GÉANT
Networks • Services • People

eduVPN
Safe and Trusted

Rogier Spoor, SURFnet

Tangui Coulouarn, DeiC

TNC19, Tallinn, 18 June 2019

Agenda

- Why eduVPN?
- What has been done?
- How to deploy & service model
- Future work/roadmap

eduVPN

Safe and trusted

Securing access for remote staff and students

Why do we need eduVPN?

Working away from the office is the norm - Hotels, Cafes, Airports and Train Stations are the new offices

“How can I get WiFi?” is often the first question when attending meetings outside the office

BUT not all WiFi is born equal….

- While eduroam is a secure environment with authenticated access and local encryption many public WiFi services are not
- Unsecured hotspots
- Shared access passwords
- “Free” WiFi with web login screens

Are our users (and their data) safe?

The Risks of public WiFi

For Users

Unprotected WiFi can expose usernames and passwords

Content filtering on public WiFi may deny access to sites

Possibility of malware injection

Unknown and untrusted proxies could redirect users to fraudulent sites

For IT Support

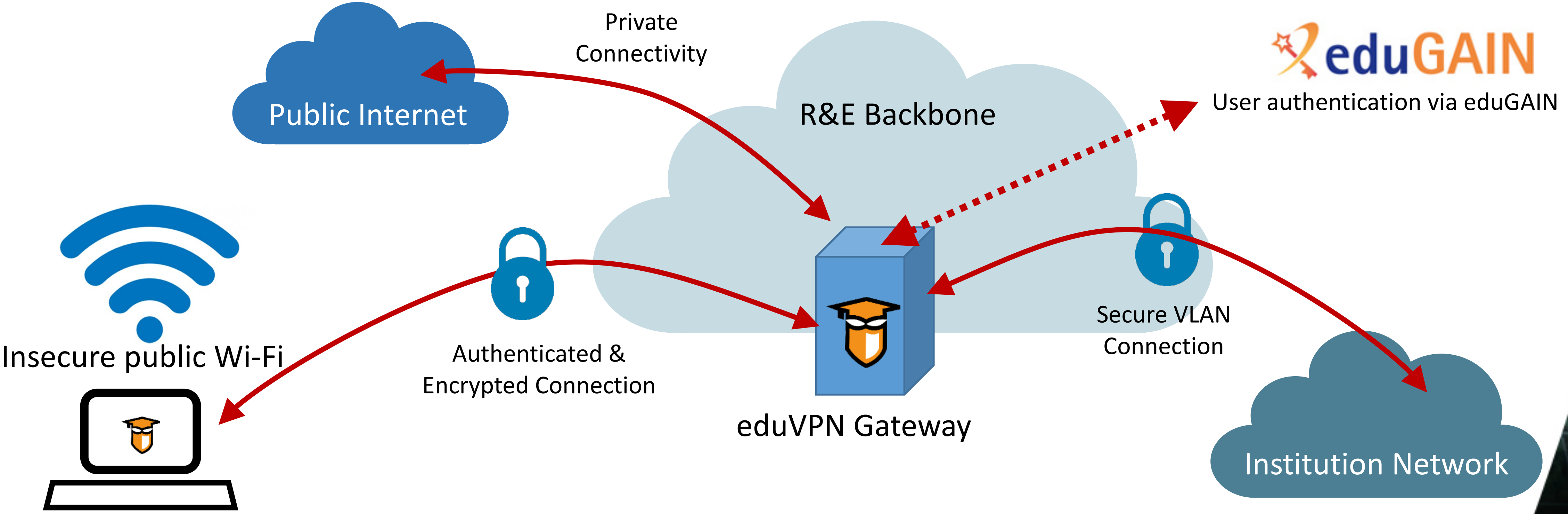
Managed devices can insecurely connect to unknown networks

Risk of data loss

Ad-hoc, unmanaged VPN solutions may proliferate

eduVPN - securing access for remote users

eduVPN provides easy-to-use client software and a secure gateway to authenticate users and encrypt data.



The 2 uses of eduVPN

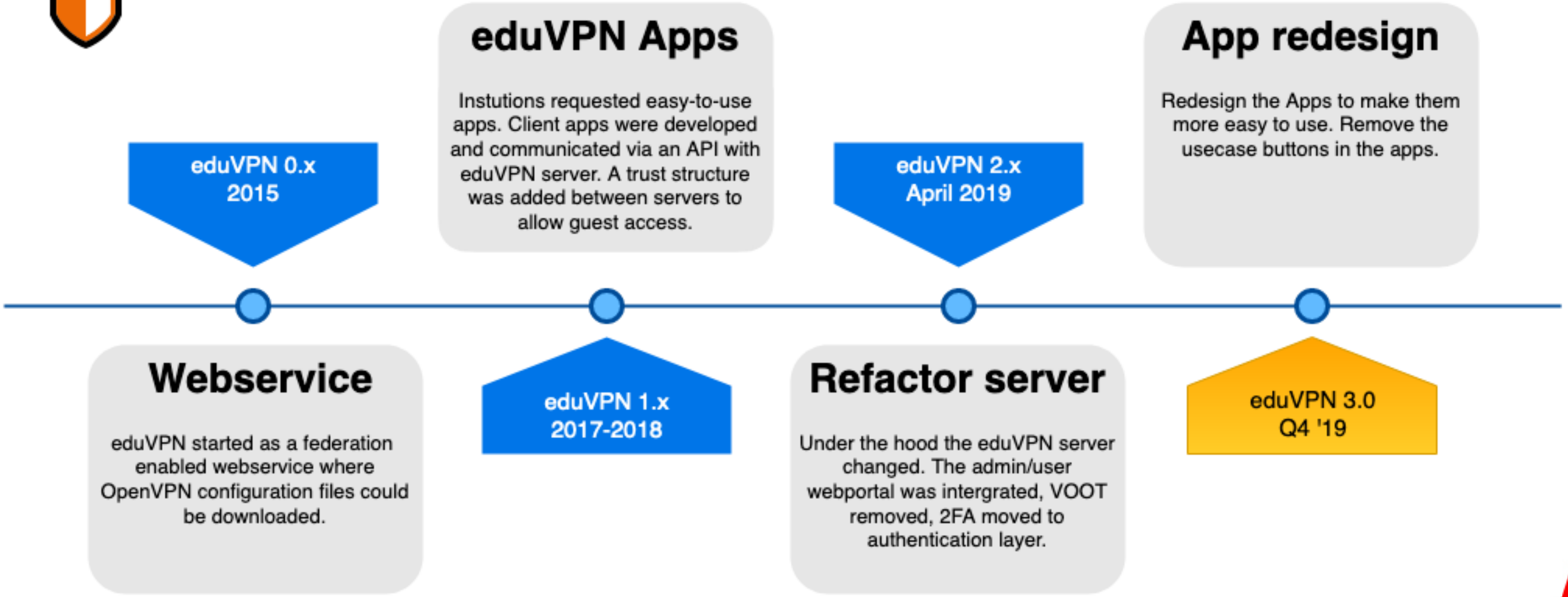
- **Secure Internet**: eduVPN instance gives access to the public Internet.
  - Possibility for guest access
  - Possibility for filtering for undesired traffic, services or content (e.g. add-free profile implemented in Germany)
  - Privacy and security enhancing

- **Institute access**: eduVPN gives access to private resources
  - Stand-alone implementation
  - Managed service
  - Possibility for strong authentication
  - Profiles for different users/groups

Open-Source VPN software comparison

Product	Technology	Scalable	Encryption	Audit	Hide traffic	Rebrandable apps	Enterprise Identity
Algo	IPsec & IKEv2	Personal or small scale	Modest - Good	No	no	no	no
WireGuard	WireGuard	Protocol supports CPU scaling	State of the Art	Formal verification	no	Yes	no
PPTP	PPTP	Not really	Bad	yes	no	no	no
SoftEther	Various	Large scale/enterprise	Modest - Good	Fuzzing	yes	yes	no
OpenVPN 2.x	OpenVPN 2.x	Personal or small scale	Modest - Good	Yes, various	yes	no	no
eduVPN - Let's Connect!	OpenVPN 2.x	Large scale/enterprise	Good	Clients and Server	yes	Yes	yes, SAML
OpenConnect	AnyConnect	Large scale/enterprise	Modest - Good	Unknown	yes	Yes	Work in Progress

eduVPN software evolution



eduVPN 0.x
2015

Webservice

eduVPN started as a federation enabled webservice where OpenVPN configuration files could be downloaded.

eduVPN 1.x
2017-2018

eduVPN Apps

Instutions requested easy-to-use apps. Client apps were developed and communicated via an API with eduVPN server. A trust structure was added between servers to allow guest access.

eduVPN 2.x
April 2019

Refactor server

Under the hood the eduVPN server changed. The admin/user webportal was intergrated, VOOT removed, 2FA moved to authentication layer.

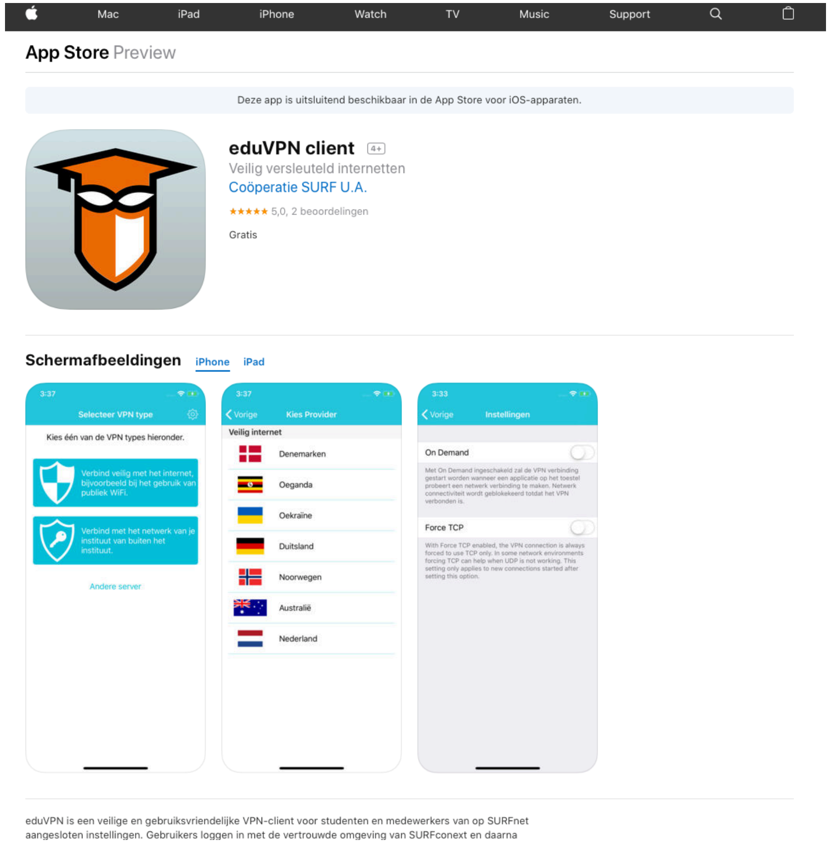
eduVPN 3.0
Q4 '19

App redesign

Redesign the Apps to make them more easy to use. Remove the usecase buttons in the apps.

Audited apps for different platforms

- iOS
- MacOS
- Windows
- Android
- Linux



Deze app is uitsluitend beschikbaar in de App Store voor iOS-apparaten.

eduVPN client

Veilig versleuteld internetten

Coöperatie SURF U.A.

★★★★★ 5,0, 2 beoordelingen

Gratis

Schermafbeeldingen

Kies één van de VPN types hieronder.

Verbind veilig met het internet, bijvoorbeeld bij het gebruik van publiek WiFi.

Verbind met het netwerk van je instituut van buiten het instituut.

Veilig internet

Denemarken
Oeganda
Oekraïne
Duitsland
Noorwegen
Australië
Nederland

On Demand

Met On Demand ingeschakeld zal de VPN verbinding gestart worden wanneer een applicatie op het toestel probeert een netwerk verbinding te maken. Netwerk connectiviteit wordt geblokekeerd totdat het VPN verbonden is.

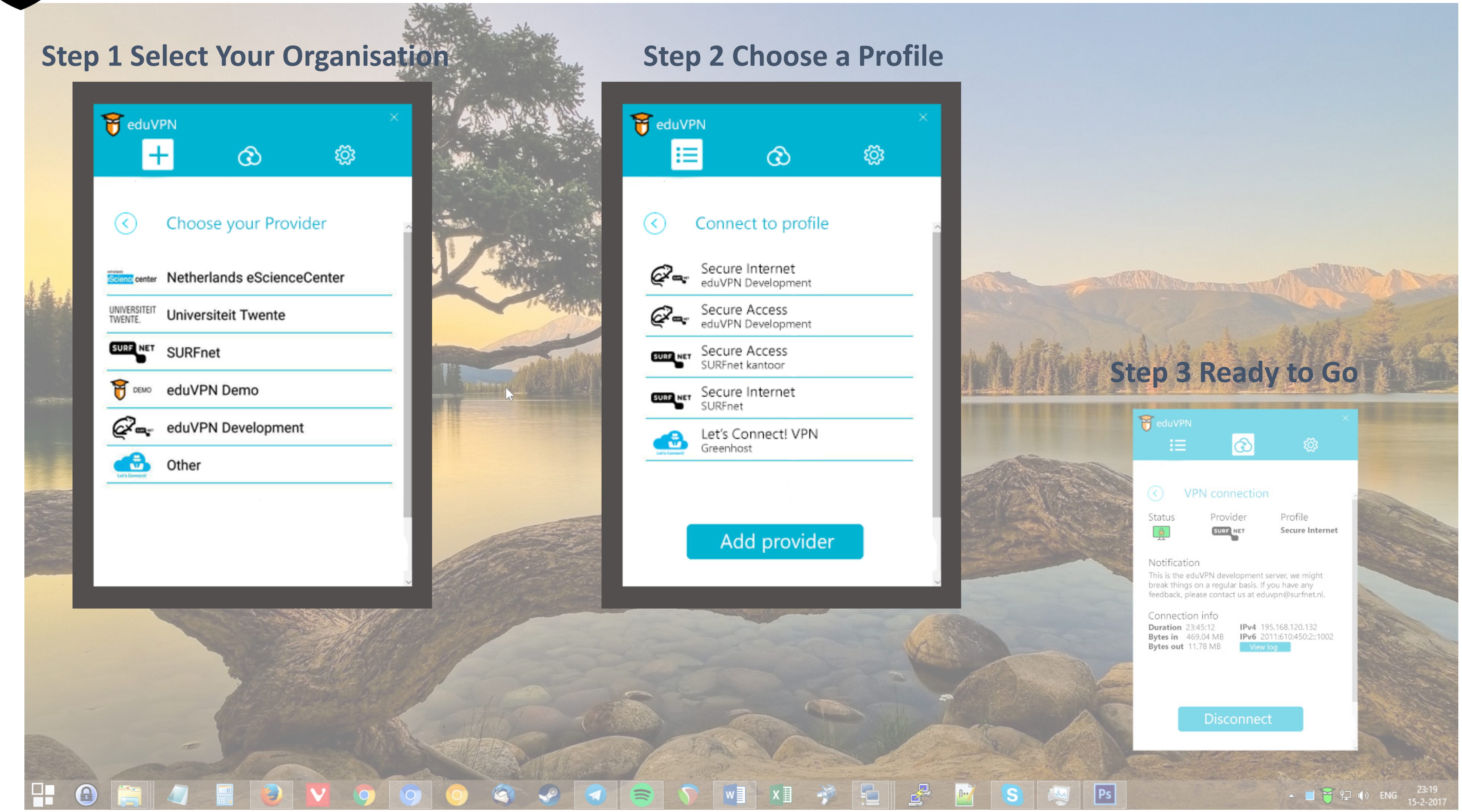
Force TCP

With Force TCP enabled, the VPN connection is always forced to use TCP only. In some network environments forcing TCP can help when UDP is not working. This setting only applies to new connections started after setting this option.

eduVPN is een veilige en gebruiksvriendelijke VPN-client voor studenten en medewerkers van op SURFnet aangesloten instellingen. Gebruikers loggen in met de vertrouwde omgeving van SURFconext en daarna

All eduVPN software approved by GÉANT Dec ’18

Three Steps to Safety



Step 1 Select Your Organisation

Choose your Provider

- Netherlands eScienceCenter
- Universiteit Twente
- SURFnet
- eduVPN Demo
- eduVPN Development
- Other

Step 2 Choose a Profile

Connect to profile

- Secure Internet
  eduVPN Development
- Secure Access
  eduVPN Development
- Secure Access
  SURFnet kantoor
- Secure Internet
  SURFnet
- Let's Connect! VPN
  Greenhost

Add provider

Step 3 Ready to Go

VPN connection

Status

Provider

Profile
Secure Internet

Notification
This is the eduVPN development server, we might break things on a regular basis. If you have any feedback, please contact us at eduvpn@surfnet.nl.

Connection info
Duration 23:45:12
Bytes in 469.04 MB
Bytes out 11.78 MB
IPv4 195.168.120.132
IPv6 2011:610:450:2::1002
View log

Disconnect

How is secure internet implemented?

NREN implementation

Each participating NREN offers a gateway to their participating institutions

GÉANT Project co-ordinates development and standards

7 NRENs currently offering gateways

Holland, Denmark, Australia, Uganda, Ukraine, Norway, Germany

Policy for a federated service

- The technical governance of eduVPN lies in the Commons Conservancy

- The service governance is defined in a policy document
  - Inspired by eduroam
  - Largely up to national operators (NRENs) to ensure compliance in a country
  - Security and incident response obligations

Guest access and abuse redress in a privacy-by-design service

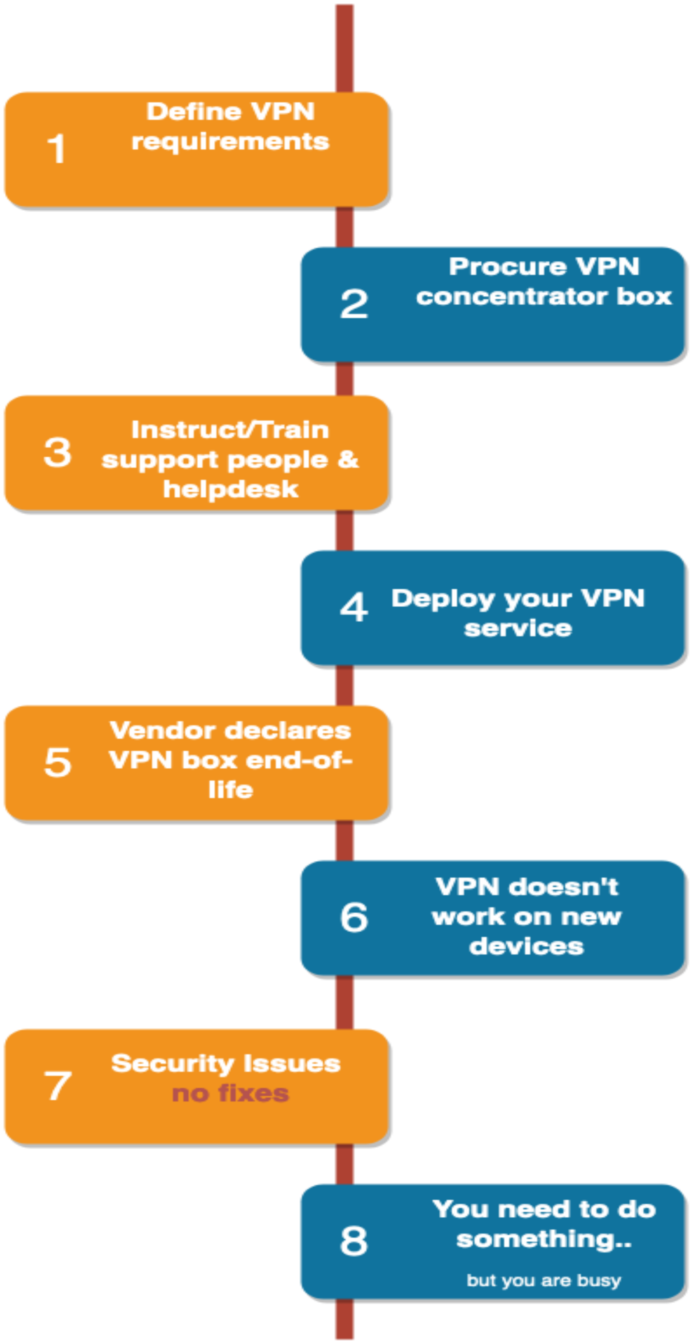
- An eduVPN operator can not identity an user alone
- Abuse can be traced to pseudonym when eduVPN instance is using public IP adresses
- Pseudonym -> person requires collaboration of the originating NREN/IdP

The 2 uses of eduVPN

- **Secure Internet**: eduVPN instance gives access to the public Internet.
  - Possibility for guest access
  - Possibility for filtering for undesired traffic, services or content (e.g. add-free profile implemented in Germany)
  - Privacy and security enhancing

- **Institute access**: eduVPN gives access to private resources
  - Stand-alone implementation
  - Managed service
  - Possibility for strong authentication
  - Profiles for different users/groups

Classic VPN service lifecycle



1 Define VPN requirements

2 Procure VPN concentrator box

3 Instruct/Train support people & helpdesk

4 Deploy your VPN service

5 Vendor declares VPN box end-of-life

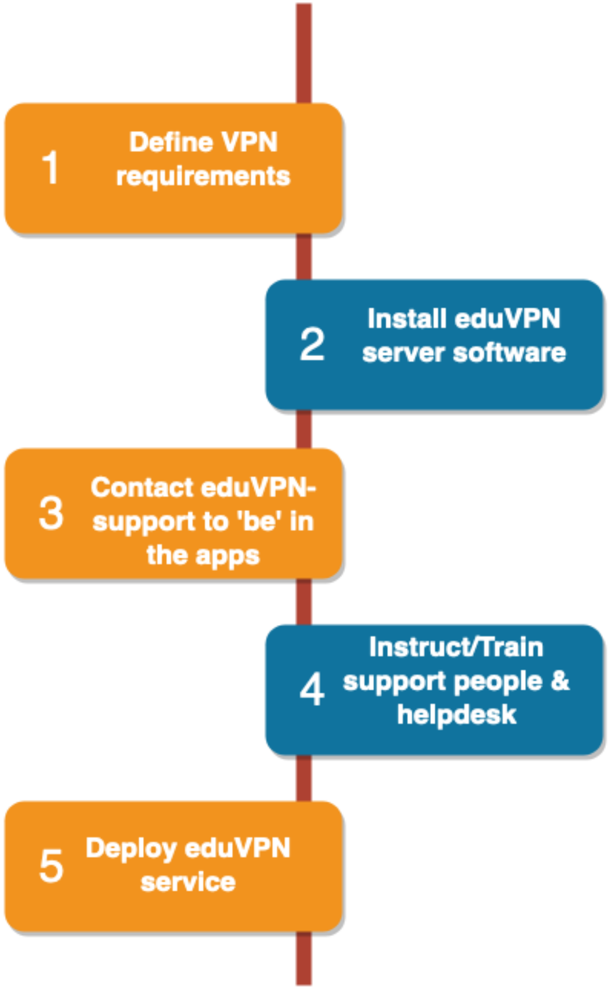
6 VPN doesn't work on new devices

7 Security Issues no fixes

8 You need to do something..

but you are busy

eduVPN service approach



1 Define VPN requirements

2 Install eduVPN server software

3 Contact eduVPN-support to 'be' in the apps

4 Instruct/Train support people & helpdesk

5 Deploy eduVPN service

We make sure:

- eduVPN apps work on generic devices
- client apps & eduVPN server will be maintained

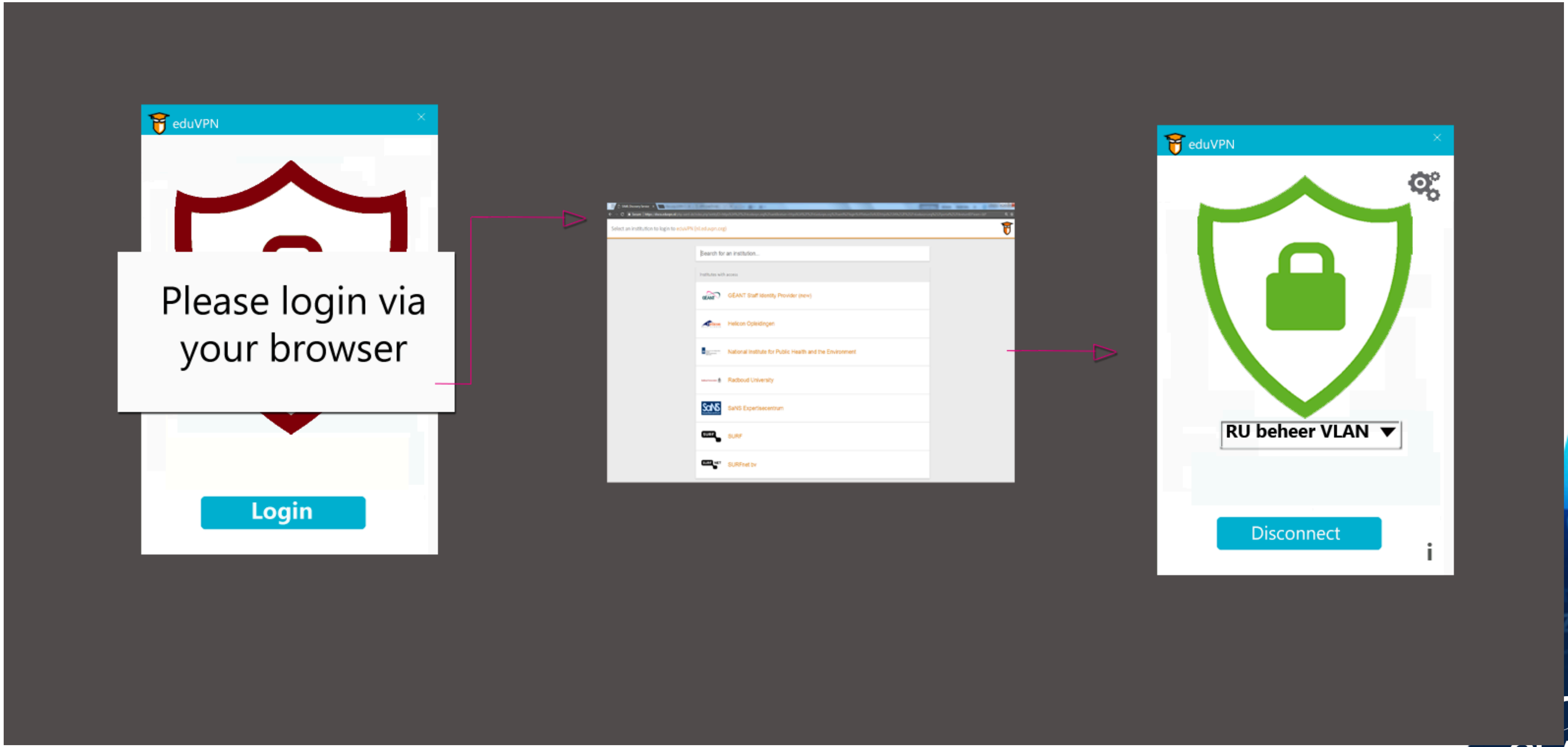
eduVPN Institute Access as a Managed Service

- Model currently implemented in the Netherlands
- eduVPN instance managed centrally by SURFnet
- Lightpath back to the private resource
- Support by SURFnet
- No need for hardware on campus or licensing limitations

Future steps

- Service Positioning GÉANT
- WireGuard support
- Investigate other usecases, like server Mesh
- New apps UI -> easier to use for non-tech users
- Continue to support community
- Continue eduVPN pilots

Future app design (impression)



eduVPN

Please login via your browser

Login

Select an institution to login to eduVPN (nl.eduvpn.org)

Search for an institution...

Institutes with access

- GÉANT Staff Identity Provider (new)
- Helicon Opleidingen
- National Institute for Public Health and the Environment
- Radboud University
- SaNS Expertisecentrum
- SURF
- SURFnet bv

eduVPN

RU beheer VLAN ▼

Disconnect

Involved Organisations

2014

Started simple VPN webservice

SURF NET

2016

Client app development start.
SIDN fund co-fund the open-source development.
NORDUnet sponsoring.

SIDNfonds

NORDUnet Nordic Gateway for Research & Education

SURF NET

2017

Vietsch foundation co-fund easy-to-use apps.
RIPE Community fund co-fund development. Software Governance via Commons Conservancy foundation.
AARNet, DeiC, NORDUnet, GÉANT, SURFnet in board.
NLnet opened eduVPN fund.

vietsch foundation

DeiC Danish e-Infrastructure Cooperation

aarnet Australia's Academic and Research Network

GÉANT

RIPE

THE COMMONS CONSERVANCY

nlnet

SIDNfonds

NORDUnet Nordic Gateway for Research & Education

SURF NET

2018

eduVPN entered GÉANT project
eduVPN software approved by GÉANT. URAN, RENU, UNINETT and DFN run eduVPN pilot.

RENU

uran Ukrainian Research and Academic Network

UNINETT

DFN deutsches forschungsnetz

DeiC Danish e-Infrastructure Cooperation

aarnet Australia's Academic and Research Network

GÉANT

RIPE

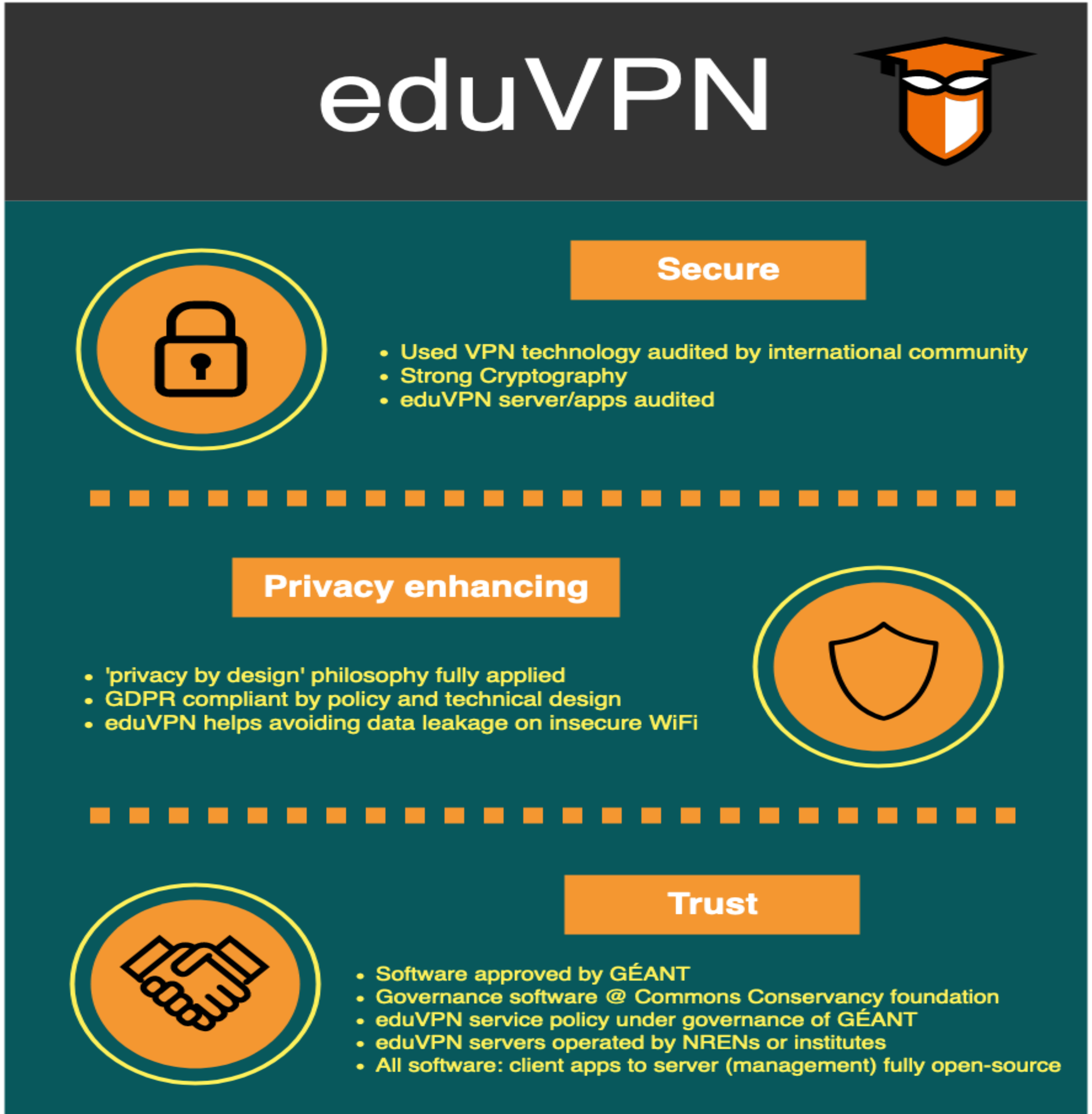
THE COMMONS CONSERVANCY

nlnet

SIDNfonds

NORDUnet Nordic Gateway for Research & Education

SURF NET



eduVPN

Secure

- Used VPN technology audited by international community
- Strong Cryptography
- eduVPN server/apps audited

Privacy enhancing

- 'privacy by design' philosophy fully applied
- GDPR compliant by policy and technical design
- eduVPN helps avoiding data leakage on insecure WiFi

Trust

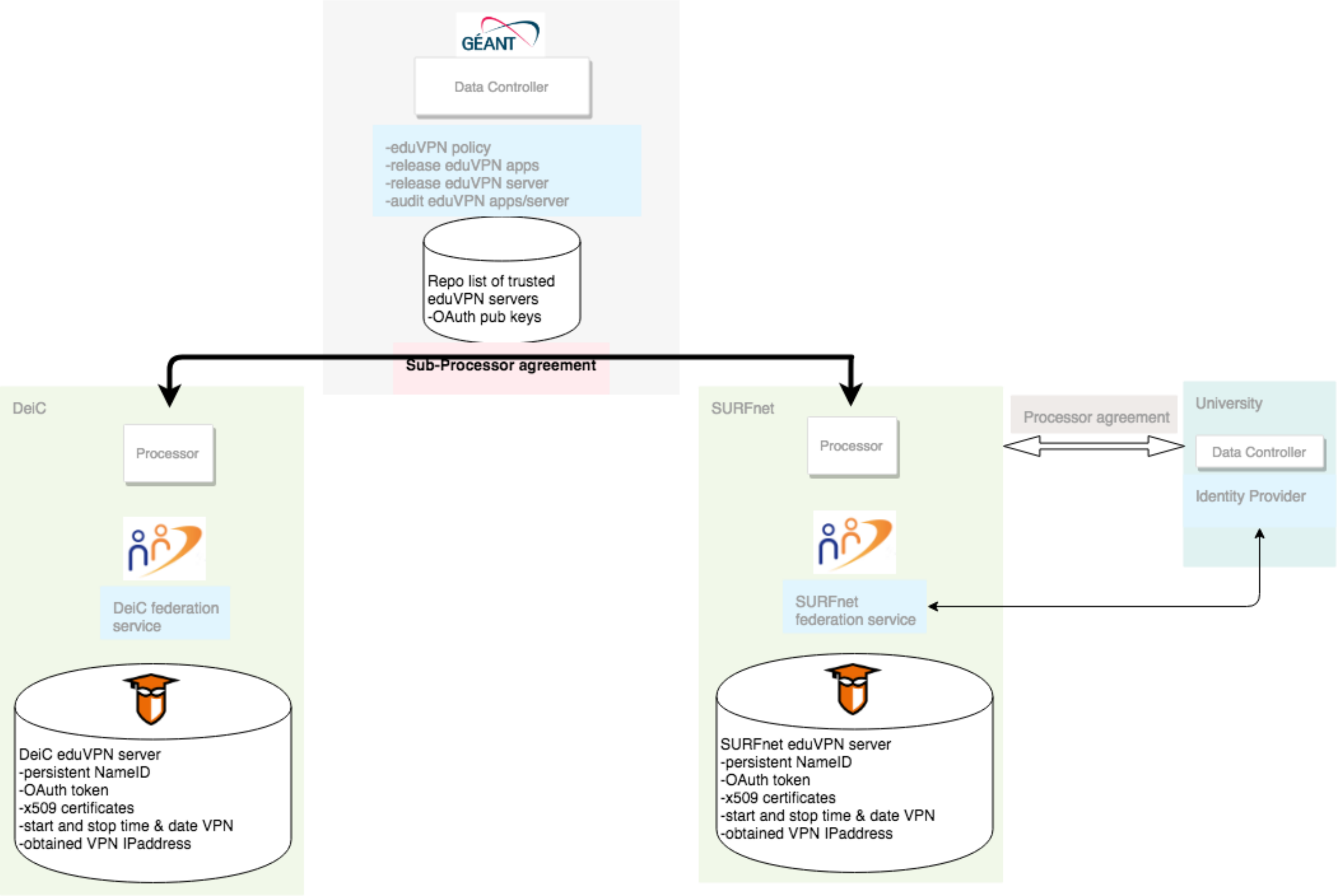
- Software approved by GÉANT
- Governance software @ Commons Conservancy foundation
- eduVPN service policy under governance of GÉANT
- eduVPN servers operated by NRENs or institutes
- All software: client apps to server (management) fully open-source

Contact

Email: eduvpn-support@lists.geant.org

GDPR Compliance (extra slide)

eduVPN GDPR Flows



GÉANT

Data Controller

-eduVPN policy
-release eduVPN apps
-release eduVPN server
-audit eduVPN apps/server

Repo list of trusted eduVPN servers
-OAuth pub keys

Sub-Processor agreement

DeiC

Processor

DeiC federation service

DeiC eduVPN server
-persistent NameID
-OAuth token
-x509 certificates
-start and stop time & date VPN
-obtained VPN IPaddress

SURFnet

Processor

SURFnet federation service

SURFnet eduVPN server
-persistent NameID
-OAuth token
-x509 certificates
-start and stop time & date VPN
-obtained VPN IPaddress

Processor agreement

University

Data Controller

Identity Provider