

Nikhef

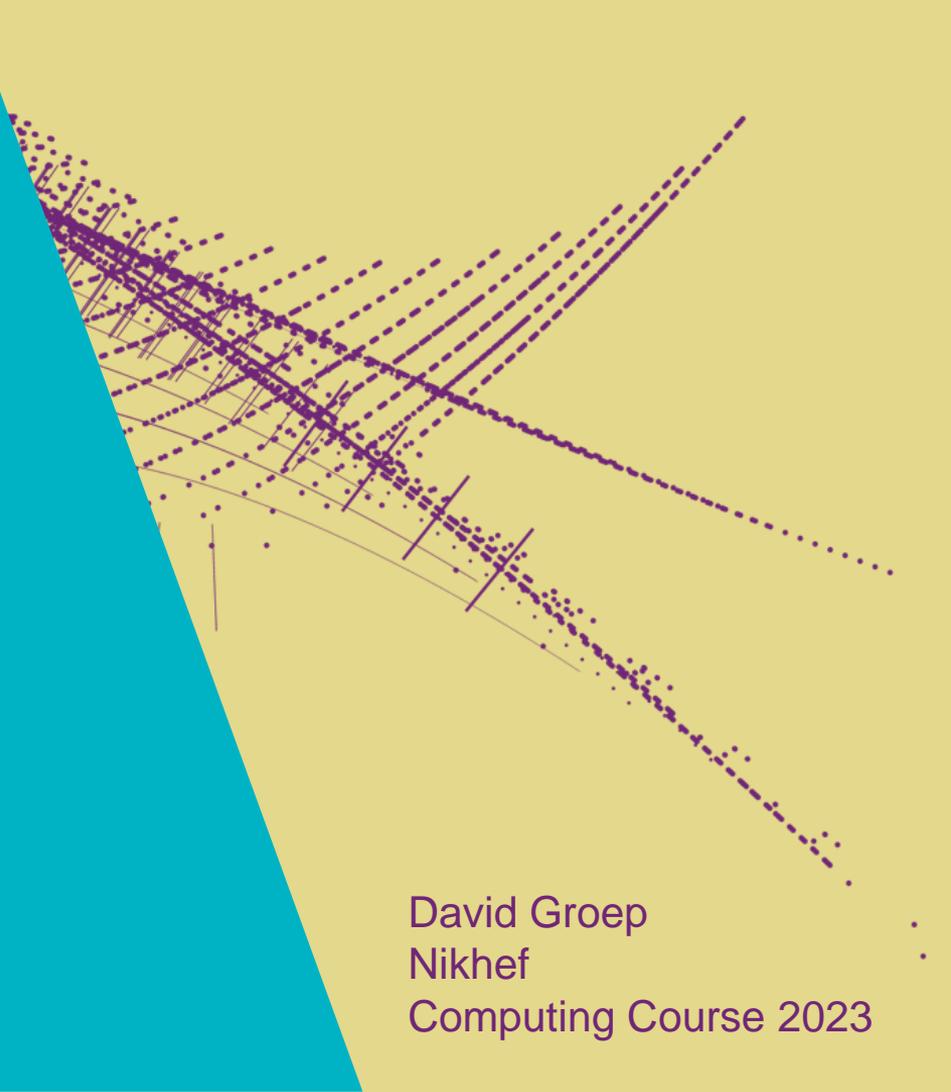


Maastricht University

how to work together, with help at hand

You, your laptop, and somebody else

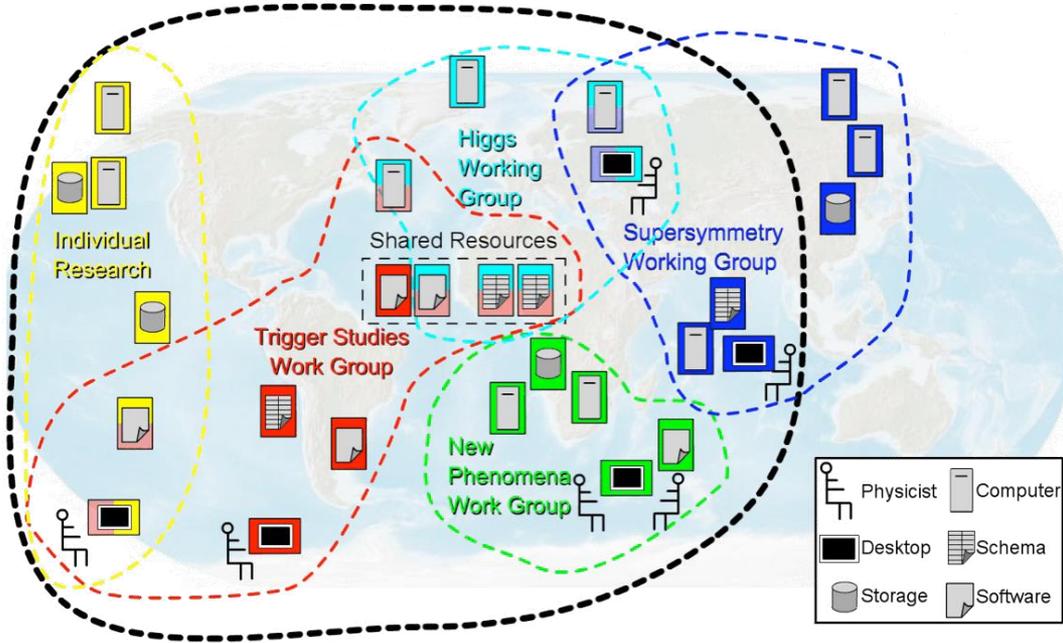
David Groep
Nikhef
Computing Course 2023



Objectives for this session

- Know how to use Identity Services & Federated Login
- 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 collaborative tools like Mattermost *and some other nice collaboration services ...*
- Security and safety in collaboration – ready to take on the world?

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 collage features several overlapping screenshots:

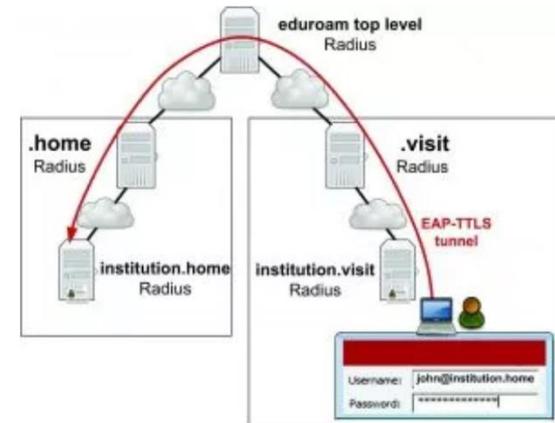
- Mattermost:** A chat interface with a sidebar showing channels like 'Town Square' and 'ComputingCourse'.
- SURF Filesender:** A file sharing interface with a 'Welcome to SURFfilesender' message and a 'Send Voucher' form. The form includes fields for 'From', 'To', 'Subject', and 'Message', along with an 'Expiry date' and 'Guest options'.
- SSO Login:** A 'Nikhef National Institute for Subatomic Physics' login screen with a message: 'Nikhef Zoom videoconferencing service requires that the information below is transferred.' It includes a 'Remember' checkbox and a 'Privacy policy' link.
- Video Conferencing:** A 'Choose Your Institution' page with options for 'Nikhef' and 'Maastricht University', and a 'Videoconferencing at Nikhef' section with buttons for 'Join', 'Host', and 'SSO Sign in'.
- Other Services:** A 'Sectigo Certificate Manager' page and a 'Surfdrive' file browser interface.

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 encrypted 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)

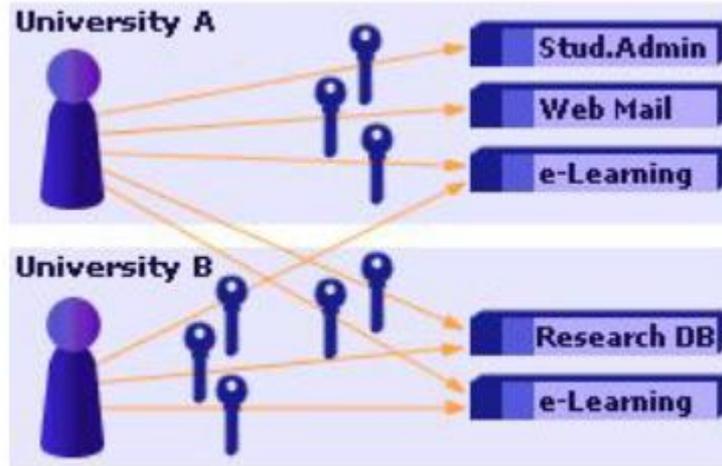


Many places: all Dutch R&E sites, a private home in Utrecht, Geneva airport, all bus stops in Poznan, Australia, UNLP La Plata ...

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

Without AAI



With AAI

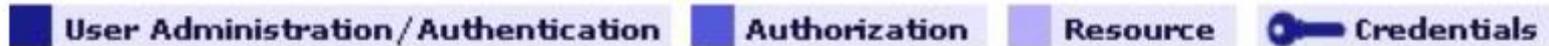
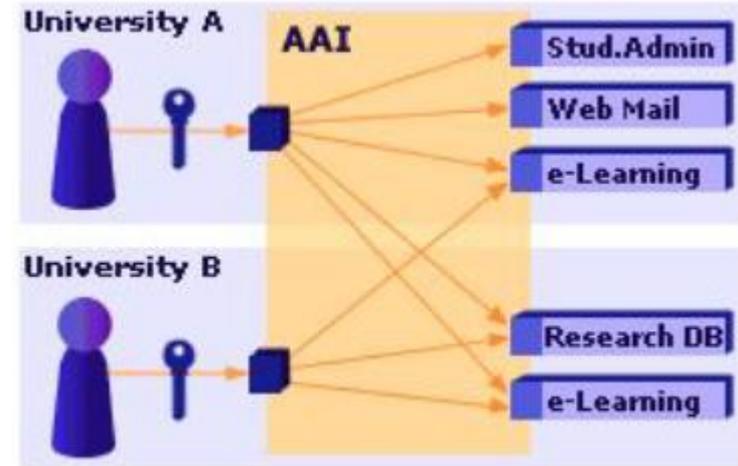
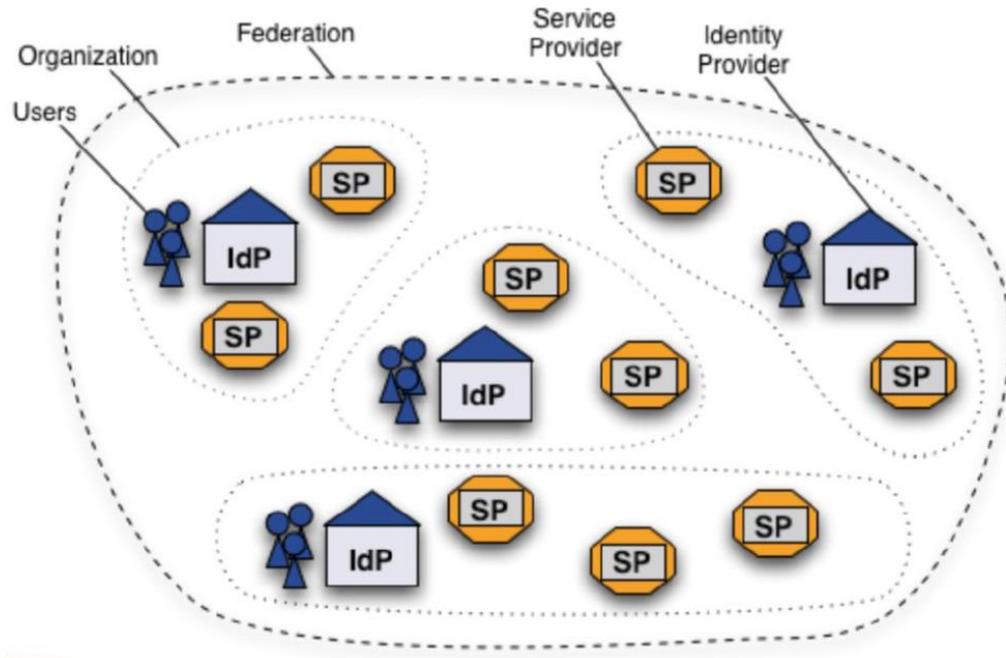


Image: AARC NA2 training module "Authentication and Authorisation 101" - <https://aarc-community.org/training/aai-101/>

Many organisations



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

Federated identity - SURFconext

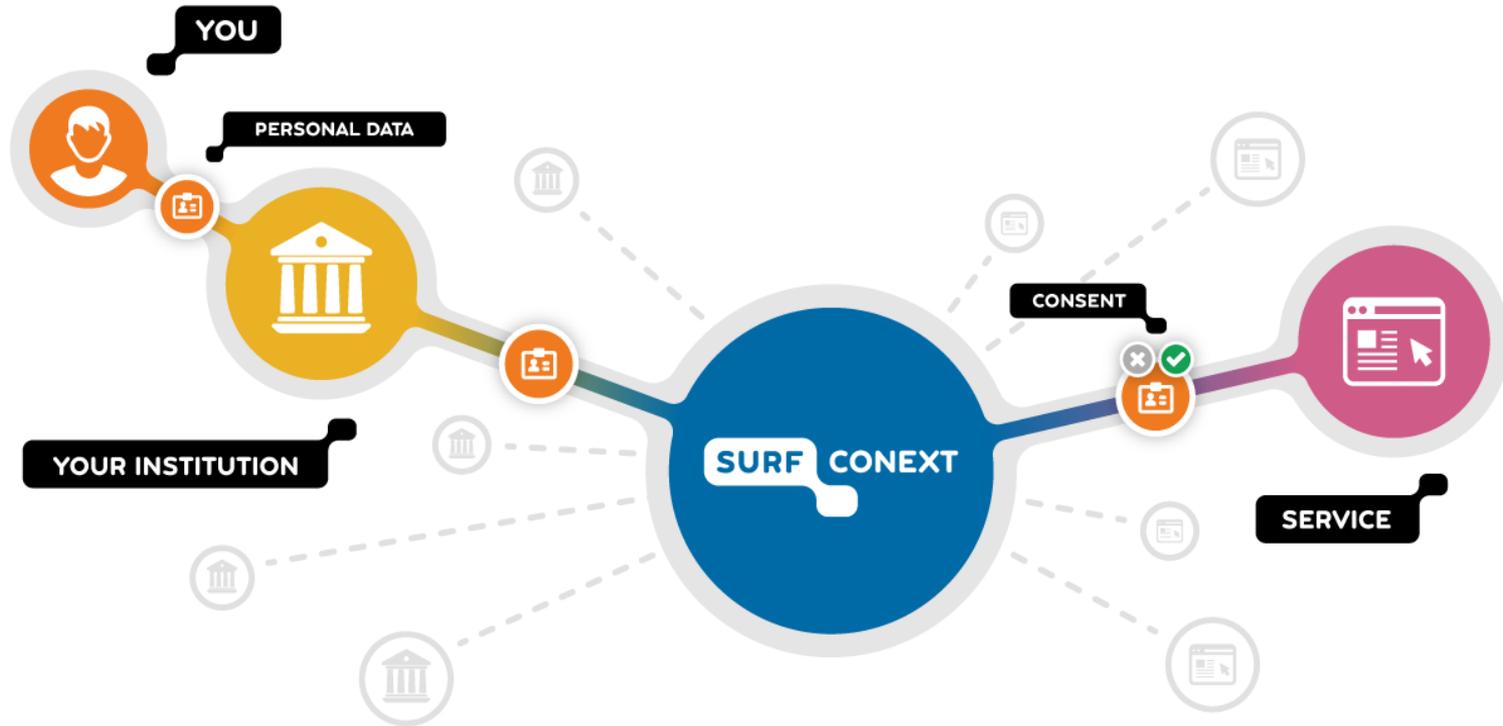


Image: SURFconext dashboard, <https://profile.surfconext.nl/>

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$HKHqUTnt2fEqQ1KA/m3J30A0AVZ5v9LCKRSQHP5
```



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

Authorization: what you are allowed to do

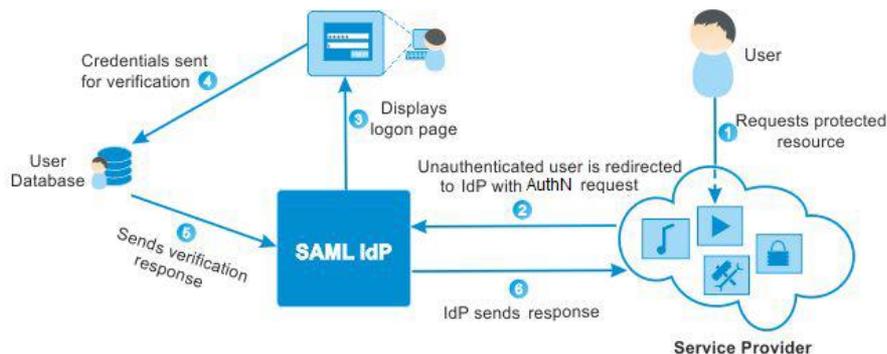
- you may need to ‘collect’ assertions bound to your identity to gain access to services
- like visa, bound to your entity through either Nikhef, or a community attribute authority (VOMS, IAM Proxy, ...)
- in the collaboration cases here the assertions you collect from the Nikhef Identity Provider (‘SSO’) 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	<ul style="list-style-type: none">• 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

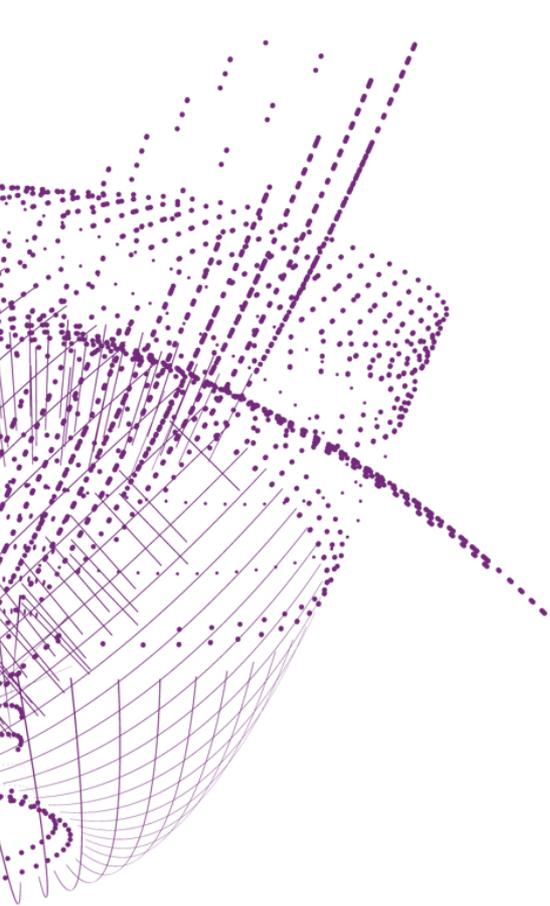
Although you may not think about it all the time ...

- 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

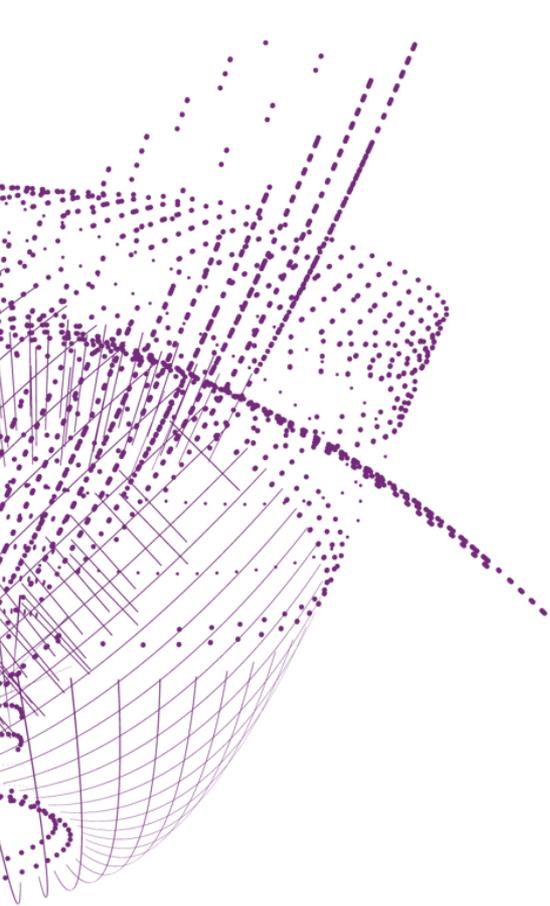
- **SURF FileSender**: trusted, and potentially encrypted, sending of large files
 - can be even a terabyte or so 😊
 - you can also issue vouchers so **others can upload files to you**
- **SURFdrive** (or **CERNbox**) sharing links
 - you can still update the documents after sending the mail
 - integrated 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)

The screenshot shows the 'Send Voucher' page in the FileSender application. At the top, there is a navigation bar with 'Upload', 'Guests', 'My Transfers', and 'My profile'. On the right, there are links for 'Help', 'About', 'Privacy', and 'Log off', along with a 'Preferred language' dropdown set to 'English'. Below the navigation bar, a small text block explains: 'A Voucher allows someone to send you a file. To create a voucher, enter an email address then select Send Voucher. An email will be sent to the recipient with a link to use the Voucher.' The main form is divided into two columns. The left column contains fields for 'From' (pre-filled with 'davidg@nikhef.nl'), 'To' (with a placeholder 'Enter recipient email(s)'), 'Subject (optional)', and 'Message (optional)'. The right column features an 'Expiry date' field set to '29/11/2022', a 'Guest options' section with a checked 'Can only send to me' option, and a 'Created transfers options' section with checked options for 'Notify me upon downloads' and 'Include me as a recipient'. There are also unchecked options for 'Notify me when upload starts', 'Notify me when guests access the upload page', 'Notify creation to guest', and 'Notify me of the guest creation', as well as an unchecked option for 'Get a link instead of sending to recipients'.



Collaborative Sync & Share Services, a.k.a. 'CS3'

SURFdrive and CERNbox

Collaborative Sync-and-Share Service ('CS3') for files

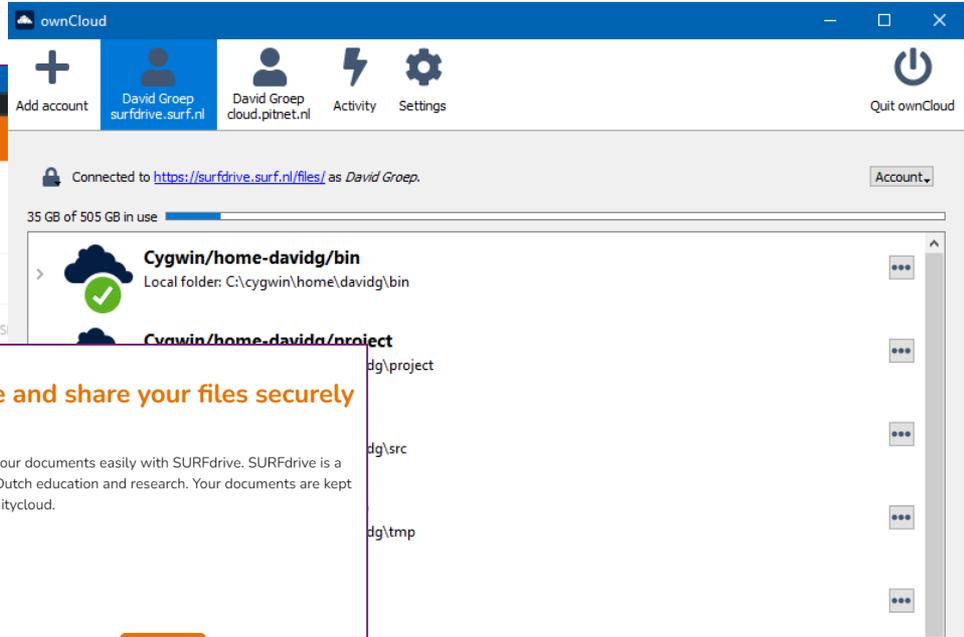
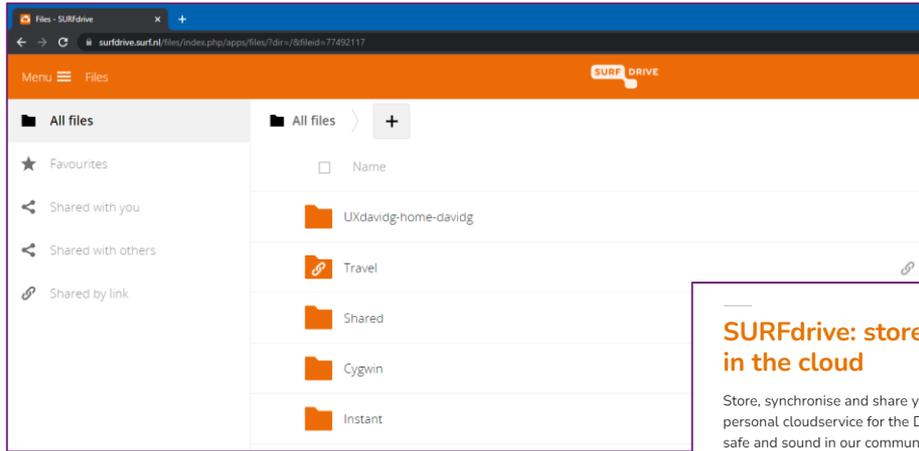
Sharing files and collaborative documents, results, papers, or your photos

- 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)

SURFdrive: store and share your files securely in the cloud

Store, synchronise and share your documents easily with SURFdrive. SURFdrive is a personal cloudservice for the Dutch education and research. Your documents are kept safe and sound in our communitycloud.

[Log in SURFdrive](#)

[SURFdrive](#) [For users](#) [For administrators](#) [Downloads](#) [Tutorials](#) [FAQ](#)

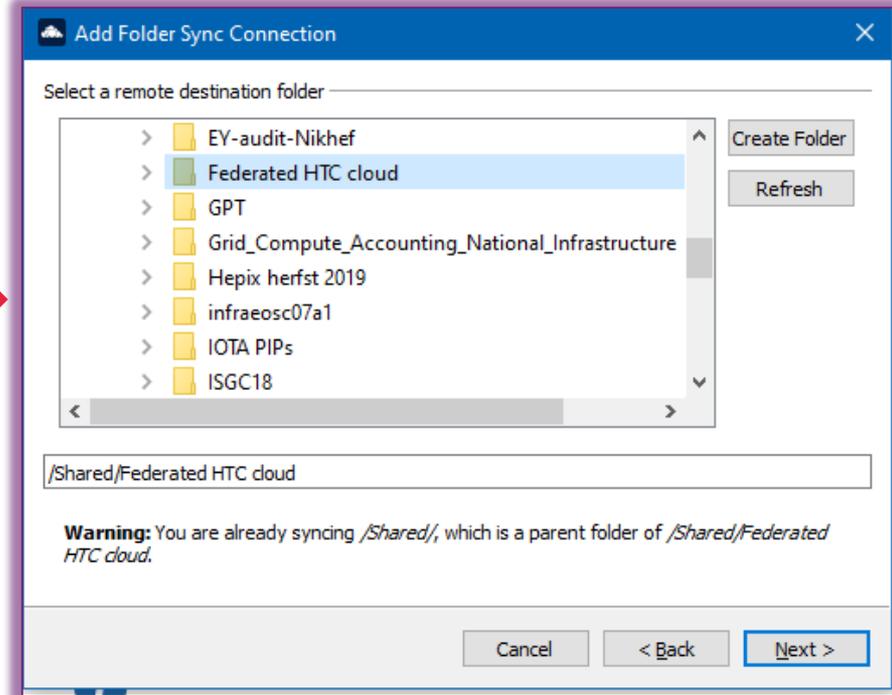
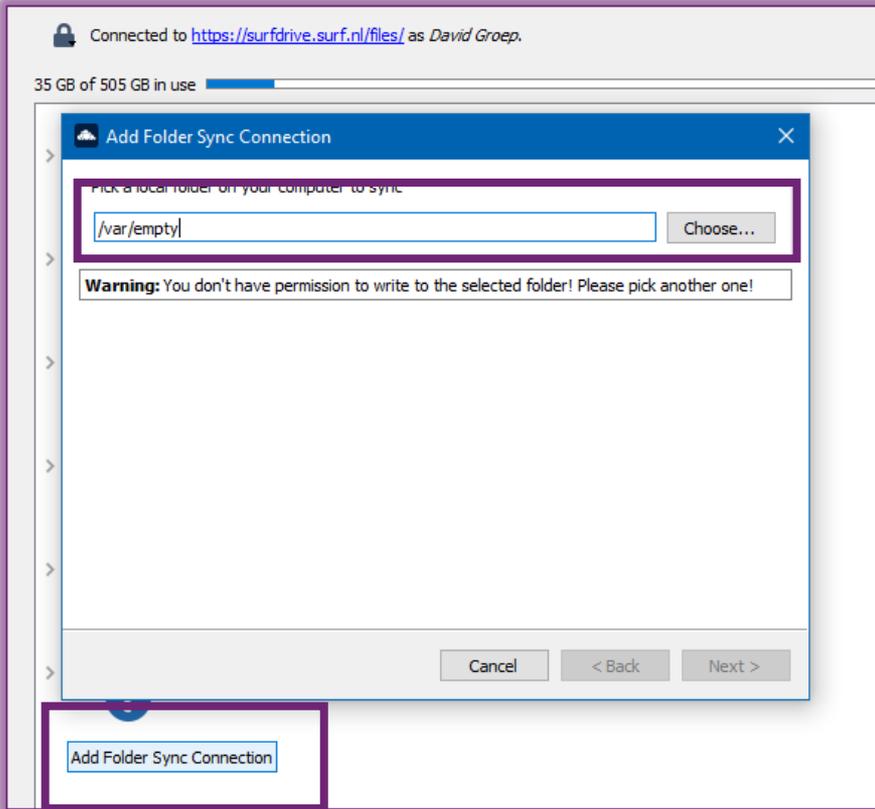
[Downloads](#)

Downloads for SURFdrive

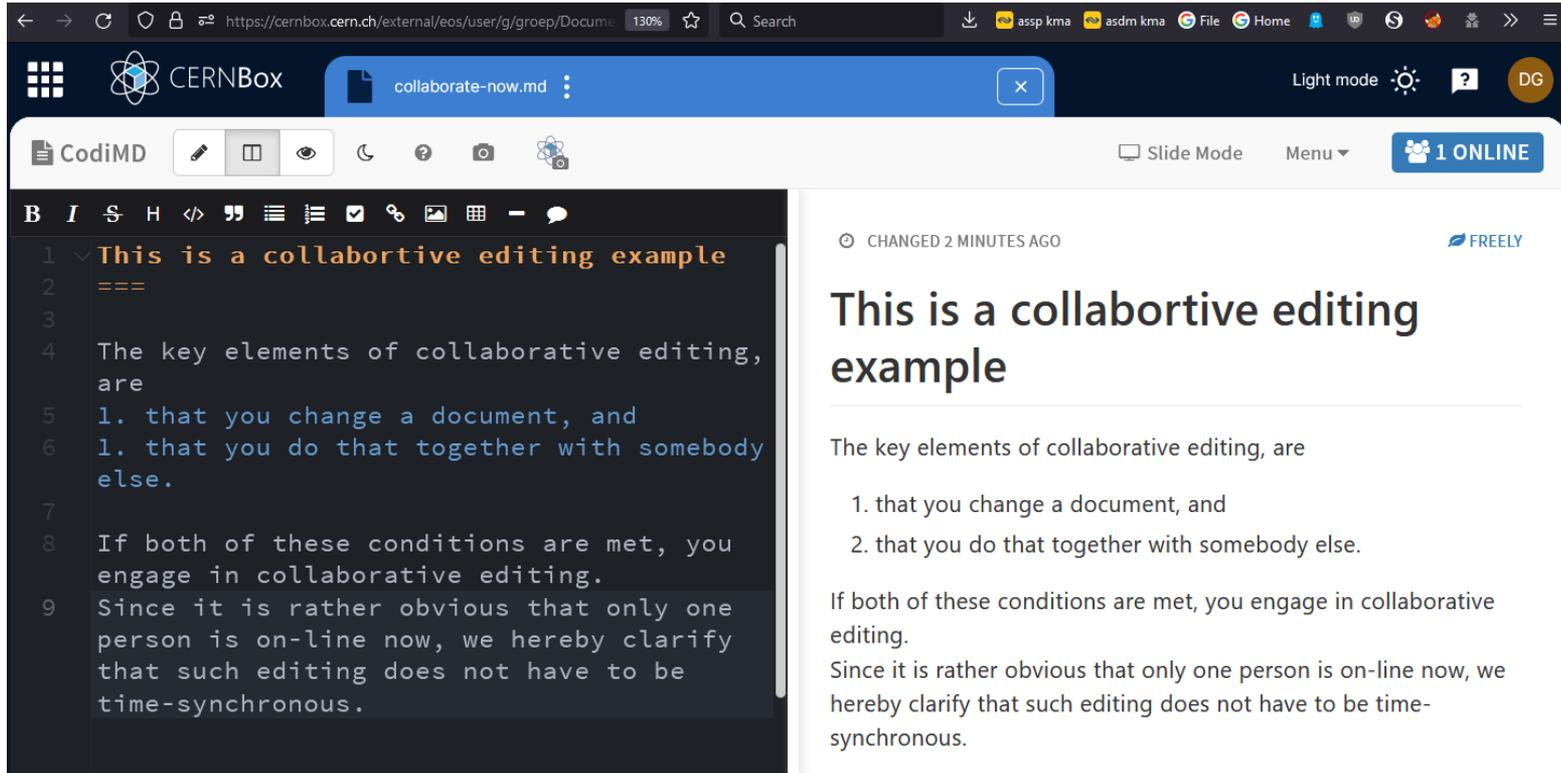
Web interface at <https://surfdrive.surf.nl/> - client download at <https://www.surf.nl/en/downloads-for-surfdrive> or use the OwnCloud client (if you already run OwnCloud)

Folder sync connection and VFS virtual file systems

try it live!



But this is also a great way of working on documents



The screenshot displays the CERNBox CodiMD interface. The browser address bar shows the URL `https://cernbox.cern.ch/external/eos/user/g/groep/Docume`. The CodiMD toolbar includes icons for editing, viewing, and collaboration. The left pane shows a markdown editor with the following content:

```
1 This is a collabortive editing example  
2 ===  
3  
4 The key elements of collaborative editing,  
5 are  
6 1. that you change a document, and  
7 1. that you do that together with somebody  
8 else.  
9  
10 If both of these conditions are met, you  
11 engage in collaborative editing.  
12 Since it is rather obvious that only one  
13 person is on-line now, we hereby clarify  
14 that such editing does not have to be  
15 time-synchronous.
```

The right pane shows the rendered HTML output of the markdown, including a timestamp "CHANGED 2 MINUTES AGO" and a "FREELY" badge. The rendered text is:

This is a collaborative editing example

The key elements of collaborative editing, are

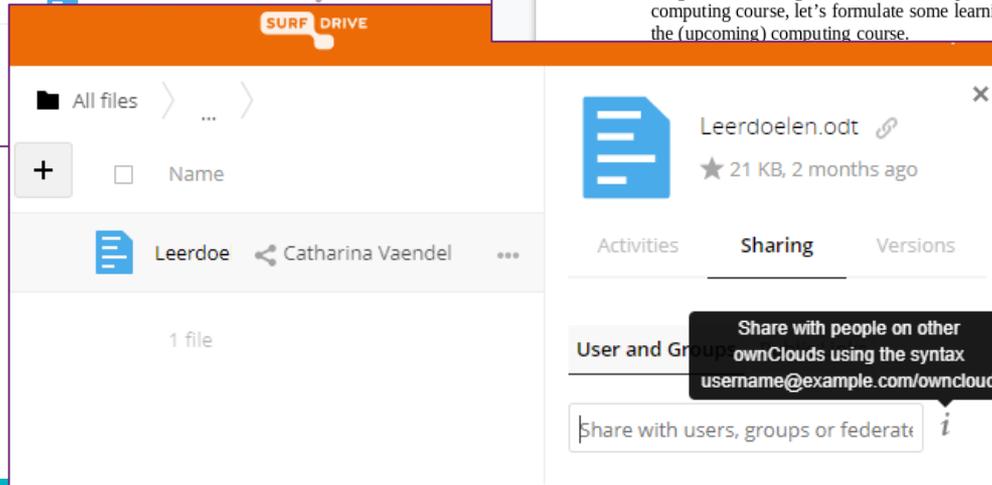
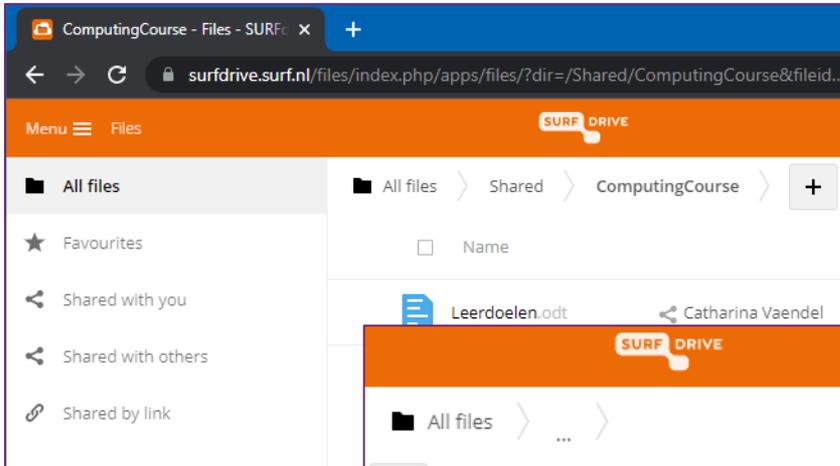
1. that you change a document, and
2. that you do that together with somebody else.

If both of these conditions are met, you engage in collaborative editing.

Since it is rather obvious that only one person is on-line now, we hereby clarify that such editing does not have to be time-synchronous.

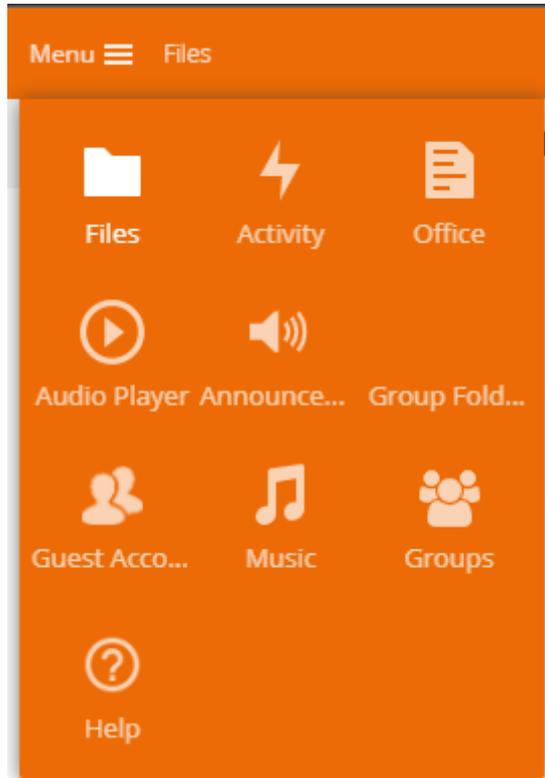
Example above from CERNbox, editing a markdown file. It also works on Word documents, spreadsheets, and presentations.

Also on SURFdrive

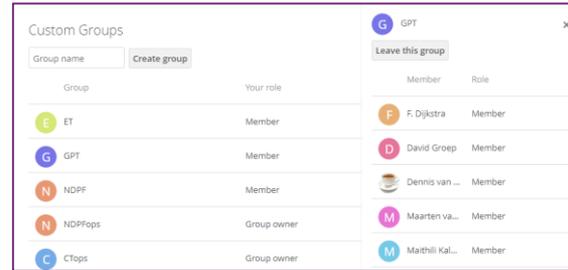


<https://surfdrive.surf.nl/files>

SURFdrive allows to share with groups, and more



- you can share with all SURFdrive users
- groups also can contain 'externals' (NL & guests)

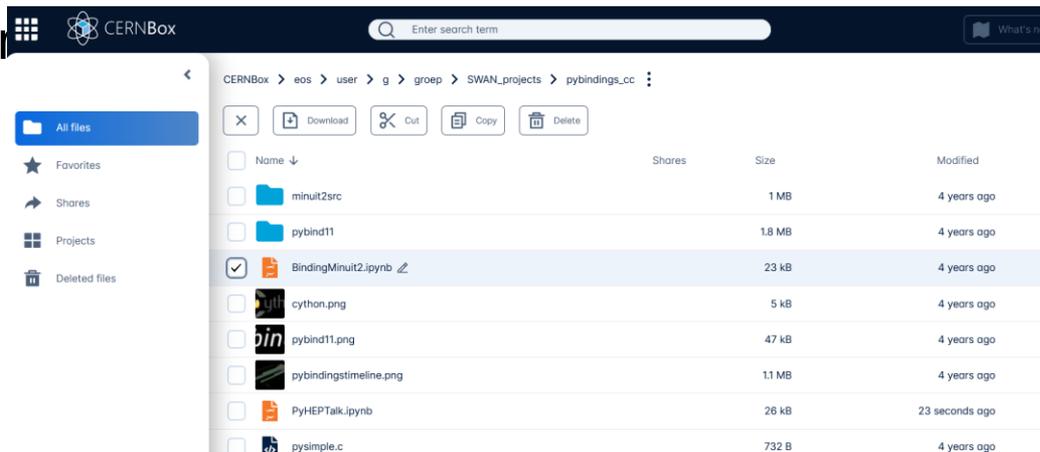


- group *folders* are like '/project' for collaboration
 - are 500 GByte each maximum, max 5 per person,
 - are charged per group folder, so don't overdo it 😊
- it is possible to create **guest accounts** for external collaborators
- it is *not* a backup solution! it is 'sync-n-share' for documents, drawings, pictures, &c

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

github.com/henryiii/pybindings_cc.', a button labeled 'Open in SWAN', 'Either use the menu option `CELL -> Run All` or run all code cells in order (don't skip one!)', and a section titled 'Focus' with a bulleted list: '• What Python bindings do', '• How Python bindings work', and '• What tools are available'. The memory usage is shown as 'Memory: 171 MB / 8 GB'."/>

Tools to Bind to Python

Henry Schreiner

PyHEP 2018

This talk is interactive, and can be run in SWAN. If you want to run it manually, just download the repository: github.com/henryiii/pybindings_cc.

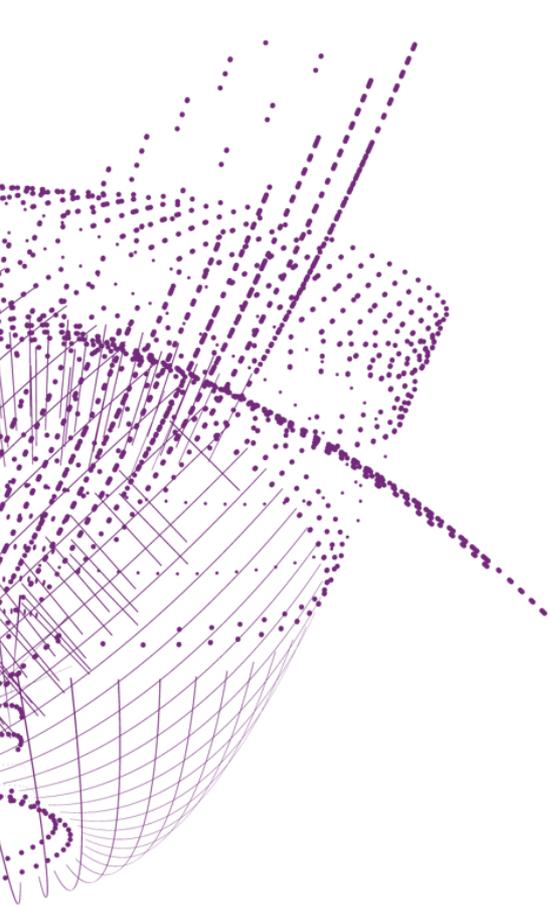
Open in  SWAN

Either use the menu option `CELL -> Run All` or run all code cells in order (don't skip one!)

Focus

- What Python bindings do
- How Python bindings work
- What tools are available

<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, SURF, 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!

The process is shown in four steps:

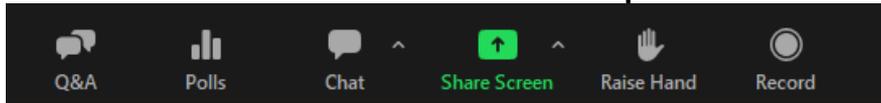
- Zoom Cloud Meetings Sign-in:** The user is on the Zoom sign-in page. The **SSO** icon is highlighted with a red box.
- Zoom SSO Sign-in:** The user is prompted to "Sign In with SSO". The domain **nikhef** is entered in the dropdown menu, which is highlighted with a red box.
- Nikhef SSO Login:** The user is redirected to the Nikhef SSO login page. The username **davidg** is entered, and the **Log In** button is visible.
- Zoom Meeting Profile:** The user is logged into a Zoom meeting. The profile for **David Groep** is shown, with the status **LICENSED** and the email **dav***@nikhef.nl**.

<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'?

CYBIKO® WIRELESS
HANDHELD COMPUTER
FOR TEENS (2000)

	TWITTER	DISCORD	MASTODON	FB	SLACK	SIGNAL	IRC	TUMBLR	REDDIT	SMS	
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 ...

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



<https://xkcd.com/927/>

The 'Nikhef default' chat system: mattermost

Nikhef hosts its own mattermost server for everyone

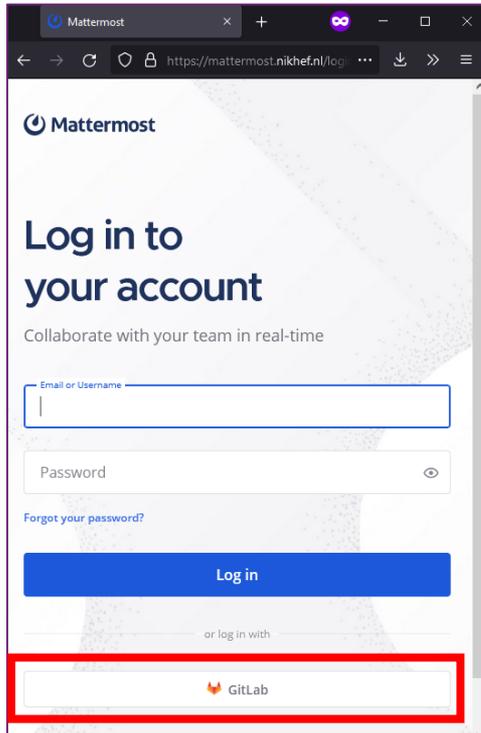
- linked also to Gitlab@Nikhef to have project chats
- login (via Gitlab) using Nikhef SSO
- you can invite anyone from the academic community on Mattermost
 - some new domains will have to be whitelisted – they can already authenticate
 - ask the helpdesk to enable new domains for Gitlab

<https://mattermost.nikhef.nl/>

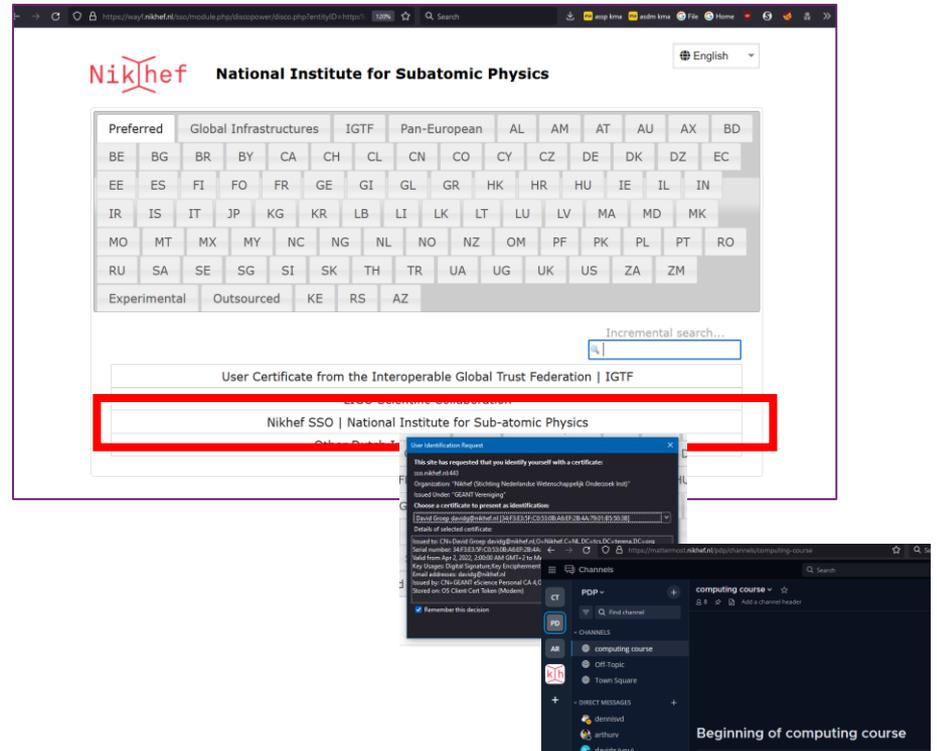
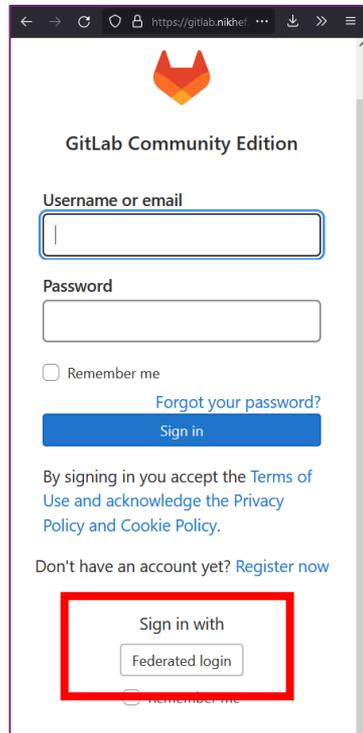
CERN also has Mattermost linked to SSO (<https://mattermost.web.cern.ch/>)

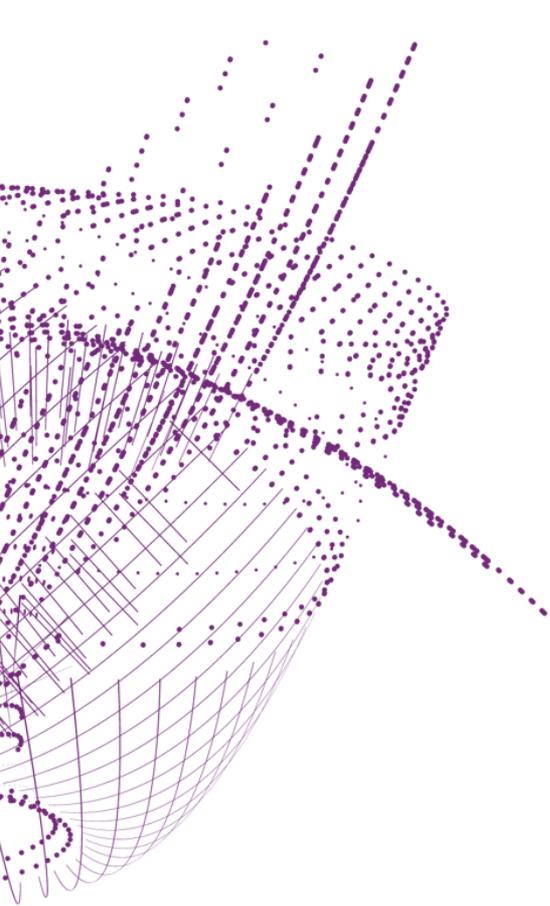
But: you can have multiple servers in the same client (so Nikhef, CERN, Ligo, ...)

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

The screenshot shows the SURFspot website interface. At the top left is the SURF SPOT logo with the tagline "SMART DEALS FOR EDUCATION". To the right are links for "Klantenservice", a user profile dropdown menu, "English", and a search bar. The user menu is open, showing options: Dashboard, Persoonlijke gegevens, Bestellingen, Reviews, Nieuwsbrief, and Inloggen. Below the navigation bar are several promotional banners: "Exclusieve studentenkorting", "Eenvoudig inloggen met onderwijsaccount", "Gratis thuisbezorgd", and "Klantscore 8,8 op Kiyoh". The main content area features a large teal banner for laptops with the text "Studeren start bij SURFspot" and "Kies je voor een Apple MacBook, Windows laptop of refurbished?". Below this are three product cards: "IBM SPSS 29" (statistical analysis software), "Ben jij creatief?" (Adobe Creative Cloud), and "Gratis Windows 11" (operating system upgrade).

<https://surfspot.nl/>

Being kind to your colleagues' fingers

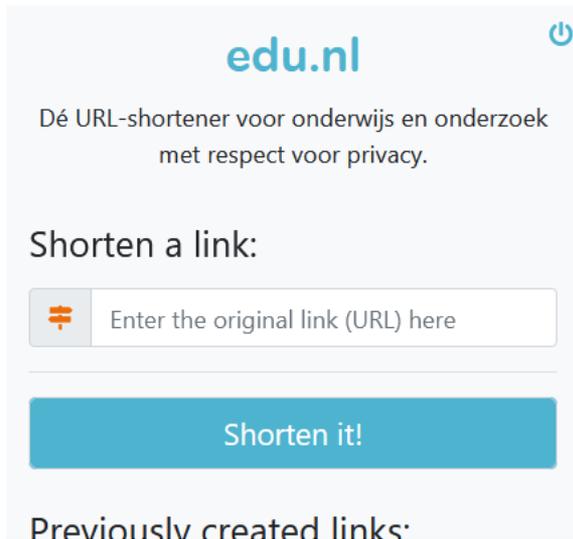
For short messages on mastodon, or for persistent URLs to (changing) destinations

<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/taevv	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 (like “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

Home - Dashboard

MY VISITORS

My visitors

Create visitor

You can have up to **500** visitors at the same time.
Those visitors can use the eduroam Wi-Fi network
for a maximum period of **30** day(s).

Currently **0** out of **500** 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

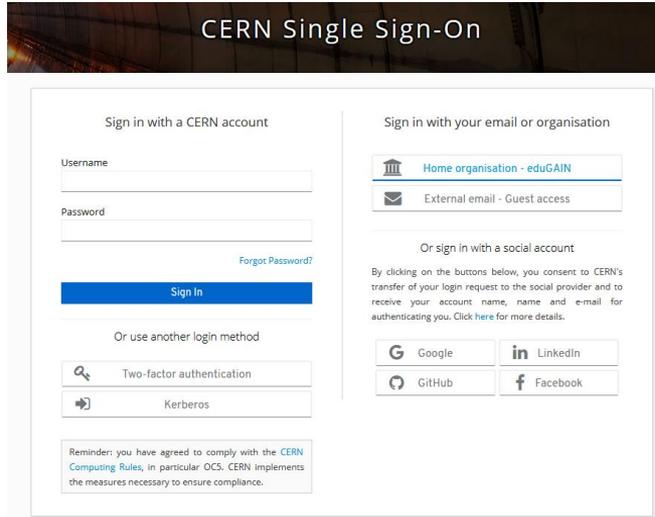
Wifi netwerk (SSID): eduroam

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

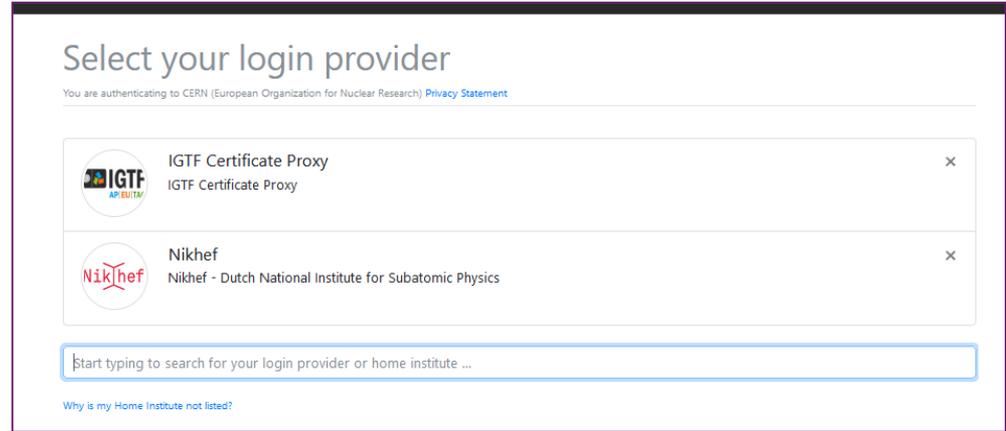
De tijdelijke toegang tot het wifi netwerk verloopt via uw gastheer/gastvrouw David Groep (Nationaal instituut voor subatomaire fysica). Heeft u vragen over deze toegang of het netwerk neemt u dan contact op met hem/haar.

CERN SSO proxy

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



The screenshot shows the 'CERN Single Sign-On' interface. It is divided into two main sections: 'Sign in with a CERN account' and 'Sign in with your email or organisation'. The 'Sign in with a CERN account' section includes fields for 'Username' and 'Password', a 'Forgot Password?' link, a blue 'Sign In' button, and a section for 'Or use another login method' with options for 'Two-factor authentication' and 'Kerberos'. The 'Sign in with your email or organisation' section includes a 'Home organisation - eduGAIN' button, an 'External email - Guest access' button, and a section for 'Or sign in with a social account' with buttons for Google, LinkedIn, GitHub, and Facebook. A reminder at the bottom states: 'Reminder: you have agreed to comply with the CERN Computing Rules, in particular OCS. CERN implements the measures necessary to ensure compliance.'



The screenshot shows the 'Select your login provider' page. It features a search bar at the top with the text 'Start typing to search for your login provider or home institute ...'. Below the search bar, there are two listed providers: 'IGTF Certificate Proxy' and 'Nikhef - Dutch National Institute for Subatomic Physics'. Each provider entry includes a logo, the provider name, and a close button (X). A link at the bottom reads 'Why is my Home Institute not listed?'.

however, works only for the 'new' CERN SSO services (and not for EDH or Ixplus)

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 an open authentication policy. Federated login is always safer than creating yet-another-password. But: please review what attributes get released 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

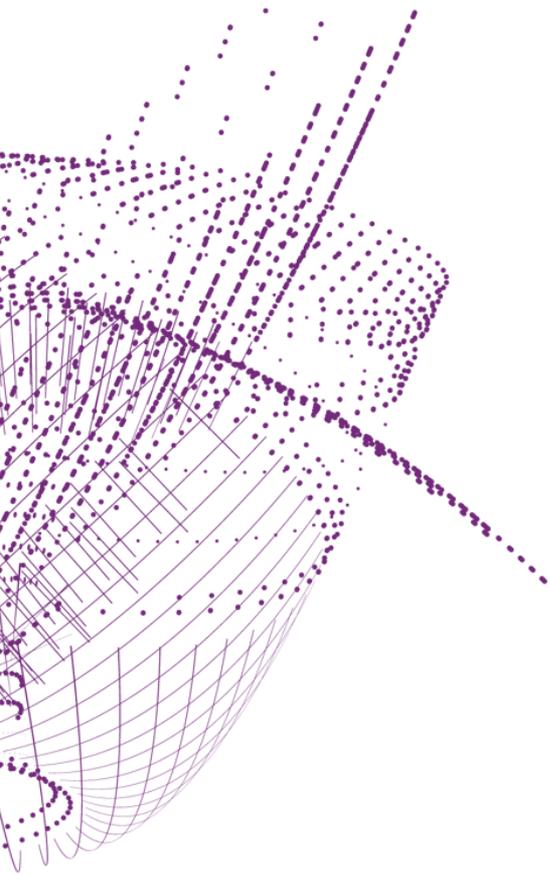
Attempt global log out

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

Services you accessed

This overview contains all services you have logged in to through SURFconext. It shows which subset of your personal data (attributes) has been shared with each service. Additionally, it shows whether you or your institution has given consent for the service.

AAI Attributes Viewer - SWITCH	▼
CERN Online Services - CERN	▼
CERN Service Provider Proxy - CERN	
CESNET e-Infrastructure - CESNET	
CESNETs Filesender - CESNET	
CILogon - National Center for Supercomputing Applications	
Cert Manager - Sectigo	
Digital Curation Centre - DMP Online	
Donders Research Data Repository - Donders	
GARR Federated Cloud - GARR Federated Cloud provided by Consortium GARR	
Gravitational Wave Astronomy Community Registry - University of Wisconsin-Milwaukee	
Gravitational Wave Astronomy Community Wiki - University of Wisconsin Milwaukee	
GÉANT SP Proxy - GÉANT	
Helmholtz AAI - Forschungszentrum Jülich GmbH	
IN2P3 - Gitter - CNRS	
IOPscience - IOPscience	



Collaboration beyond tools and
some words on security

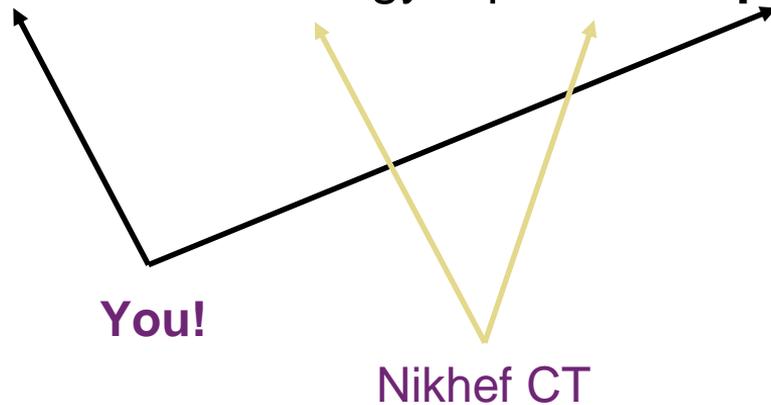


Talking to somebody else...
but to whom?

Collaboration and our open environment

Why security & privacy?

human behaviour + technology + process + physical security



slide: Ronald Starink, Nikhef

Example: phishing and credential theft

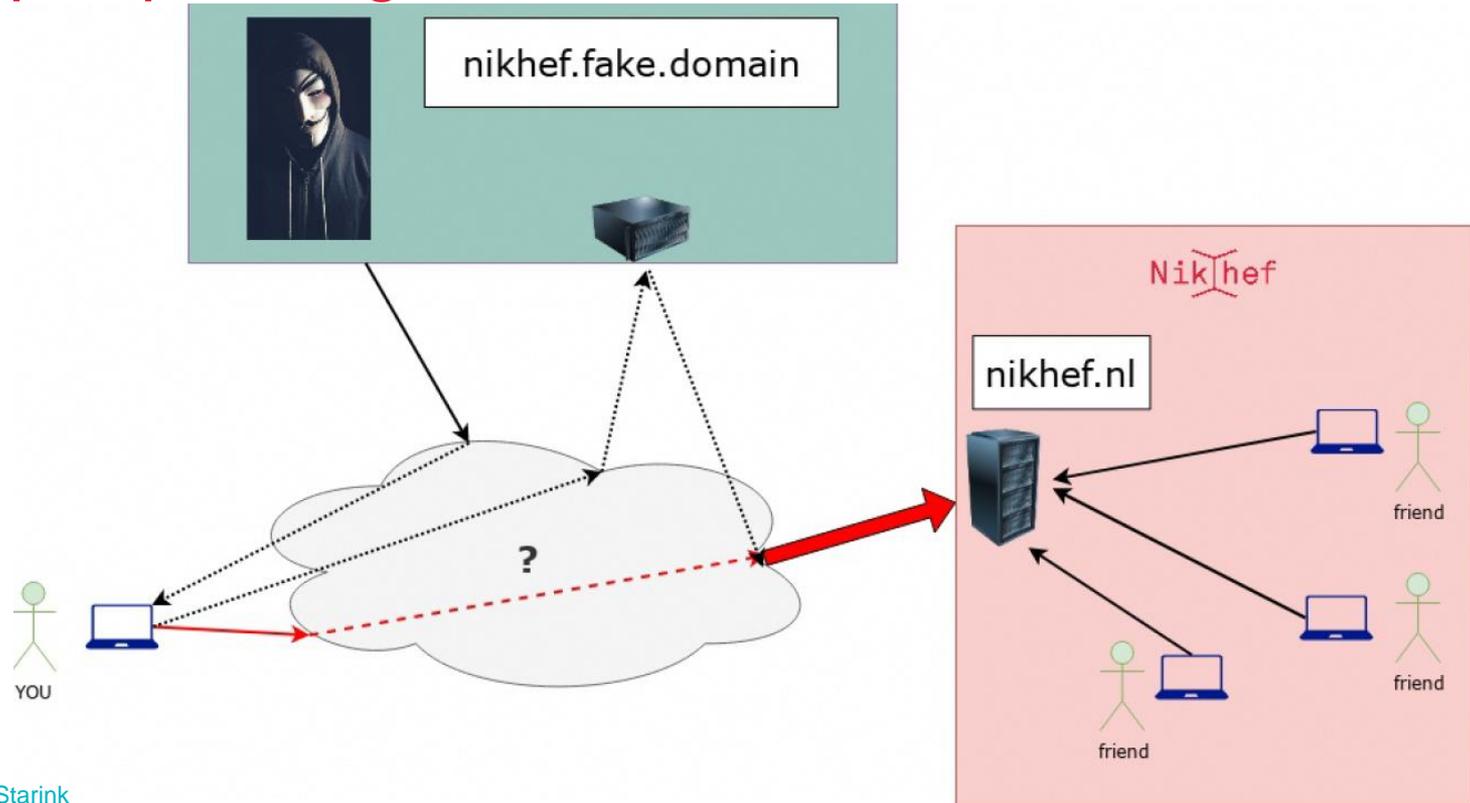


Image: Ronald Starink

Example: phishing and credential theft

possible damage:
weeks-months recovery
data losses
many unhappy people

security@nikhef.nl
+31 20 592 2200

emergencies out of office
hours: 020 592 5090

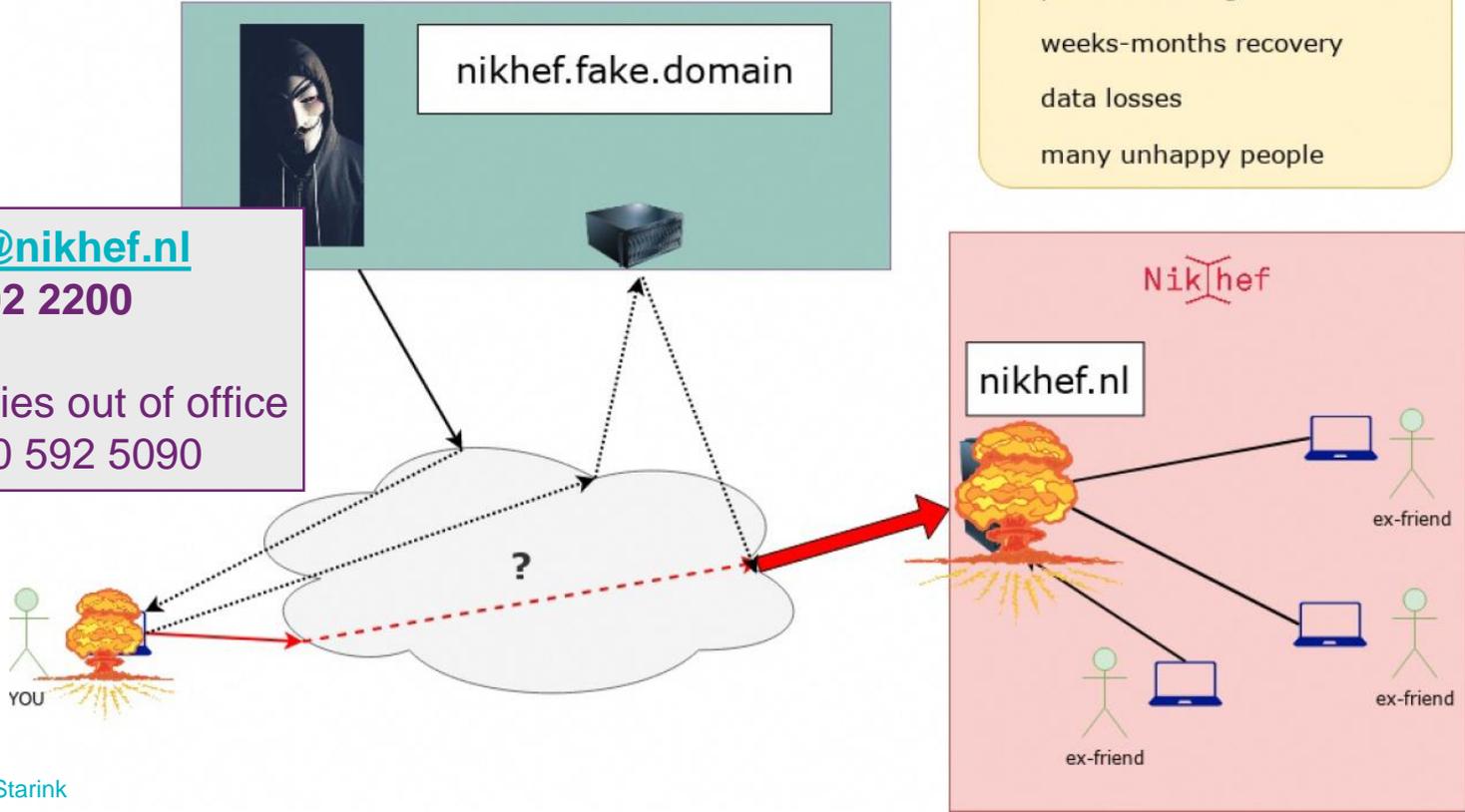


Image: Ronald Starink

Security - concretely



- Choose a **unique, strong password** & store in password **safe**
- Only **change** your password at sso.nikhef.nl. Don't enter it outside nikhef.nl.



- Emails:

- **Links** – does the domain match the site?
- Attachments – expected?



- Use **ssh** with public/private keys instead of password
- Encrypt connections with **eduVPN**
- Only use (legal!) software from **reliable** sources (e.g. CT Helpdesk) that you are free to use
downloads? **only** Open Source
– since you cannot *on your own* agree any other license for 'work'
- Use firewall & virus scanner, install (security) updates
- **Be critical & think!** (or ask)

Complementary aspect: Privacy and 'GDPR'

Protection of *personal data of identifiable individuals* and data leaks must be *formally reported (e.g. stolen laptops, phones, &c)*, so please:

- Don't **collect, store or publish** personal data
Unless strictly needed → need it anyway: you must **register** processing
- **Encrypt** harddisk, drives (also backup!)
- **Lock** your computer's **screen**
- Be **careful** with free online services
If the service is free, you are the product
- Possible privacy **incident** → **report** to privacy@nikhef.nl

Quizz

Is it a good idea to publish this on your personal home page?

```
login2.nikhef.nl — Konsole
[ronalds@solnan ~]$ qstat -n1 | head -20
burrell.nikhef.nl:

```

Elap Job ID Time	Username	Queue	Jobname	SessID	NDS	TSK	Req'd Memory	Req'd Time	S
12211103	burrell.nikke	generic7	ana_Offshell-def	93549	1	1	12000	24:00:00	R 2
3:35:28	wn-sate-059								
12211104	burrell.nikke	generic7	ana_Offshell-def	111466	1	1	12000	24:00:00	R 2
3:28:58	wn-sate-062								
12211105	burrell.nikke	generic7	ana_Offshell-def	78956	1	1	12000	24:00:00	R 2
3:19:34	wn-sate-061								
12211106	burrell.nikke	generic7	ana_Offshell-def	119700	1	1	12000	24:00:00	R 2
3:18:45	wn-sate-062								
12211107	burrell.nikke	generic7	ana_Offshell-def	124909	1	1	12000	24:00:00	R 2
3:14:13	wn-sate-062								
12211108	burrell.nikke	generic7	ana_Offshell-def	77690	1	1	12000	24:00:00	R 2
2:09:31	wn-sate-067								
12211109	burrell.nikke	generic7	ana_Offshell-def	42035	1	1	12000	24:00:00	R 2
2:14:21	wn-sate-062								
12211110	burrell.nikke	generic7	ana_Offshell-def	19471	1	1	12000	24:00:00	R 2
1:10:01	wn-sate-066								
12211111	burrell.nikke	generic7	ana_Offshell-def	123833	1	1	12000	24:00:00	R 1
9:32:43	wn-sate-059								
12211112	burrell.nikke	generic7	ana_Offshell-def	58256	1	1	12000	24:00:00	R 1
9:31:20	wn-sate-079								
12211113	burrell.nikke	generic7	ana_Offshell-def	22894	1	1	12000	24:00:00	R 1
9:16:55	wn-sate-058								

Knowledge safety

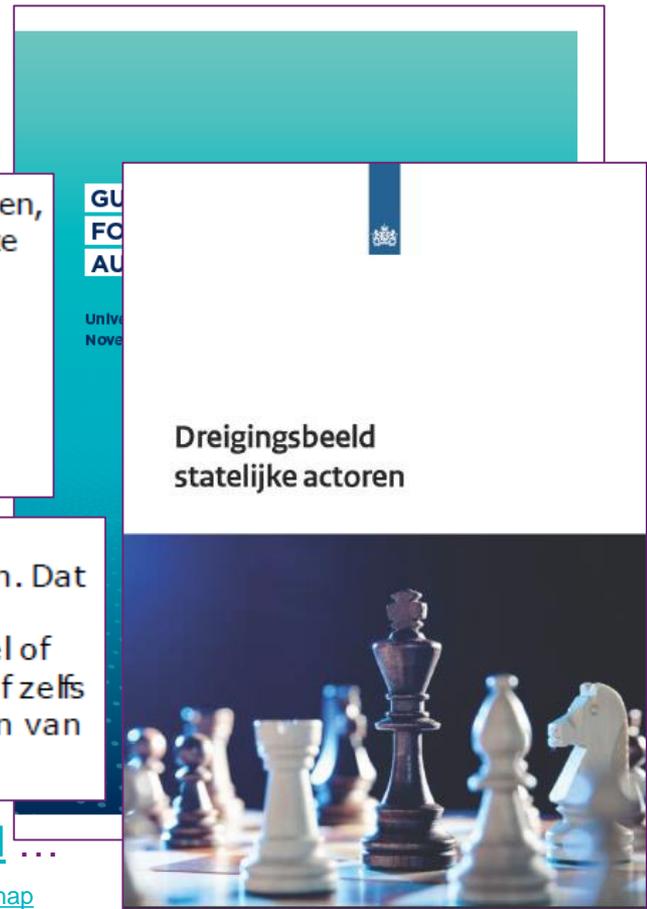
Nederlandse kennisinstellingen worden geconfronteerd met statelijke dreigingen, zoals de overdracht van kennis en technologie die vanuit het oogpunt van onze nationale veiligheid ongewenst is. Maar ook met vormen van heimelijke beïnvloeding en daarmee samenhangende (zelf)censuur die de academische vrijheid kan aantasten. Ook zijn er ethische overwegingen verbonden aan internationale samenwerkingen wanneer wordt samengewerkt met kennisinstellingen en bedrijven uit landen waar grondrechten niet worden gerespecteerd.

Het is daarbij belangrijk te benadrukken dat, hoe robuust maatregelen ook worden vormgegeven, een honderdprocentgarantie niet gegeven kan worden. Dat heeft ook te maken met de aard van de statelijke dreigingen in relatie tot internationale samenwerking: situaties zijn vaak niet zwart/wit ('het mag wel of het mag niet'). Het kan voorkomen dat iets wel mag, maar niet verstandig of zelfs ronduit schadelijk is. Het blijft uiteindelijk dus een kwestie van balanceren en van gedegen afwegingen maken van kansen en risico's.

Don't feel good? contact pietervb@nikhef.nl & infosec@nikhef.nl ...

<https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap>

<https://www.loketkennisveiligheid.nl/>



Knowledge safety – know with whom you collaborate

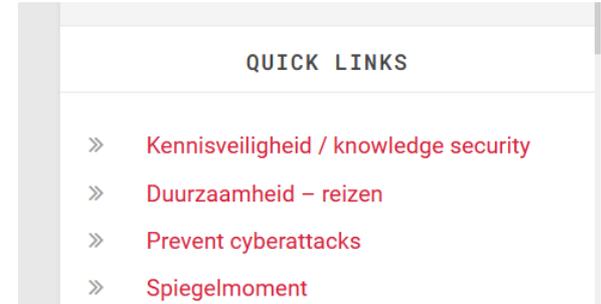
“as open as possible, as closed as necessary”

Four guidelines – of which 2-3 are relevant for you

- Secure foreign business trips
- Secure visitor procedure
- Secure (international) collaboration
- Secure recruitment and selection

Most importantly: they are risk-based, and you can (and in general should) ask for support if you hit a risk

- *example: the CT helpdesk has burner laptops on loan*



<https://intranet.nikhef.nl/kennisveiligheid-knowledge-security/>

One guideline highlighted as example: foreign travel

QUESTION 1: Risk areas		
Is your destination, or one of the destinations, located in a country that the Dutch General Intelligence and Security Service (AIVD) has designated as a country that poses a national threat (hereafter referred to as a 'risk country')? According to the AIVD, these countries are North Korea, Iran, Russia and China (PRC).	YES	no
QUESTION 2: Protected data and knowledge		
Are you taking research data or knowledge with you that are part of the institute's crown jewels? Use as source: the crown jewels document (internal). Ask the contact person at the institute or the institute manager.	YES	no
Are you taking research data or knowledge with you that fall within the sensitive technology area or a discipline to which export controls apply, such as a dual-use discipline? Use as source: (draft) list sensitive technologies (not yet public; inquire with the institute manager); https://www.rijksoverheid.nl/onderwerpen/exportcontrole-strategische-goederen/beleid-controle-strategische-goederen-en-diensten (in Dutch)	YES	no
Are you taking research data or knowledge with you that are risk-sensitive (such as information about politically sensitive research topics, information of, or about, confidential sources, highly privacy-sensitive data, or something similar)?	YES	no



At least one 'YES' to question 1 AND to question 2

Significant risks are associated with this trip. In some cases, this can even violate export legislation. Consult with the institute director or institute manager about changes to the trip and contact the ICT manager about the safe use of ICT devices. Refer to the checklist below.

At least one 'YES' to question 1 OR to question 2

This trip concerns a risk area or sensitive knowledge. Please contact the ICT manager about the secure use of ICT devices. During the trip, be aware of knowledge security and if necessary refer to the checklists below.

For destinations flagged as risky, we then provide burner laptops, you must reset any credentials used afterwards, and we monitor activity from the destination region during the trip

23.0523-EN-NWO-I-Secure-foreign-business-trips.pdf

You are not alone: there's help – lots of it

Don't know where to start? CT Knowledge Base!

- <https://kb.nikhef.nl/ct>

Wonder why it is not working as before?

- <https://nikhef.status.io/> - you can also *subscribe*

Stoomboot full? How does the network look like?

- <https://www.nikhef.nl/pdp/>
- stbc-users@ list (<https://mailman.nikhef.nl/>)
- Nikhef Mattermost #stbc-users channel

and your own group pages for analysis and workflow scripts and frameworks

Nikhef CT User Documentation

CT User Documentation

Home

Accounts >

Calendar & Mail >

Printing

Laptops & Hardware >

Network (WiFi/VPN) >

Phones >

Meeting Rooms

Remote Access Desktops & Servers ▾

Working Remotely Best Practices

SSH access and configuration

Remote Desktop

Configure remote desktop

SOCKS Proxy Tutorial

Course Environment

Home

- Accessing email
- Account request
- Adobe Creative Cloud
- Acceptable Use Policy
- CPU batch jobs
- GPU batch jobs
- Bitlocker
- Change Mattermost to GitLab authentication
- Change your password
- Conda environments
- Configure remote desktop

And there's the helpdesk!

Please ask when something does not work as expected!

if you don't tell the helpdesk, nobody will know and thus nobody will ever fix the issue when it's broken!

- Generic software (MS office and such)
- Services (mail, wifi, network, **backup**, printing)
- Hardware (laptop or desktop, monitor, docking station)
- Cables and small things
- Account (password, SSO, MFA for ResearchDrive)
- Video conference equipment (OWL)

helpdesk@nikhef.nl

+31 20 592 2200

<https://servicedesk.nikhef.nl/>

H1.22, next to the vide, from
~8.30 till 17.00

help the helpdesk help you: can you reproduce it? are you the only one in the group? did you change anything?

More practical help ... for data management

Simple thing: don't try to do everything on your own, use what's already there!

Nikhef has no dedicated 'data stewards' (since most of that is done in our collaborations), but we do have data management support

- <https://nikhef.nl/pdp/rdm/>
- a lot of existing data management plans (not all public)
- contact: rdm-support@nikhef.nl (goes to davidg@, templon@, and ronalds@)
- if you need data management advise for an external future grant or position, also ask (we might well be able to help or link you up internationally)

Elsewhere? look for dedicated 'Data Stewardship' group or 'research support' office

Same thing for processing ...

Open Science and FAIR data are nice concepts, but it's easy to drown ...

- use provided tools (from your experiment, from Nikhef CT/PDP, from our DCC)
- make sure data is safe and managed (any USB or external drive will fail in the end)
- keep copious logs and use organised (cookie-cutter) and time-stamped notebooks
- don't expose confidential data inadvertently (e.g. thinking your home page is secret)

The CT documentation has endorsed central services and guides

<https://edu.nl/arvc4>

Research tooling and some data integrity guidance is on the Nikhef PDP pages

<https://www.nikhef.nl/pdp/doc/>

Open Science (and reproduction packages) helps ...

“building reproducible data and software is hard, and takes time ...
... yet is an essential part of the integrity and value of your results”

- make sure your data is in the right place when you finish up a chapter
 - software in gitlab.nikhef.nl or your collaboration software versioning system (git.cern.ch,...)
 - data should not remain on a laptop or home directory, but in dCache (for re-creatable data) or archived (/project for things the group will re-use and are ‘smallish’, or in dCache + SURF Data Archive, in archive.nikhef.nl, or distributed in collaboration infra for e.g. WLCG)
 - notes, logbooks, executable notebooks: in /project *with good descriptive meta-data* and in archive.nikhef.nl or Zenodo (for things that do not need to remain private)

... and if in doubt, talk about this in your group, or with your supervisors, or mail us!

<https://intranet.nikhef.nl/personeel-organisatie-po/> and <https://www.nikhef.nl/medewerker/els-de-wolf/>;
and for NWO-IRI se <https://intranet.nikhef.nl/2022/01/20/vertrouwenspersonen-wetenschappelijke-integriteit-confidential-advisers-scientific-integrity/>

General computing, login, mail, eduVPN helpdesk@nikhef.nl or <tel:+31205922200>
mattermost, zoom, account reset, SURFdrive, ...

Stoomboot and local dCache

stbc-users@nikhef.nl for self-help

Mattermost: **Nikhef-members#stbc-users**

How to best use distributed computing

stbc-admin@nikhef.nl, grid.support@nikhef.nl

Security concerns or incidents

security@nikhef.nl or <tel:+31205925090>

prefer to read up?

<https://kb.nikhef.nl/ct/> for all answers!

Office Hours in the central Vertex
every **1st Thursday** of the month **at 1300**,
cake for everyone with an ICT question!

and there's <https://nikhef.status.io/>





Maastricht University

Nikhef

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>

