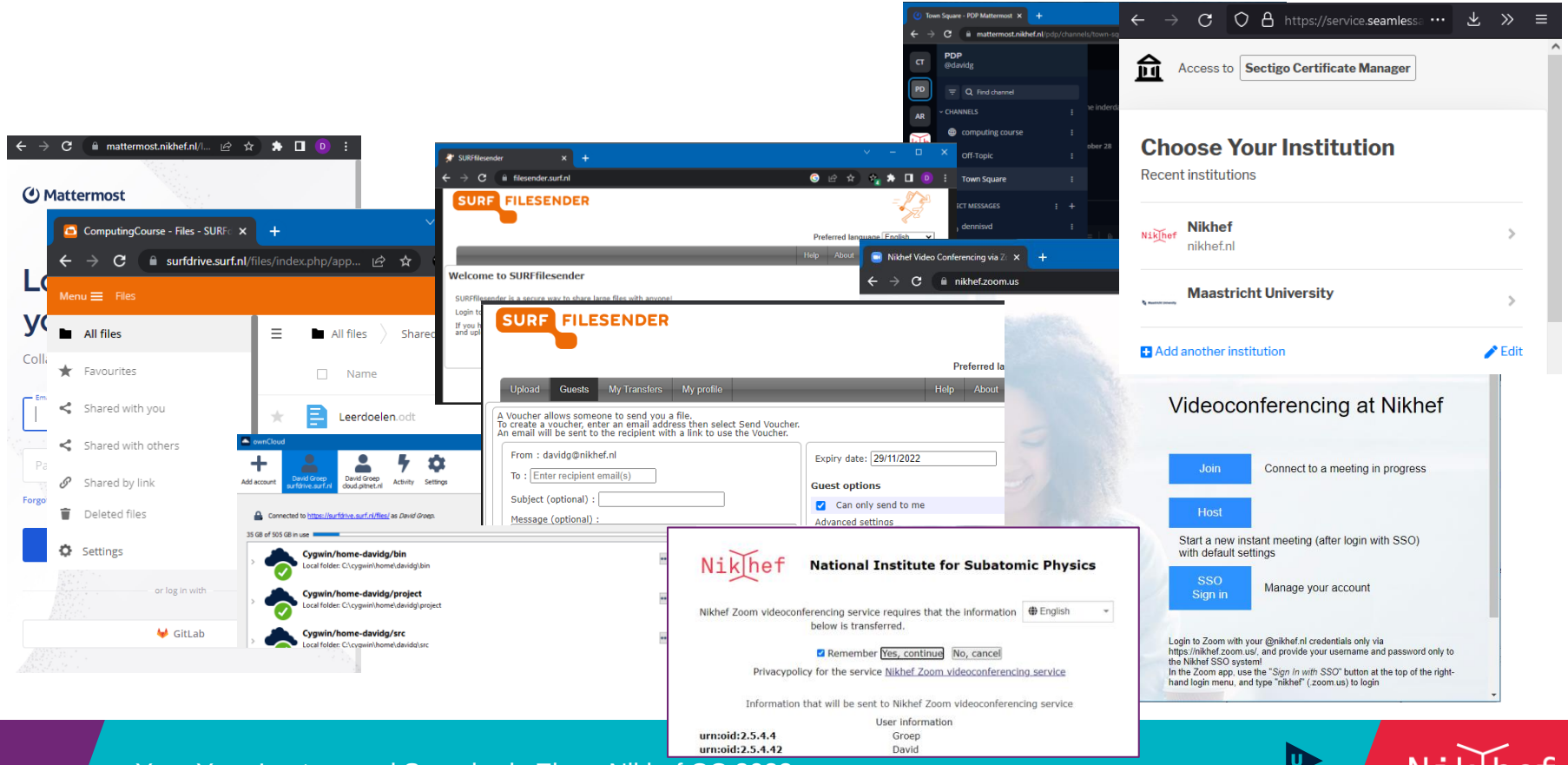
- Know how to send big files: Surf File Sender
- Know how to find and use SurfDrive and CernBox
- Understand which services are safe to use and which are not
- Know how to use Identity Services & Federated Login
- Know how to use Zoom and Mattermost

Actual collaborations



Left image source: GGF 2003, by way of Ruth Pordes: Paradyn and Condor Week 2004; Photo on the right by Valiant Made on Unsplash

Services for collaboration

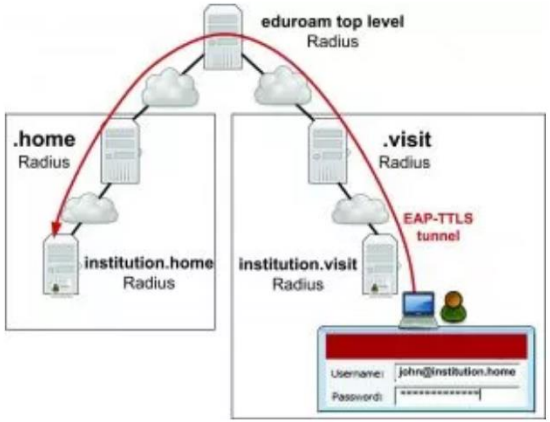


The most simple service to get out of your laptop

Global WiFi access for research & education

- same SSID everywhere
- same authentication method (802.1x + EAP)
- your name and password are never revealed to the visited site, only to Nikhef
- Through an encypted tunnel (TTLS) to send your credentials (PAP), or asymmetric authentication with certificates (TLS)

Do you also have a UvA account? Login to eduroam using Nikhef credentials or use the “NIKHEF” network – otherwise you cannot print here (but your printing will go to the UvA



Many places: all Dutch R&E sites, a private home in Utrecht, Geneva airport, all bus stops in Poznan, Australia, UNLP La Plata …

eduroam: Klaas Wieringa et al., image from https://eduroam.org/how/, GEANT ; use the eduroam CAT tool, the Nikhef helper app, or go to https://wiki.nikhef.nl/ct/Eduroam

Federated Authentication and Authorization Infrastructure

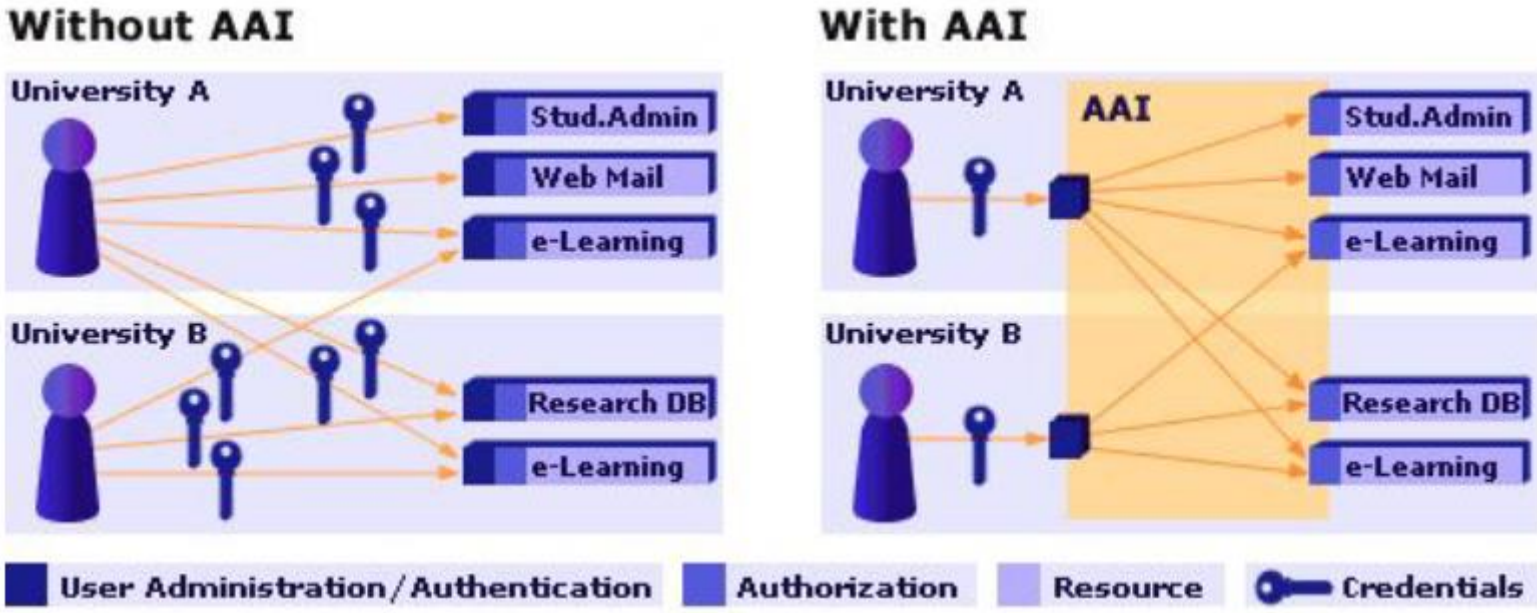
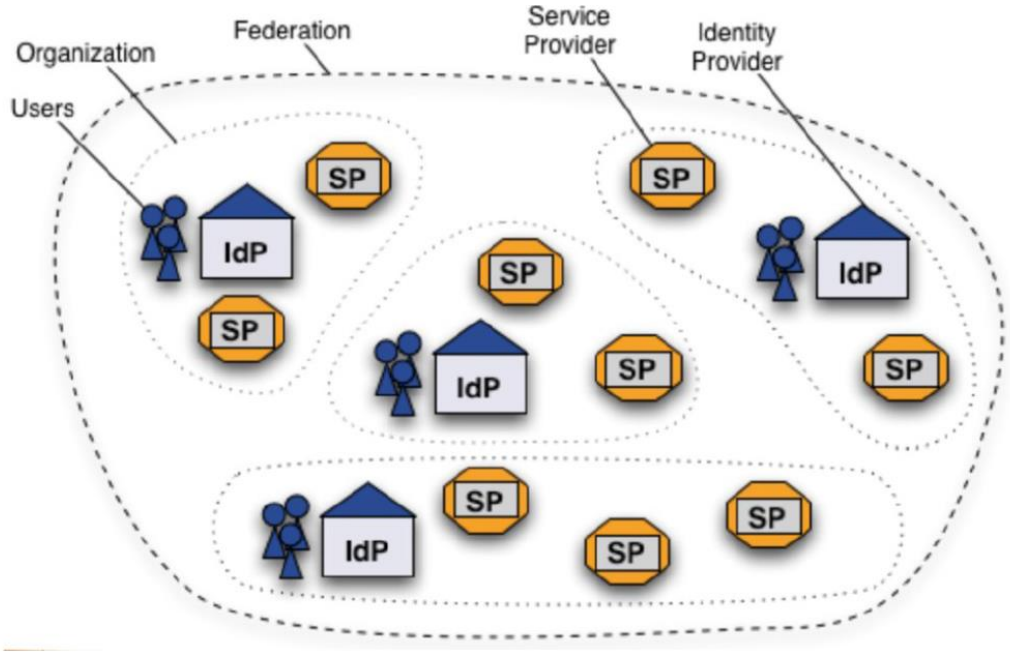


Image: AARC NA2 training module “Authentication and Authorisation 101” - https://aarc-community.org/training/aai-101/

Many organisations



Shibboleth IdP image and SAML2 auth flow by SWITCH (CH)

Federated identity - SURFconext

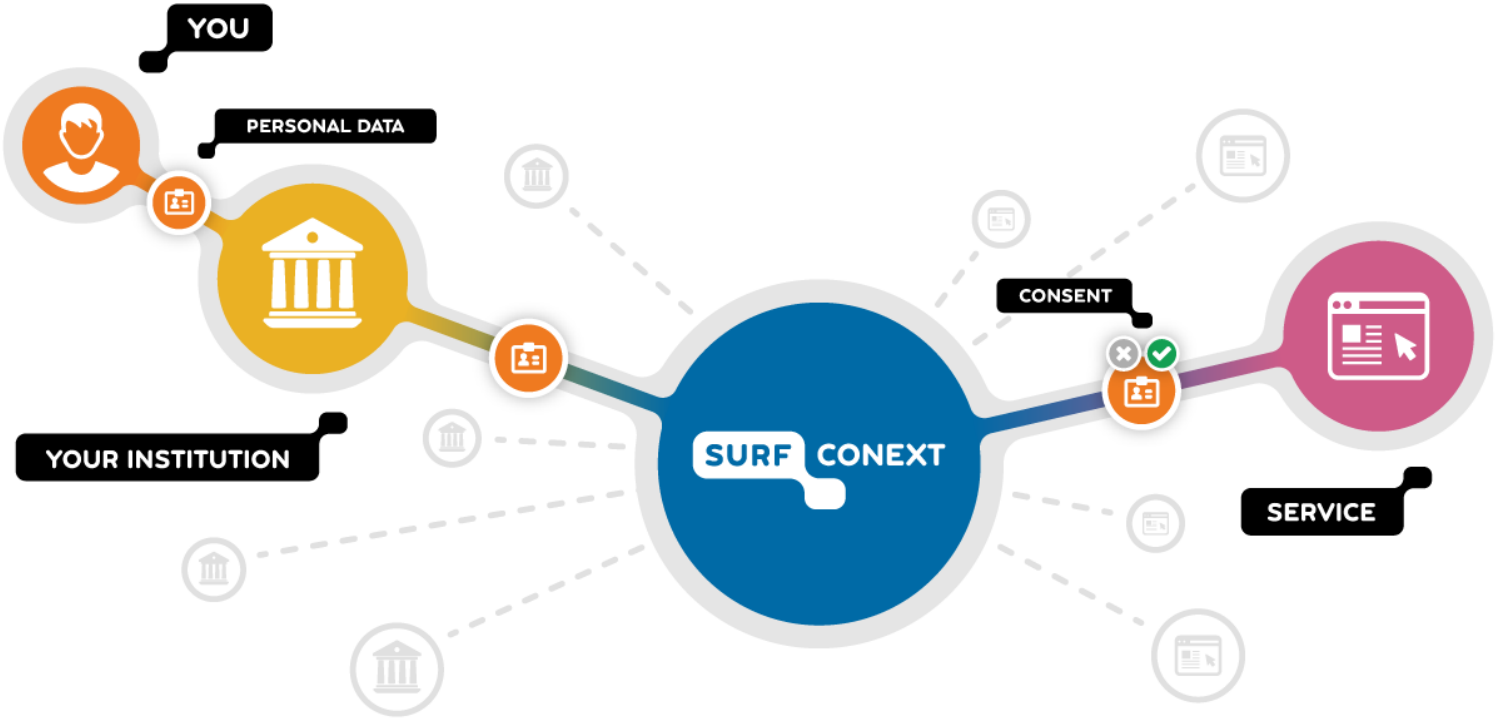


Image: SURFconext dashboard, https://profile.surfconext.nl/

Authentication – who are you

To a single system or service relatively simple

- per-system identity (username) and secrets (e.g. password or TOTP token)
- server-side: list of valid users and (salted and hashed) secrets

```
[root@kwark ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
root:$6$s8ciAG5gLuv2bPQS$6EcskgtKvQ.rHb
davidg:$6$nDYcIez2Uaufbtlg$R1hS/Qjn0qYQ
marianne:$6$p3CeevG6jfNDqZj1$HKHqUTnt2fEqQrkA/m5J3OAOA02SvgLCKOSQhPS
```

Passport image: cropped from original by Jon Tyson on Unsplash https://unsplash.com/photos/Hid-yhommOg

Authorization: what you are allowed to do

- you may need to ‘collect’ assertions
  bound to your identity to gain access to services
- like visa, bound to your entity through either Nikhef, or
- a community attribute authority (VOMS, IAM Proxy, …)

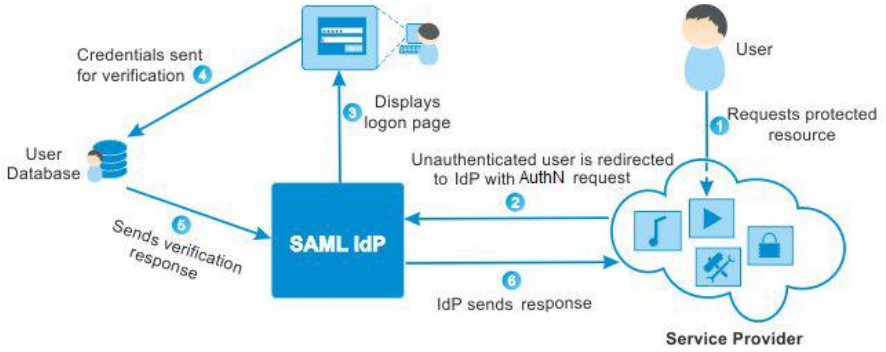
- in the collaboration cases here
  the assertions you collect
  from the Nikhef Identity Provider (‘SSO’) are enough

- Service provider ultimately determines access
- although some have a very ‘open’ policy, like we do for eduroam network access

USA visa image source: https://2009-2017.state.gov/m/ds/rls/rpt/79785.htm

SAML federation and Nikhef SSO

Attributes	Values
E-mail	davidg@nikhef.nl
Affiliation	• employee • member • faculty
Targeted ID	https://sso.nikhef.nl/sso/saml2/idp/metadata.php!https://attribute-viewer.aai.switch.ch/shibboleth!b9f858169ea28dc68b6753baa1084d8c039e36a7
Common Name	David Groep
Display Name	David Groep
Principal Name	davidg@nikhef.nl
Home organization (international)	nikhef.nl
Home organization type (international)	urn:mace:terena.org:schac:homeOrganizationType:int:other



"SAML2.0" login flow

Try at https://attribute-viewer.nikhef.nl/

SAML WebSSO flow image: SWITCH, CH

Not all services are created equal

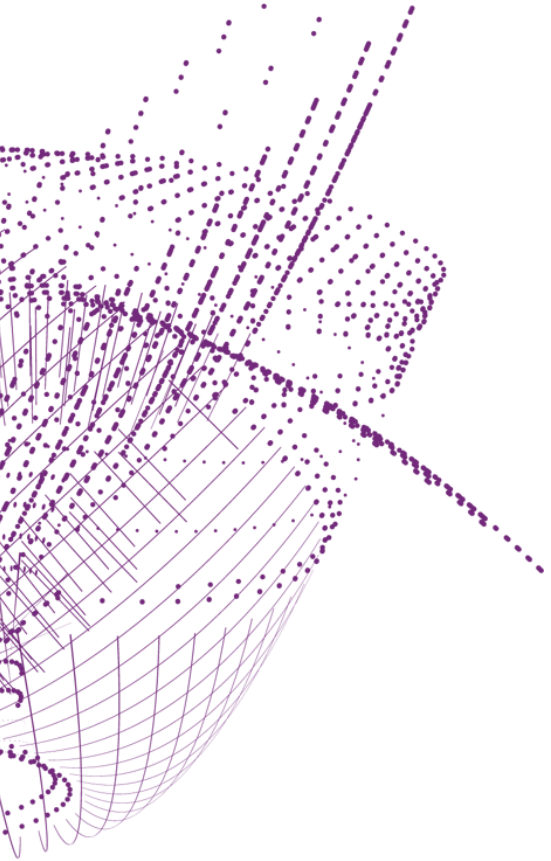
Although you may not think about it all the time …

- your personal data is sensitive (and can be used for identity theft)
- the data you store and share can also be sensitive
  - your appraisals and C3 documents should probably not be world-readable by a random ‘free’, ‘cloud’ provider- not should your email (since you mail those documents)
  - Nikhef data can be sensitive as well: we got it under ‘non disclosure agreements’ from suppliers, or work with industry (e.g. in Detector R&D)
  - Or can be dual-use (even if you don’t realise it)

So, while you collaborate freely:

- never, ever, put your Nikhef password in another service than @Nikhef (that’s why we have federation)
- use Nikhef-endorsed services for sharing personal and sensitive data, which includes email
- we **want you to collaborate**, and **rely on your cooperation**

See https://wiki.nikhef.nl/nikhef/ctb/NikIDM/Services (accessible from within Nikhef and on eduVPN) for federated services and attribute release



‘I want to send a big file to Jane Doe’

FileSender

Sending larger files

Email is only for very small files

- order kilobytes (and less than 1MByte)
- only to one recipient – otherwise the size just multiplies
- and even then: how many times did you discover a mistake just after sending?

For sharing larger files

- SURF **FileSender**: trusted, and potentially encrypted, sending of large files
  - can be even a terabyte or so ☺
  - you can also issue vouchers so **others can upload files to you**

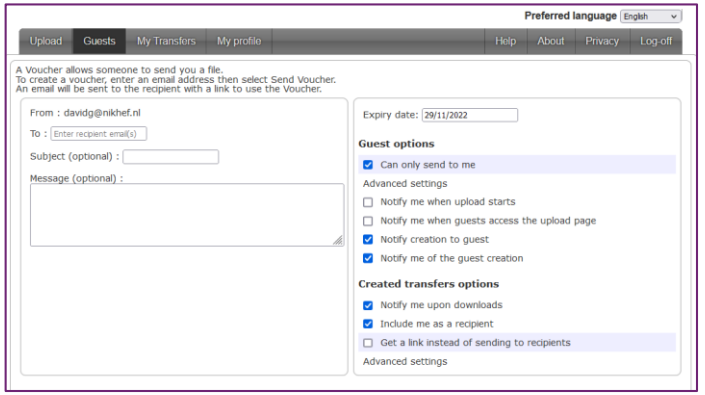
- **SURFdrive** (or **CERNbox**) sharing links
  - you can still update the documents after sending the mail
  - integrated in your sync-n-share environment
  - total file size up to 500 GByte

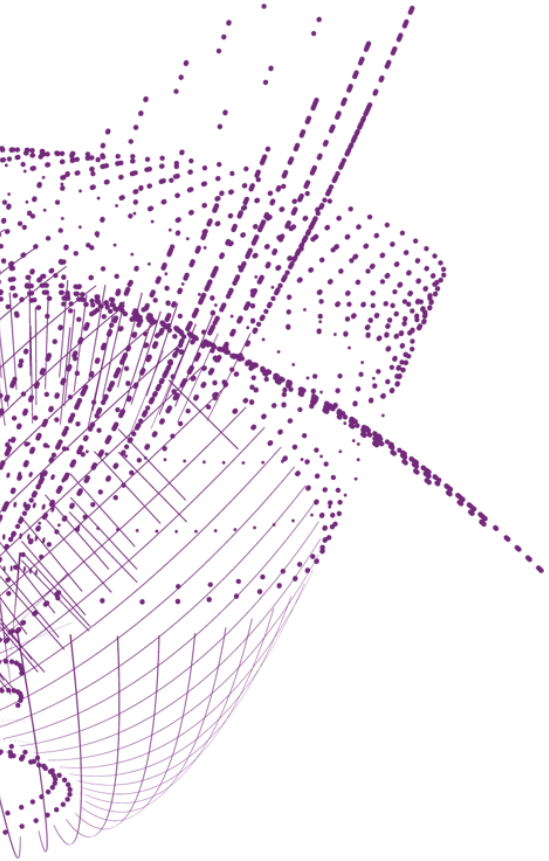
FileSender

https://filesender.surf.nl/

- Unlimited file size
- Federated login
- Download notification and statistics, overview of pending transfers
- Can send mail directly or give you a link
- 3 week download period, 2 months upload window

- Safe and private storage at SURF (Amsterdam)
- Transfers can be encrypted (send key out of band)
- Endorsed, trusted service (obviously ad-free)





Collaborative Sync & Share Services, a.k.a. ‘CS3’

SURFdrive and CERNbox

Collaborative Sync-and-Share Service (‘CS3’) for files

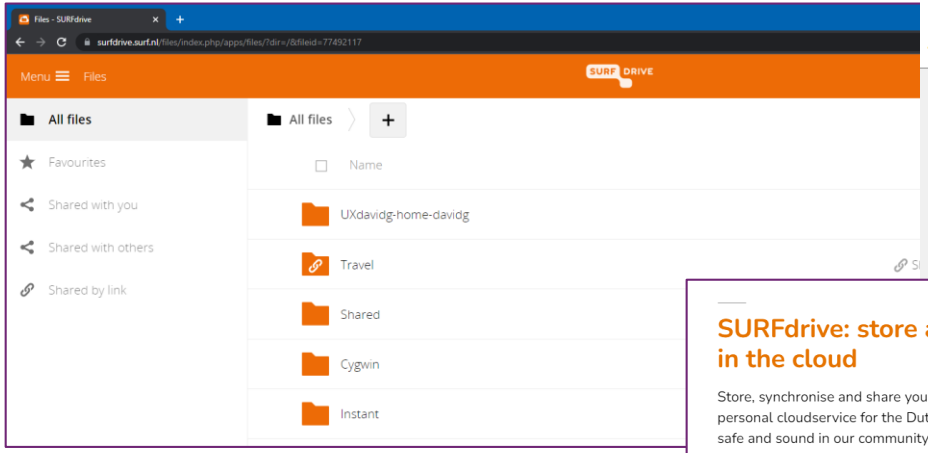
Sharing files and collaborative documents, results, papers, or your photos

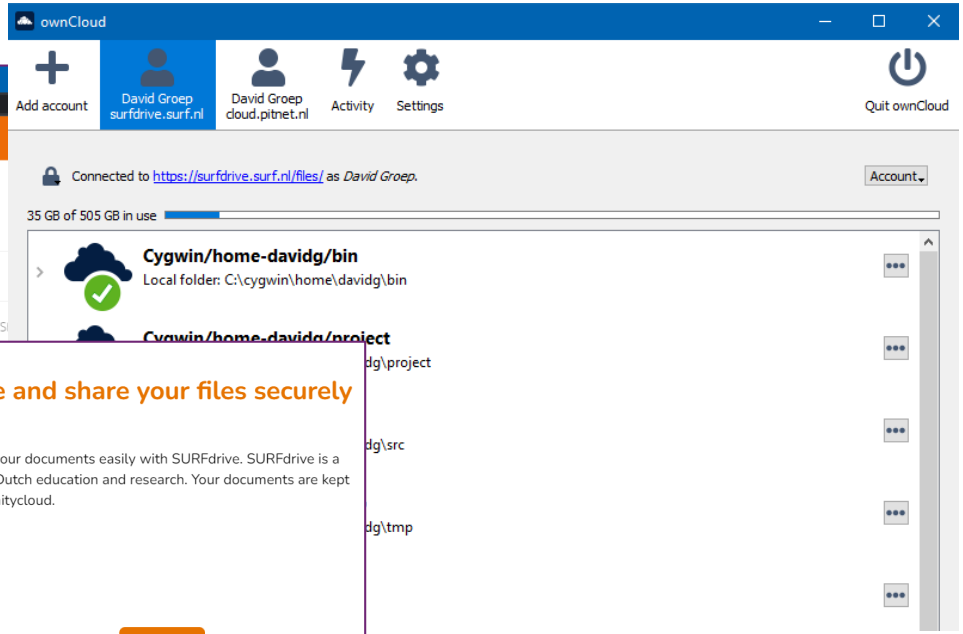
- SURFdrive (and CERNbox that uses the same technology)
- 500 GByte
- you can create project/group folders (but use wisely)
- share with people in NL universities and institutes, with invited guests, or fully public links for everyone else in the world
- collaborative editing using Collabra OpenOffice
- web-based and sync-client access
- not encrypted at rest (but the people at SURF are not looking at your data)

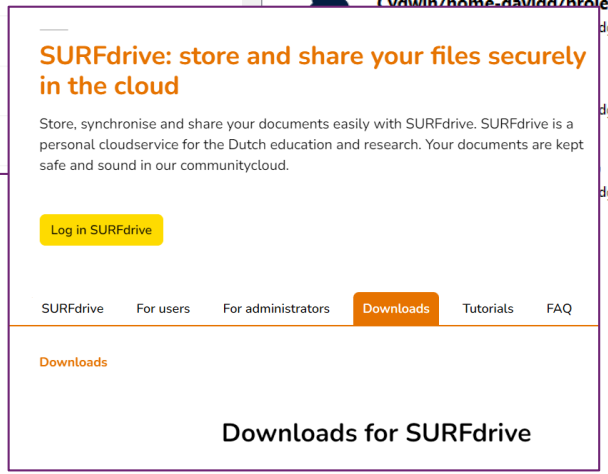
Then

- Nikhef AUP is pretty open on how to use that 500 GByte on SURFdrive
- CERNbox subject to OC5 and OC11

SURFdrive





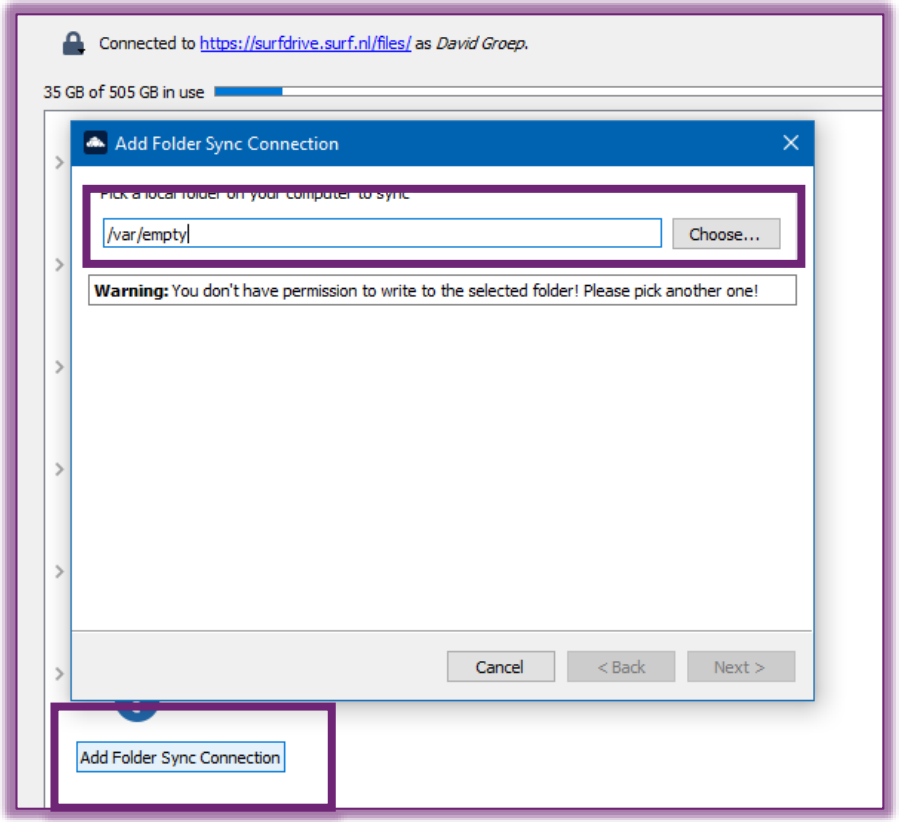


Also provides

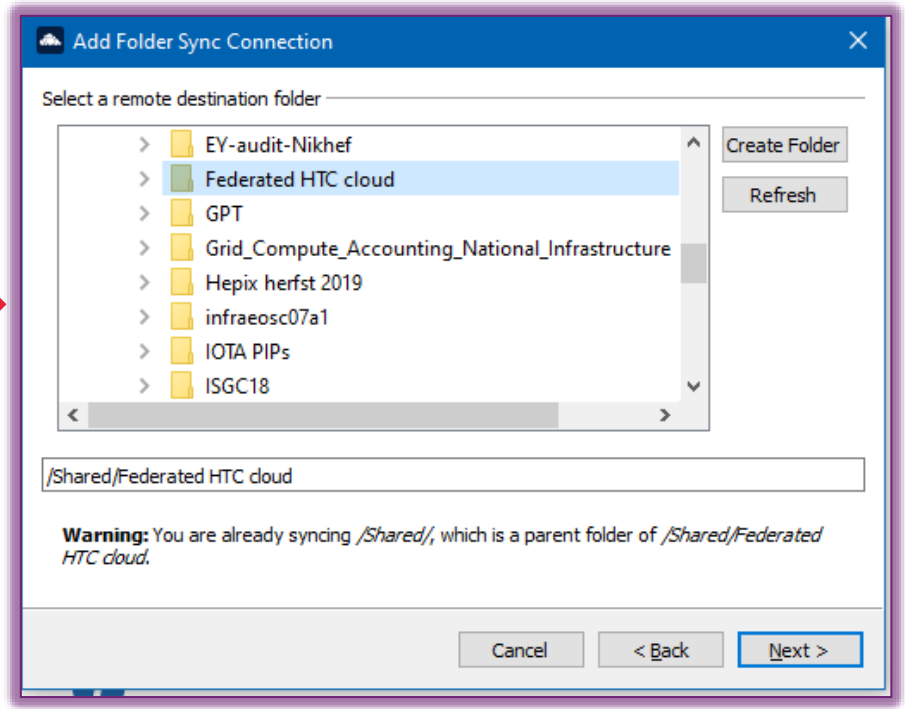
- 30-day roll-back of changed or deleted files
- limited protection against ransomware (restore of ‘everything’ is quite hard)

Web interface at https://surfdrive.surf.nl/ - client download at https://www.surf.nl/en/downloads-for-surfdrive or use the OwnCloud client (if you already run OwnCloud)

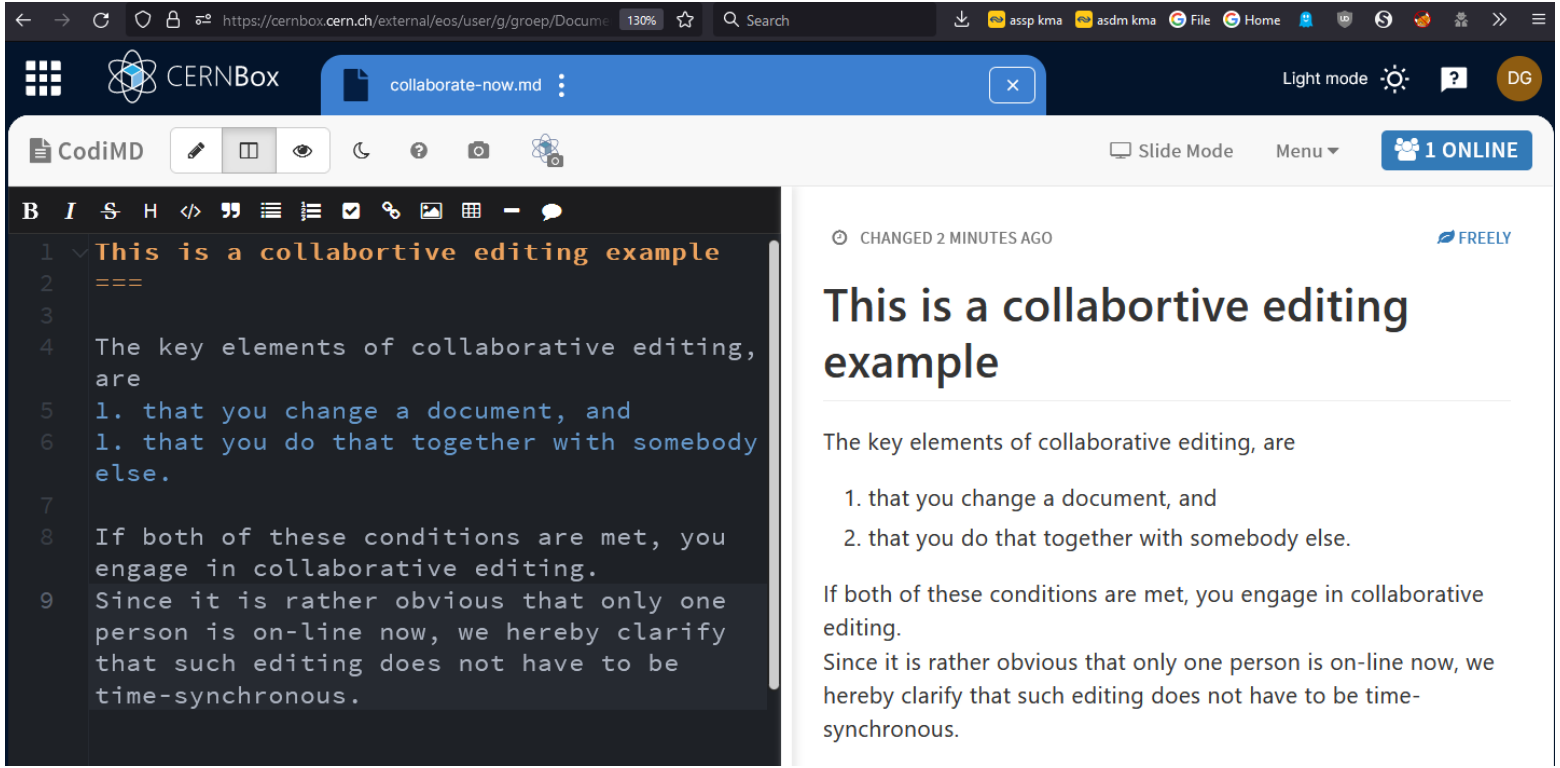
Folder sync connection and VFS virtual file systems



try it live!

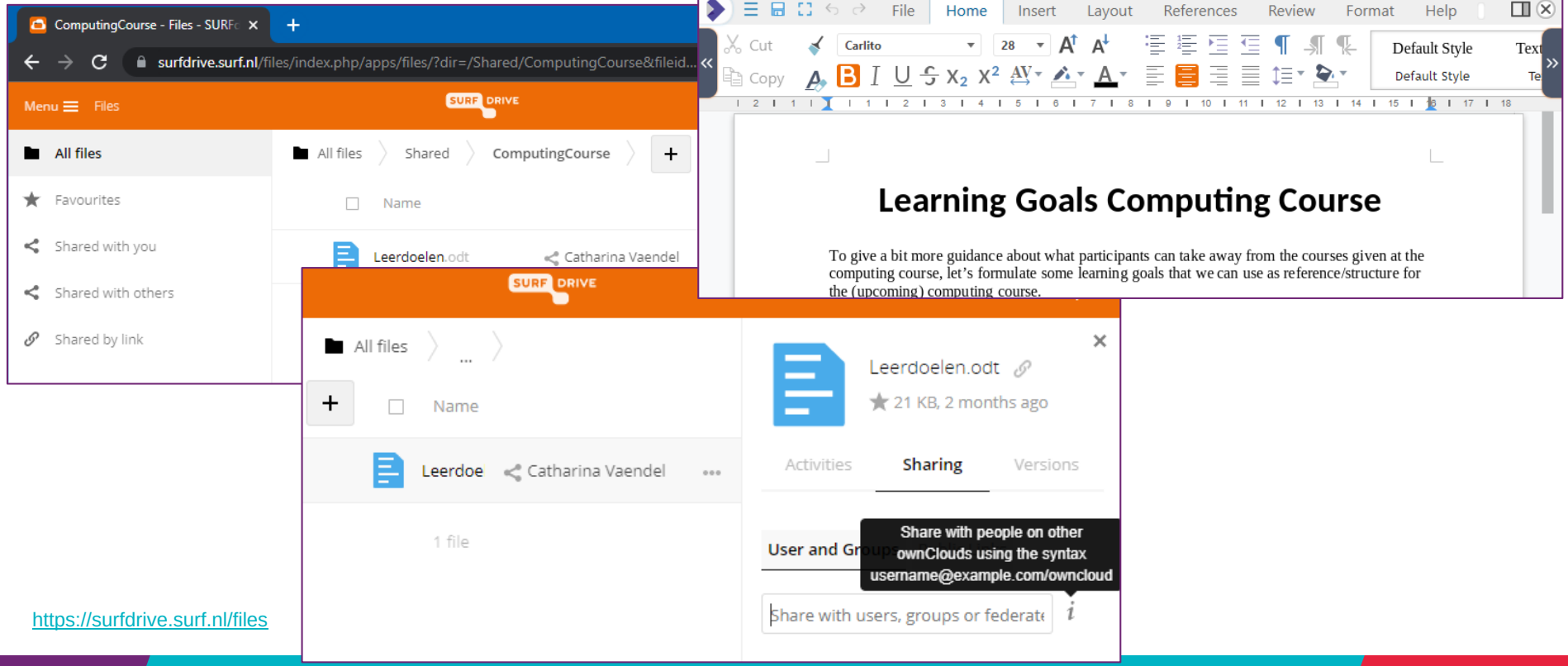


But this is also a great way of working on documents



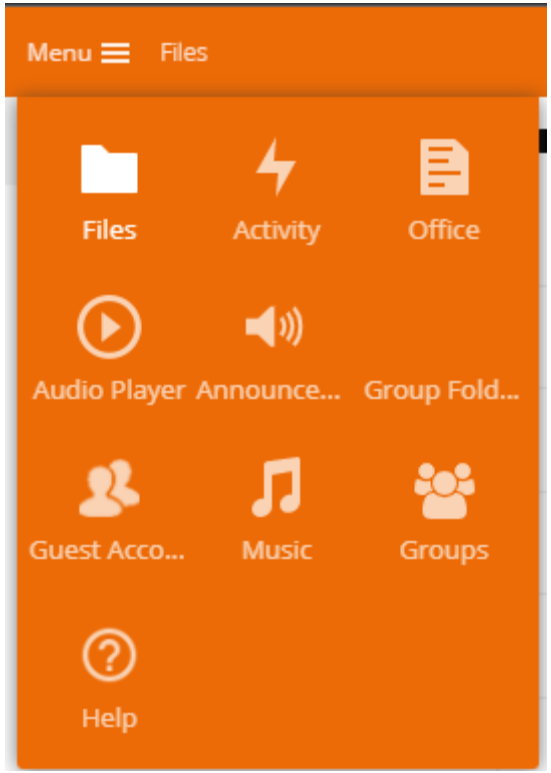
Example above from CERNbox, editing a markdown file. It also works on Word documents, spreadsheets, and presentations.

Also on SURFdrive

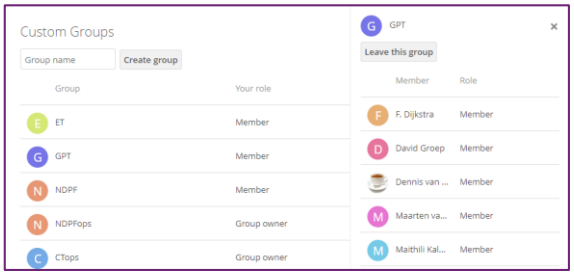


https://surfdrive.surf.nl/files

SURFdrive allows to share with groups, and more



- you can share with all SURFdrive users
- groups also can contain ‘anyone in NL’

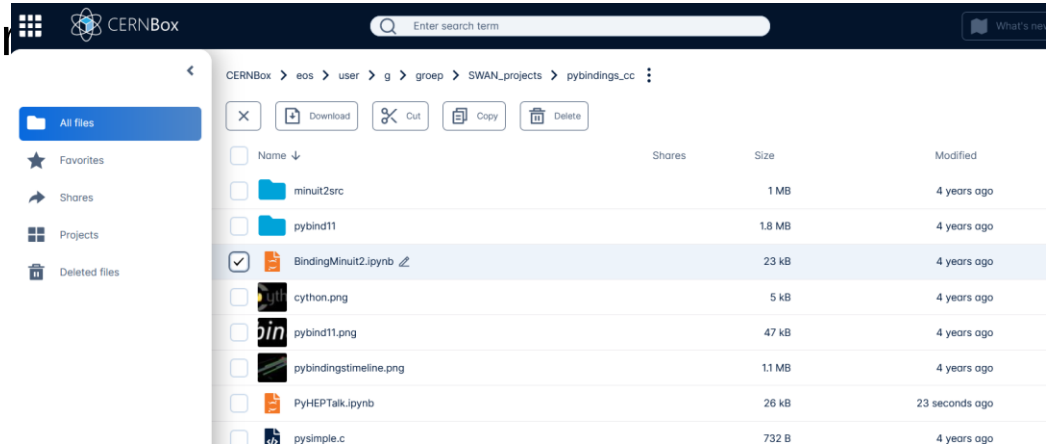


- group *folders* are like ‘/project’ for collaboration
  - are 500 GByte each, max 5 per person,
  - are charged per group folder, so don’t overdo it ☺
- it is possible to create guest accounts for external collaborators (ask the helpdesk for now)

CERNbox – same technology, with some extras @CERN

For CERN users only – sorry for

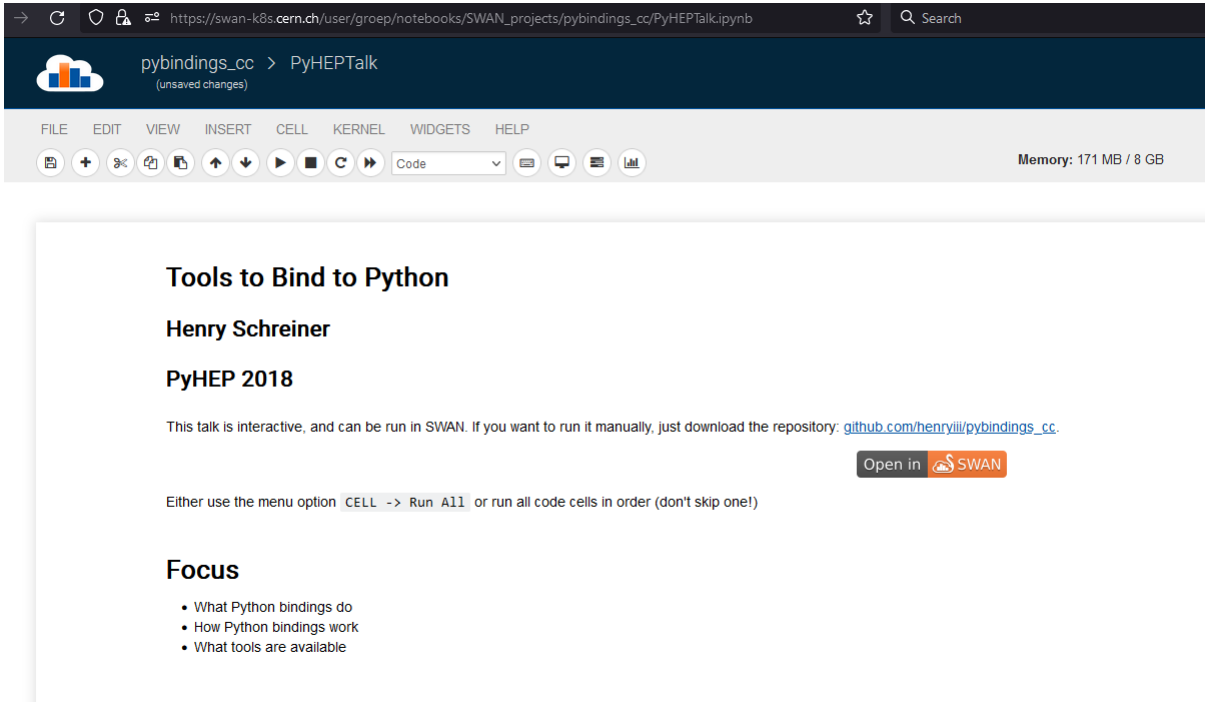
- CERNbox is linked to **SWAN** and **EOS**
- usually 1 TByte
- share with CERN users only (or fully public links)



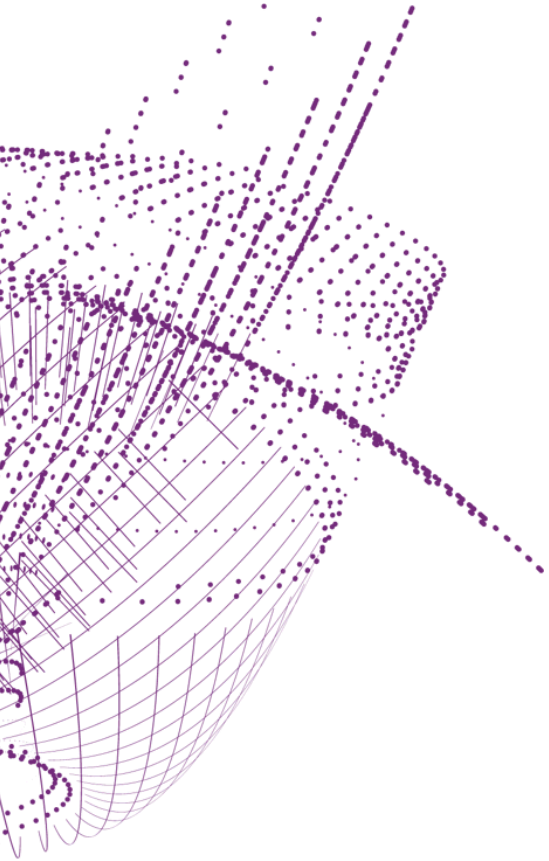

```
-bash-4.2$ hostname
lxplus753.cern.ch
-bash-4.2$ ls -l /eos/user/g/groep/SWAN_projects/pybindings_cc/PyHEPTalk.ipynb
-rw-r--r--. 1 groep c3 25984 Nov  6 21:15 /eos/user/g/groep/SWAN_projects/pybindings_cc/PyHEPTalk.ipynb
-bash-4.2$
```

https://cernbox.cern.ch/

SWAN K8S



https://swan.cern.ch



chat & zoom

From a distance …

A multitude of options

Our community has a long tradition of remote collaboration

- Zooms (many of these) … after having VRVS, Evo, and Vidyo
- Indico … based on CDS Agenda
- lately: many chat clients as well

Also here, not all tools are appropriate for what we need

- especially for video, which is very personal, use endorsed systems
  - we and CERN reviewed Zoom as ‘ok’. If your university has settled on Teams, OK as well
- for chat discussing personal or sensitive matters, use a trusted system
  - realise that ‘who talks to whom’ is *also* sensitive, so e.g. Signal is *much* better than WhatsApp

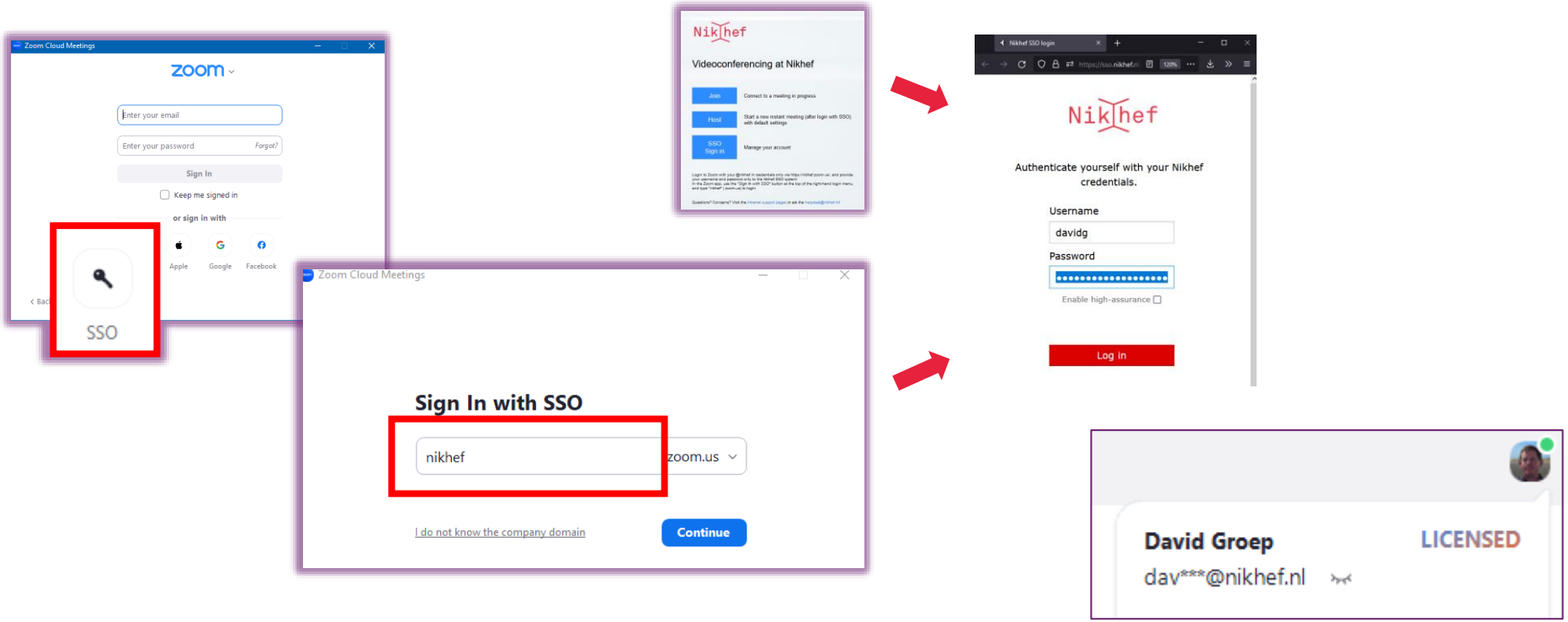
Video conferencing

Every employee (incl. staff at all partners and all PhDs) at Nikhef
can get a licensed zoom membership (although the number of licenses *is* limited)

- up to 500 attendees per meeting
- up to 500 in a webinar
- recording included (will be visible to participants)
- unlimited duration
- everyone can create meetings and webinars
- use Nikhef SSO login to get the right privileges

https://nikhef.zoom.us/

Zoom login – use SSO to get the Nikhef benefits!

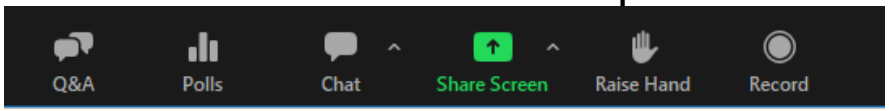


https://nikhef.zoom.us/ for web management interface.

Creating zoom meetings

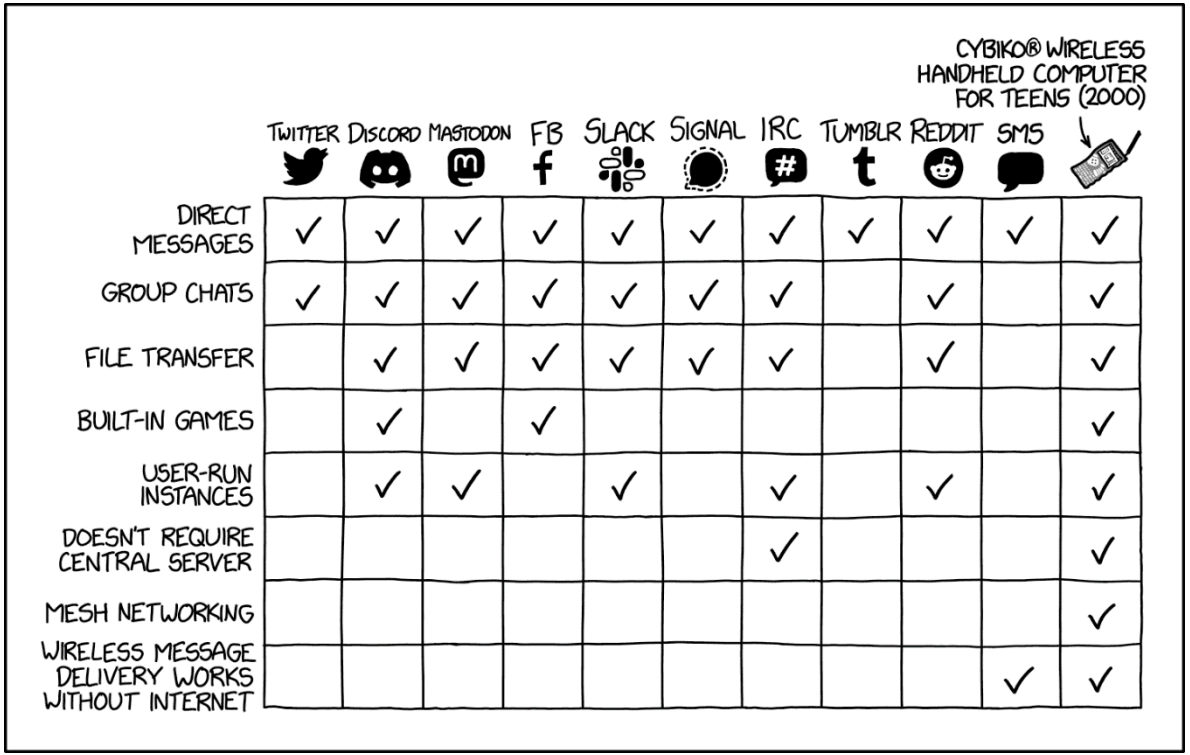
On Zoom **you** create ‘meetings’, and thus is unlike VRVS or Vidyo ‘rooms’

- meetings can be one-off, recurring, or continuous
- you can create meetings as needed, also a new one every time
- you must protect your meetings with either a passcode, or a waiting room
  (after all the incidents with ‘Zoom Bombing’ in early 2020)
- invite link can include the pass-token as well
- for webinars (few talking, many listening), you can create series of 20
  and webinars do **not** need a password to listen in (and you ‘promote’ speakers &c)



To connect use a Zoom client, web browser, PSTN phone, or H.323 room system

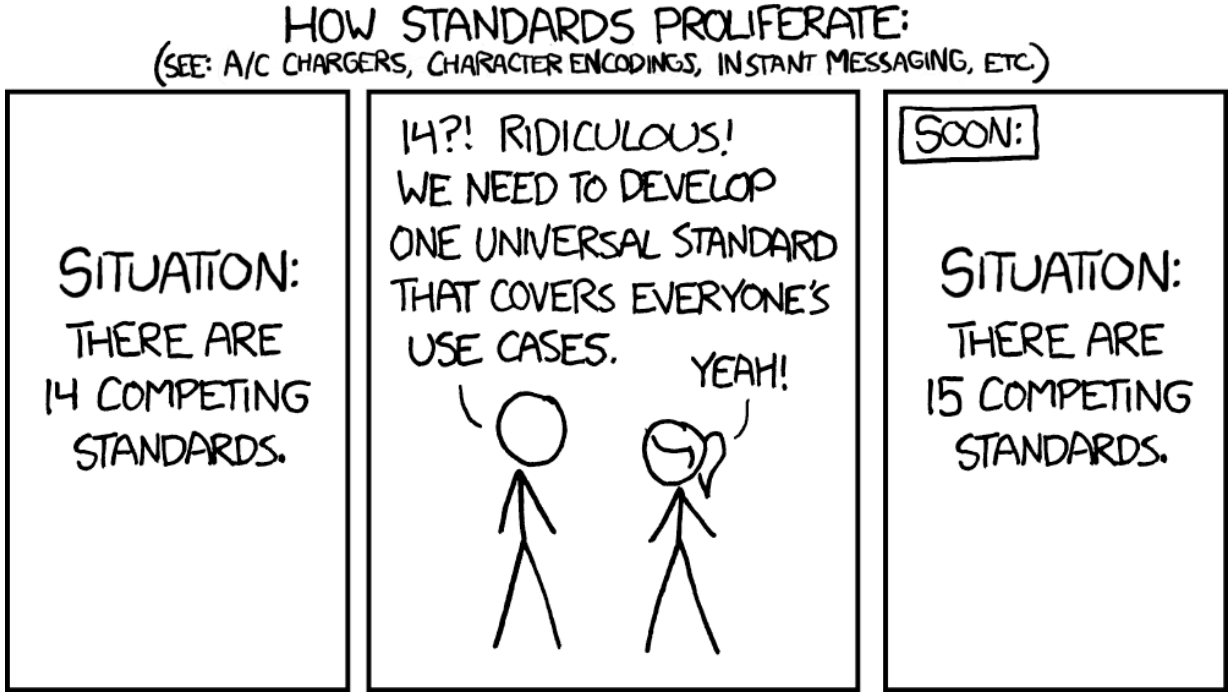
Now what about … ‘just chat’?



	TWITTER	DISCORD	MASTODON	FB	SLACK	SIGNAL	IRC	TUMBLR	REDDIT	SMS	CYBIKO® WIRELESS HANDHELD COMPUTER FOR TEENS (2000)
DIRECT MESSAGES	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
GROUP CHATS	✓	✓	✓	✓	✓	✓	✓		✓		✓
FILE TRANSFER		✓	✓	✓	✓	✓	✓		✓		✓
BUILT-IN GAMES		✓		✓							✓
USER-RUN INSTANCES		✓	✓		✓		✓		✓		✓
DOESN'T REQUIRE CENTRAL SERVER							✓				✓
MESH NETWORKING											✓
WIRELESS MESSAGE DELIVERY WORKS WITHOUT INTERNET										✓	✓

https://xkcd.com/2699/ (thanks for finding this, Dennis!)

But of course we know …



https://xkcd.com/927/

The ‘Nikhef default’ chat system: mattermost

Nikhef hosts its own mattermost server for everyone

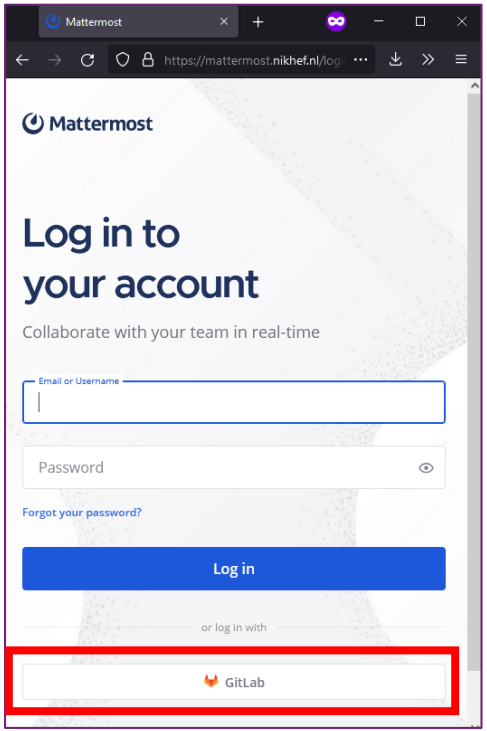
- linked also to Gitlab@Nikhef to have project chats
- login (via Gitlab) using Nikhef SSO
- you can invite anyone from the academic community on Mattermost
  - some new domains will have to be whitelisted – they can already authenticate
  - ask the helpdesk to enable new domains for Gitlab

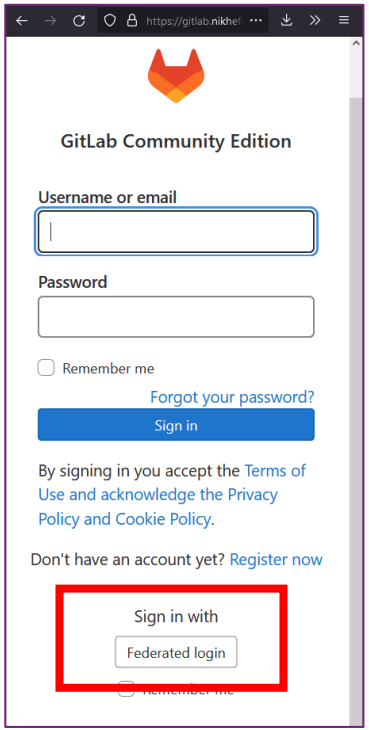
https://mattermost.nikhef.nl/

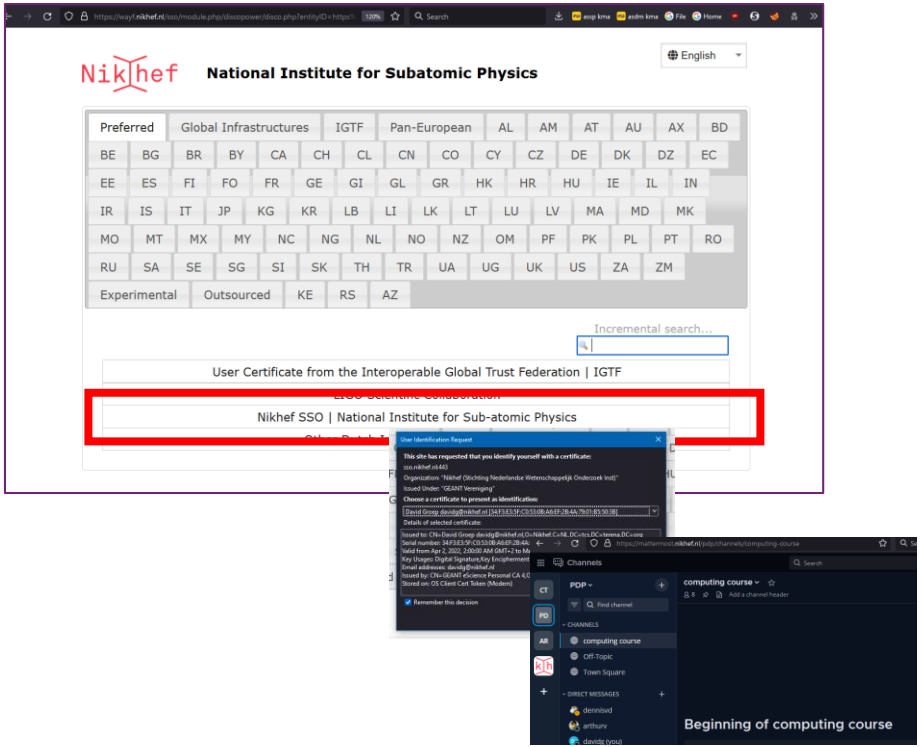
CERN also has Mattermost linked to SSO (https://mattermost.web.cern.ch/)

- On the desktop client, you can have multiple servers
- For android, use the Mattermost beta client
  - https://play.google.com/store/apps/details?id=com.mattermost.rnbeta

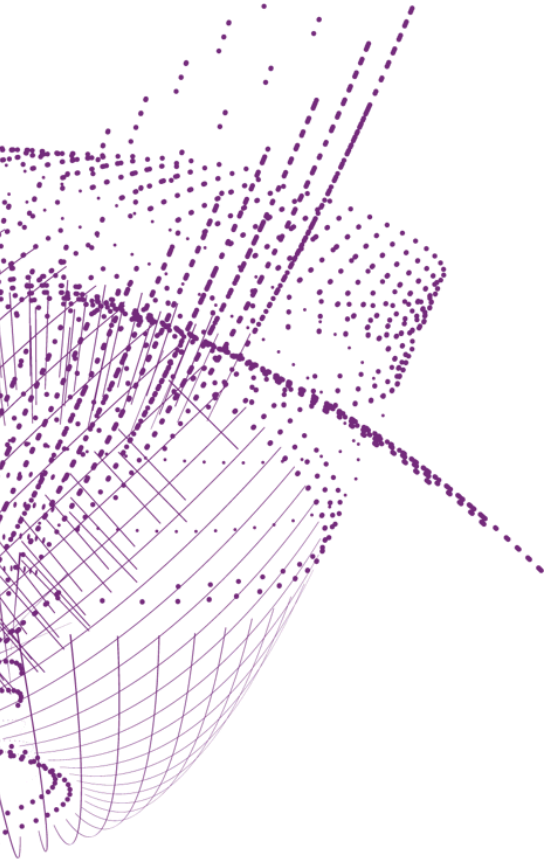
Mattermost login dance (saves us € 36000 per year)







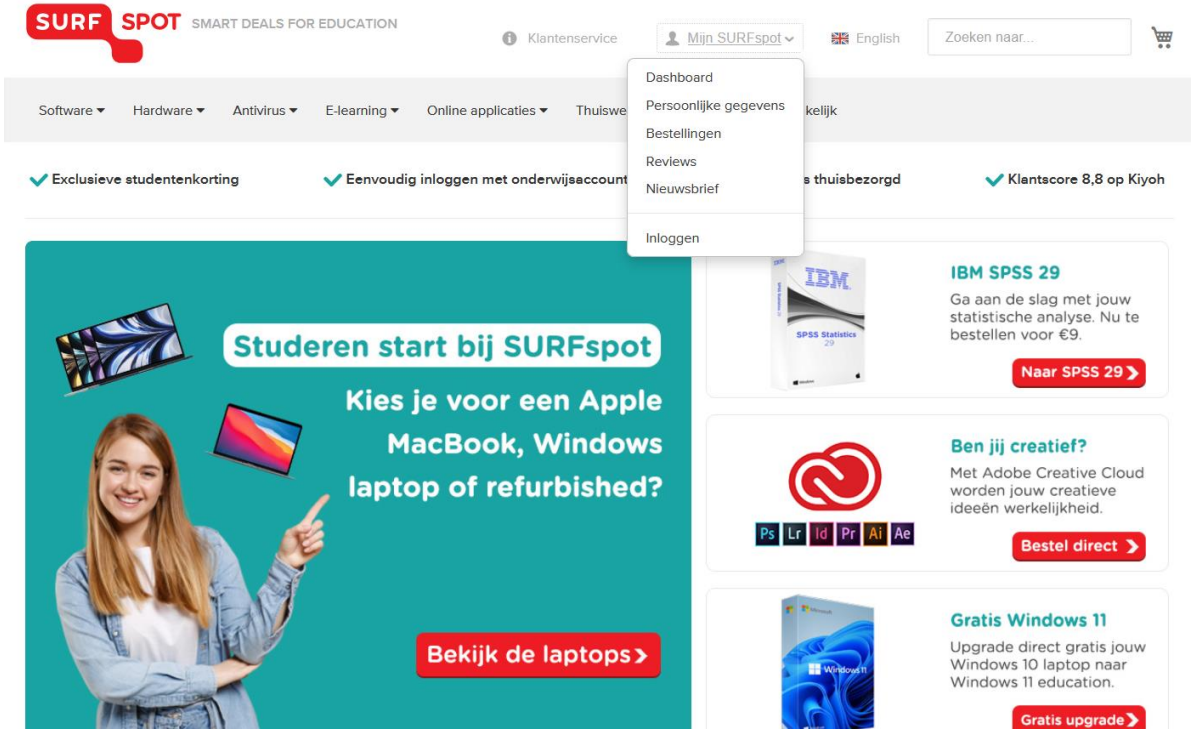
https://mattermost.nikhef.nl/



surfspot.nl
edu.nl - when typing becomes too much
eva - eduroam Visitor Access
cern login - for ‘medium-assurance’ services like Indico
… and many more federated things, from IWGN to …

Collaborative services just to make folk happy

Cheap or free software and hardware … SURFspot



https://surfspot.nl/

Being kind to your colleagues' fingers

For short messages on mastodon, or for persistent URLs to (changing) destinations

https://edu.nl/

- tracking-free short links
- can change after creating the shortcut
- get high-level statistics
- save fingers and characters on (social) media

39	edu.nl/kc63d	2022-06-10	https://surfdrive.surf.nl/files/index.php/s/VcC
16	edu.nl/taecv	2022-06-07	https://surfdrive.surf.nl/files/index.php/s/t62
170	edu.nl/envyq	2022-03-16	https://docs.egi.eu/providers/operations-ma

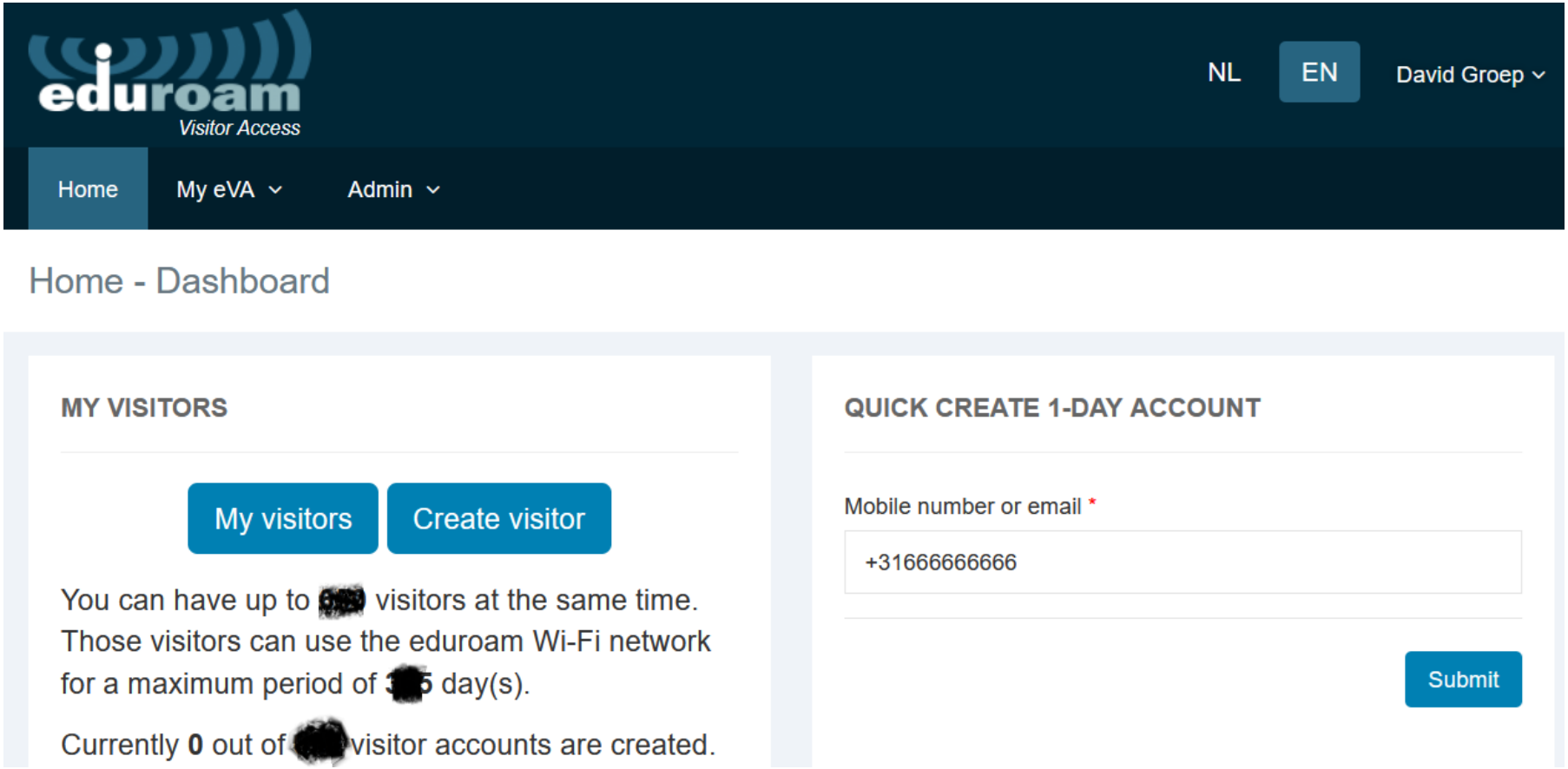
Note: bitly and others rely on click tracking behaviour and collect lots of data from visitors, abusing your friends. And only works with JavaScript. Edu.nl is ad-free as well

eduroam visitor access – gets you instant popularity

“eduroam Visitor Access enables higher education and research institute visitors to access the secure and trusted eduroam Wi-Fi network. The service can provide temporary access to the eduroam network on a simple and suitable manner.”

https://eva.eduroam.nl/en/

- you get one, or a range, of temporary accounts (lile “awfcu@edu.nl”)
- identified by email (kind-of a recursive loop), or SMS on their mobile
- by default: 10 visitors per Nikhef user at a time, max. 9 days validity
- need more? ask the helpdesk to enable it for your
- our secretariat can create large (600 people) events
- also useful for temporary ‘loan’ laptops or other non-personal devices when off-site
- federated service through SURFconext

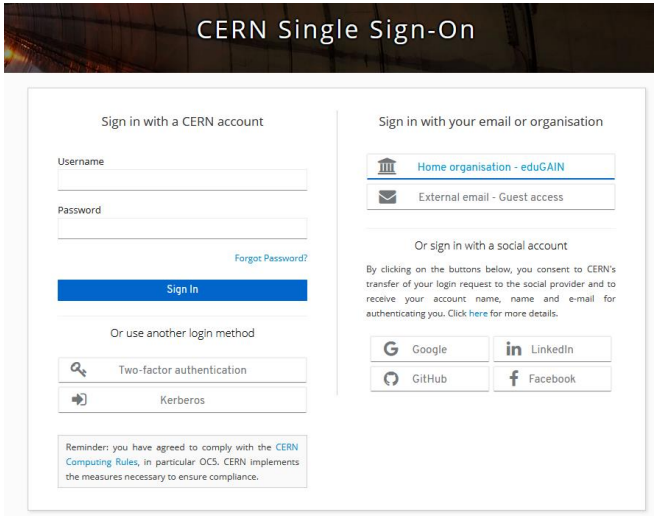

eduroam
Visitor Access
NL
EN
David Groep
Home
My eVA
Admin
Home - Dashboard
MY VISITORS
My visitors
Create visitor
You can have up to [redacted] visitors at the same time.
Those visitors can use the eduroam Wi-Fi network
for a maximum period of [redacted] day(s).
Currently 0 out of [redacted] visitor accounts are created.
QUICK CREATE 1-DAY ACCOUNT
Mobile number or email *
+31666666666
Submit

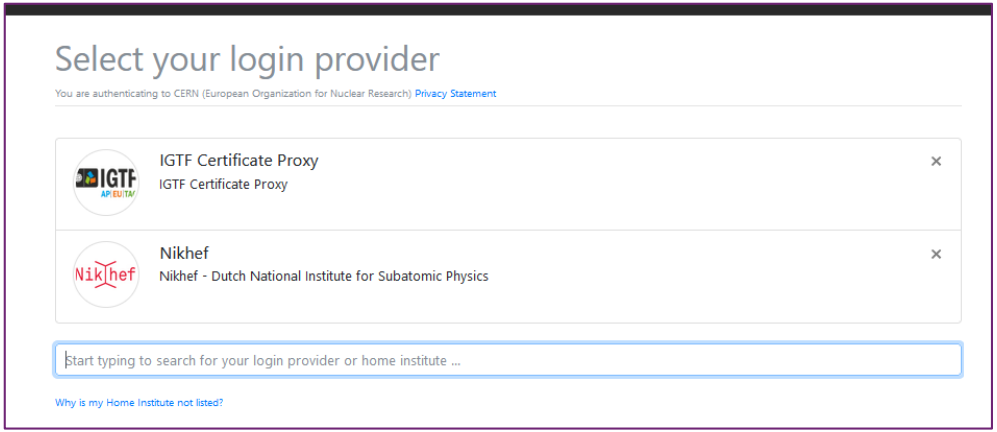
the recipient gets a mail or text message

```
Toegangsgegevens
U heeft de volgende toegangsgegevens nodig bij het aanmelden op het wifi netwerk:
Gebruikersnaam: awfcu@edu.nl
Wachtwoord: trhbi
Wifi netwerk (SSID): eduroam

Uw heeft netwerktoegang vanaf 16-11-2022 00:00 tot en met 16-11-2022 23:59 (CET).

De tijdelijke toegang tot het wifi netwerk verloopt via uw gastheer/gastvrouw David Groep (Nationaal instituut
voor subatomaire fysica). Heeft u vragen over deze toegang of het netwerk neemt u dan contact op met hem/haar.
```

CERN SSO proxy

For CERN services at assurance level ‘4’ (e.g. Indico), you can use Nikhef SSO login





however, works only for the ‘new’ CERN SSO services (and not for EDH or lxplus)

More federated collaborative services

3.1 Internal Services
- 3.1.1 Unix Login
- 3.1.2 Electronic Mail
- 3.1.3 Directory (phonebook)
- 3.1.4 Subversion and code management
- 3.1.5 Radius authentication service
- 3.1.6 Windows Domain AD FS Logon
- 3.1.7 Account Management
- 3.1.8 Nikhef Wiki
- 3.1.9 Gallery
- 3.1.10 Gitlab (public gitlab.nikhef.nl)
- 3.1.11 Travel and expenses
- 3.1.12 Timetell working hours registration
- 3.1.13 Website www.nikhef.nl
- 3.1.14 dCache storage access
- 3.1.15 NX TeamCenter
- 3.1.16 Matrix/Element (under construction)
- 3.1.17 Other Purposes

https://wiki.nikhef.nl/nikhef/ctb/NikIDM/Services
from within Nikhef (eduVPN or on-site)

3.2 Necessary External Services
- 3.2.1 GEANT Trusted Certificate Service (TCS) by way of Sectigo
- 3.2.2 ORCID
- 3.2.3 PeopleXS
- 3.2.4 SURFspot
- 3.2.5 Elsevier Science Direct
- 3.2.6 SURFdrive
- 3.2.7 SURF FileSender
- 3.2.8 eduroam (as a user outside Nikhef)
- 3.2.9 eduroam Visitor Access (eVA)
- 3.2.10 eduVPN
- 3.2.11 Videoconferencing via Zoom

3.3 Optional External Services

Optional services

Since logging in securely without passwords, we have a open authentication policy. Federated login is always safer than creating yet-another-password. But: please review what attributes get release on the SURFconext dashboard.

https://profile.surfconext.nl/ and on https://sso.nikhef.nl/

Please note that the necessity of attribute release may or may not have been reviewed by Nikhef or SURFconext. Please refer to the term and conditions (if displayed), the information presented about the entity, and any trust marks associated with the entity (such as "Research and Scholarship" as an entity category).

To review the attributes released to service providers, an overview of released attributes and their values for each user is managed by SURFconext at https://profile.surfconext.nl/ (user login required - you will be required to release the attribute above to access the Profile service)

SURFconext Profile

Your Account
Change your password
Change profile settings
Connect your certificate
Review your account
Federated Attributes viewer

Local services
Complete time sheets
Request WiFi guest accounts
Register networked device
Resolve email addresses

Commute reimbursement

Curfew attestations

Federated Services
Services via SURFconext
SURFconext permissions manager
Your InAcademia status

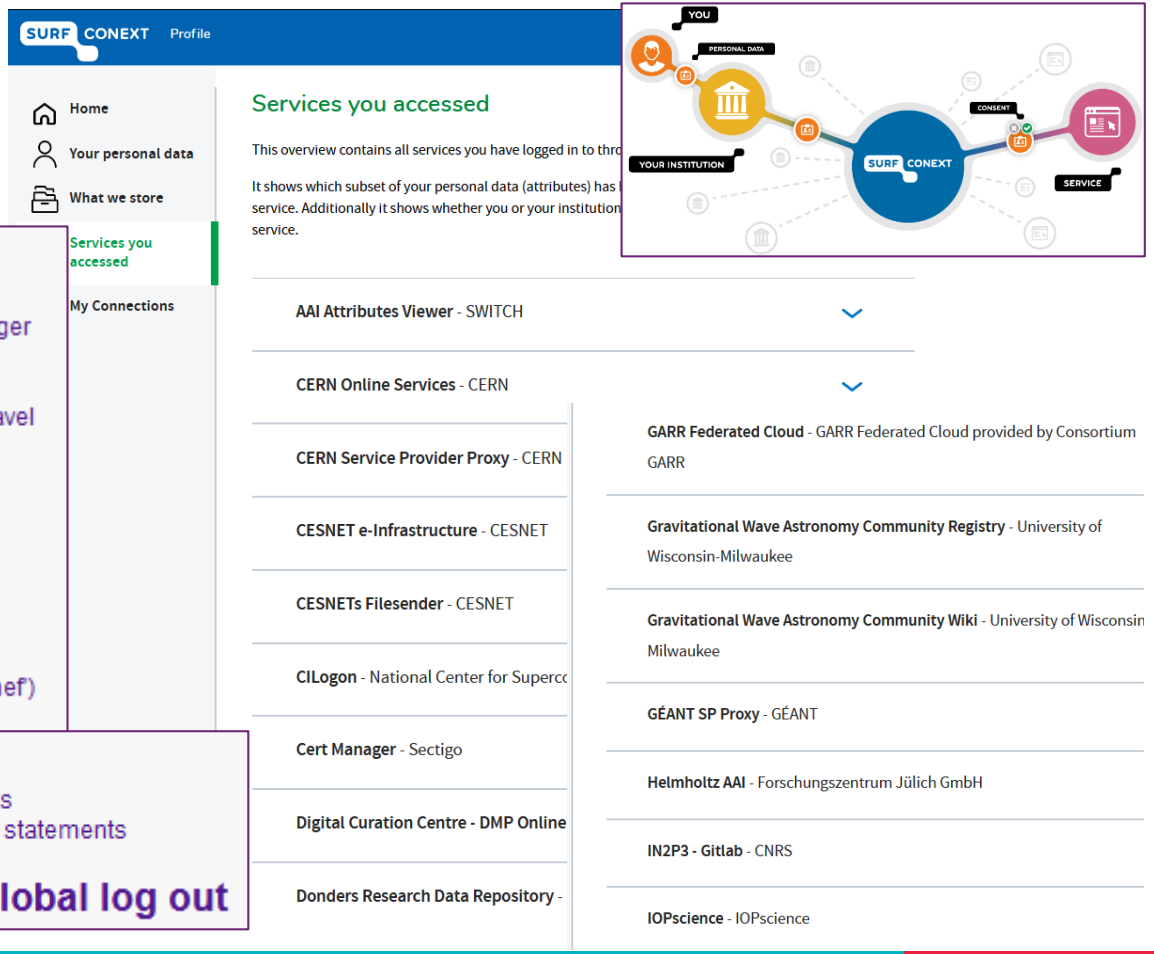
UBW Expenses, Finance and Travel

SURFspot.nl
SURF Mail Filter
SURFfilesender
SURFdrive
eduVPN Safe Browsing
eduVPN Institute Access
eduroam Visitor Access (eVA)
Grid and email Certificates ('Nikhef')

ORCID
SURFteams

Policy
Policy documents
Attribute release statements

Attempt global log out



https://sso.nikhef.nl/
https://profile.surfconext.nl/my-services

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

Maastricht University

Nikhef

CC BY