

12-02-2021

Deliverable D8.3

eduVPN v2.0

Release of New eduVPN Client Apps

Deliverable D8.3

Contractual Date:	31-01-2021
Actual Date:	12-02-2021
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 3.5
Nature of Deliverable:	O (Other)
Dissemination Level:	PU (Public)
Lead Partner:	DeiC/NORDUnet
Document ID:	GN4-3-21-406E3D
Authors:	Tangui Coulouarn (DeiC/NORDUnet)

© GÉANT Association on behalf of the GN4-3 project.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document presents the second generation eduVPN client apps, which were released during Q4 2020. The new design of the client apps simplifies the user experience by hiding complexity. It puts identity discovery first and solves the service discovery issue users were previously confronted with. All apps now also have the same look-and-feel and the same flow.

Table of Contents

Executive Summary	1
1 Introduction	2
2 New Apps Development	3
2.1 Limitations of Existing Apps	3
2.2 New Apps	5
2.2.1 Similar Look-and-Feel	5
2.2.2 New Flow: Prioritising Identity Provider Discovery	7
2.2.3 Release Dates and Change Log	8
2.2.4 IPR and Licensing	8
3 Conclusions	9
References	10
Glossary	10

Table of Figures

Figure 2.1: Flow in the existing apps	3
Figure 2.2: Flow in the old android client app	4
Figure 2.3: Style guide for eduVPN developers	5
Figure 2.4: Guidelines for the successive screens in the different apps	6
Figure 2.5: Example of an instance web-portal	6

Table of Tables

Table 2.1: Release dates and change logs of the second generation eduVPN apps	8
---	---

Executive Summary

This document presents the second generation eduVPN client apps which were released during Q4 2020.

eduVPN is a service by multiple independent providers (NRENs, universities, research institutions, etc.). It serves two very different and independent use cases:

1. Institute access (access to the private network of an institution).
2. Secure internet (access to a public network through a safe gateway).

The requirements for these two use cases differ. For example, in the case of secure internet instances, guest access is normally allowed, i.e. a user authorised on a secure internet instance by a provider can use other secure internet instances but this is not the case for users of institute access instances. Typically, an end-user has access both to one instance for Institute Access and all instances for Secure Internet.

The new design of the client apps simplifies the user experience by hiding this complexity. It puts identity discovery first and solves the service discovery issue users were confronted with. All apps now also have the same look-and-feel and the same flow.

The design and implementation of the apps was carried out in collaboration with the Design for Security [[D4S](#)] project, a third- party project that has received funding from [[NGI TRUST](#)].

1 Introduction

eduVPN is a VPN solution [[eduVPN](#)] designed to provide secure access to both private institutional networks (as in typical corporate solutions) and public networks.

eduVPN has already been functional for several years and has grown rapidly; it started as a project in SURF - the Dutch National Research and Education Network (NREN) - and it is now offered by 16 NRENS as well as around 100 higher education institutions which have replaced their traditional VPN solutions with eduVPN (this is the case in Cyprus, Finland, France, Germany, Indonesia, Ireland, Kenya, Malaysia, the Netherlands, New Zealand, Norway, Pakistan, Poland, Portugal, Romania, South Africa, Sri Lanka, Sweden and Uganda, among others)¹. A few private companies outside the field of research and education also use the software which is in these cases branded as Let's Connect! (for example, XS4ALL in the Netherlands).

The success of eduVPN is related to a number of factors linked to the environment in which it is adopted and supported. The NREN community and GÉANT have experience and have proven their capacity to support similar services (eduroam, eduGAIN). The growth in the number of deployments of eduVPN has been accelerated by the COVID-19 pandemic and the need for secure solutions for remote working. The increasing number of adopters is also related to the properties of the software. eduVPN has rich features [[eduVPN Docs](#)], its code is regularly audited, it is one of the only fully open-source solutions (both on server and client sides) and it can scale to a large number of users. Last but not least, eduVPN is easy to use and, over the years, different clients have been developed for different operative systems. The vision is that end-users should be able to install and use a VPN on any of their devices with a few clicks.

As the number of instances and users grew, some of the limitations of the first generation of apps became apparent. In particular, end-users had to select which eduVPN instance they wanted and were authorised to use and the existing flows were not adapted to such instance or service discovery.

This document describes some of the issues the new apps have fixed. Part of the redesign has been done through the D4S project, funded by the 1st NGI Trust Open Call².

¹ <https://status.eduvpn.org> provides a list of instances which are hard coded in the apps. However, as eduVPN is fully open source and free to use, a significant number of institutions chose to use it without being in the apps. The list referred to above is therefore incomplete.

² D4S stands for "Design 4 Security – Making VPNs easy" and it is a third-party project that has received funding from the NGI_Trust, the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825618. The partners in D4S were the Technical University of Denmark, The Royal Danish Academy (KADK) and Commons Caretakers. The project included user consultation (interviews, workshops).

2 New Apps Development

This section describes some of the limitations of the existing apps and how these were addressed in the new apps. The release dates for the new versions of the apps are also given.

2.1 Limitations of Existing Apps

The flow and functioning of the eduVPN client apps of the 1st generation exposed the end-user to a diversity of design and graphical interfaces. But the flow was roughly similar in all apps.

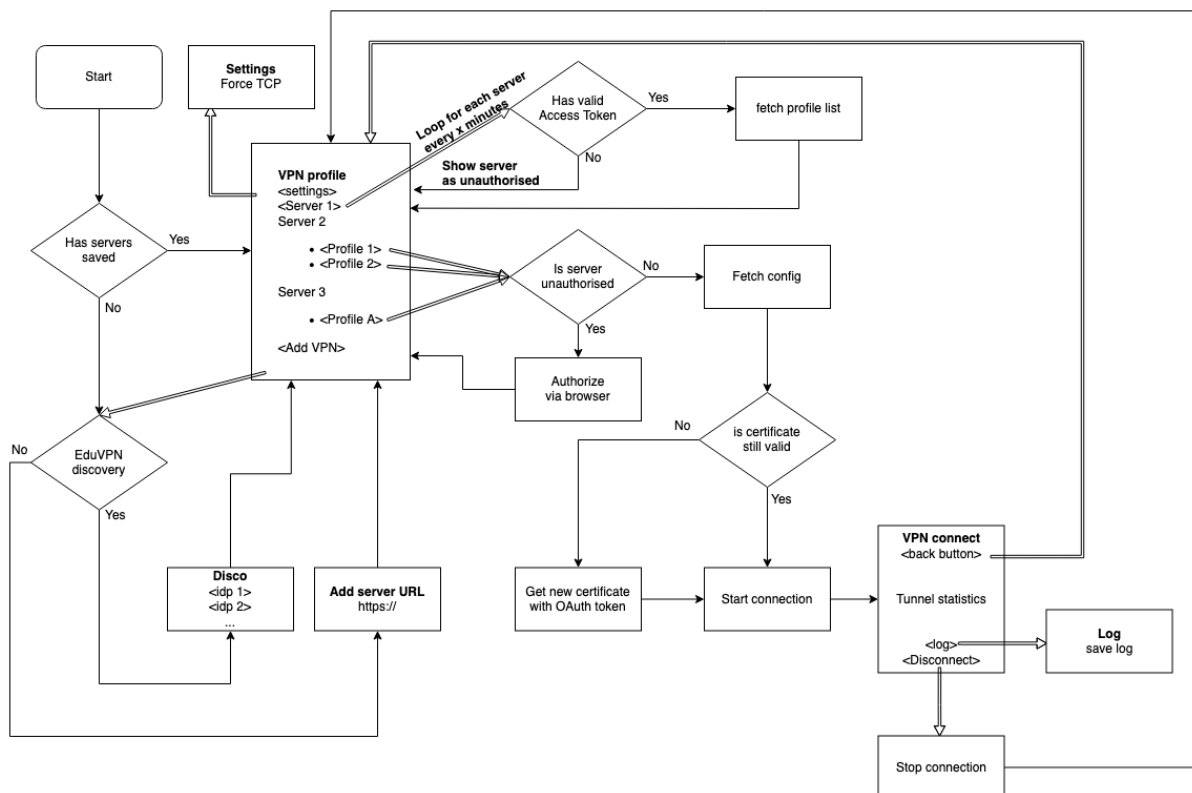


Figure 2.1: Flow in the existing apps

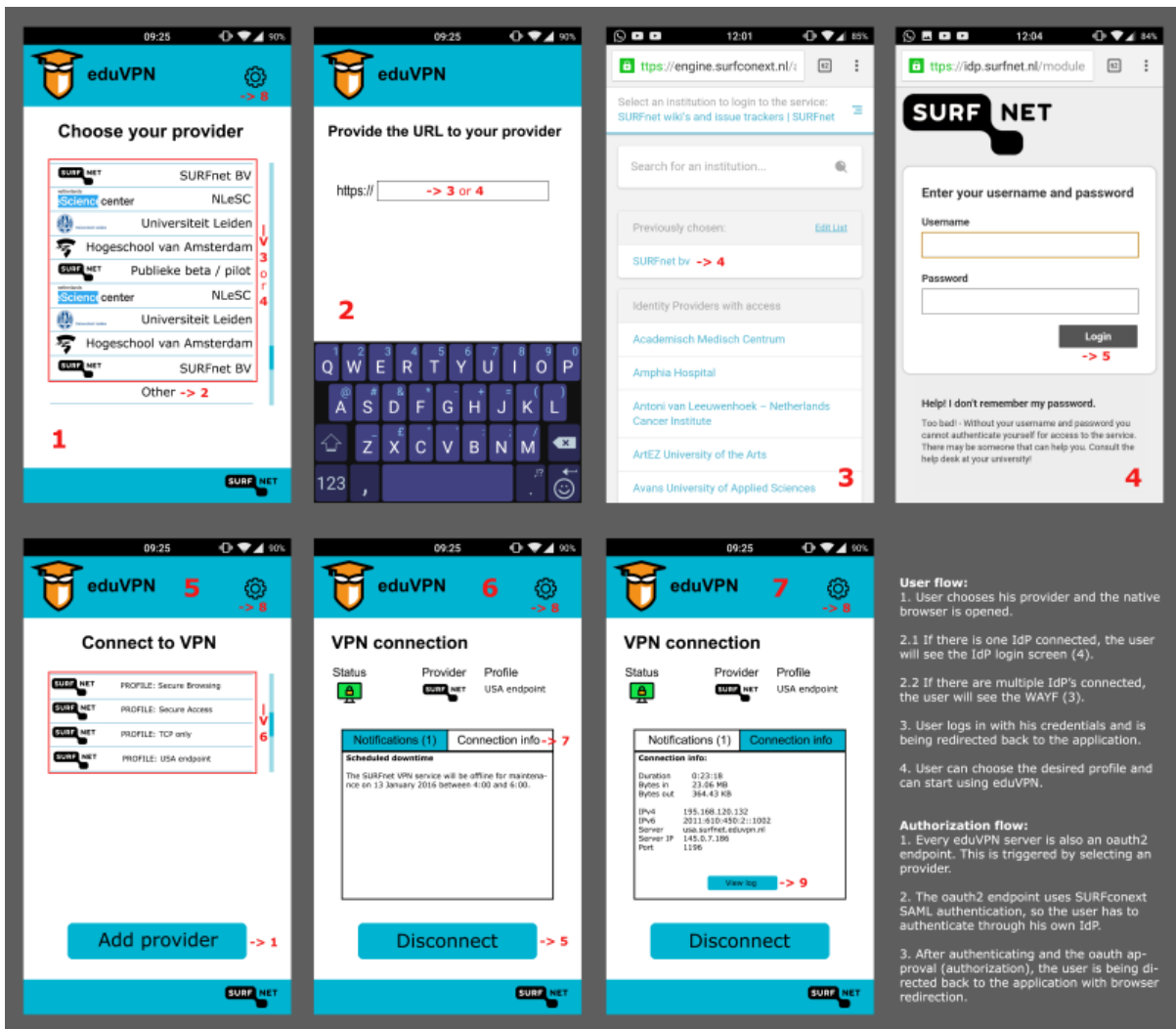


Figure 2.2: Flow in the old android client app

In eduVPN, the same apps are used for two quite different purposes. Some instances offer “institute access”, i.e., access to a private network as with other “corporate VPN” solutions. Other instances, typically managed by NRENs, offer “secure Internet”, i.e., access to public networks / the Internet. These instances are operated by different independent stakeholders. While secure internet instances normally allow for guest access, i.e., an end-user authorised on another secure internet instance can use all secure internet instances, this is not the case for institute access.

Previously, after choosing which use case they wanted to use (institute access or secure internet), the end-user had to select their server/instance from a list (or provide the URL of the instance). This would happen in the app.

The user was then typically sent to an Identity Provider (IdP) discovery service in a web browser (screen 3 in Figure 2.2 above) with a different look-and-feel. After selecting their IdP, they would then have to log in on their institution page (with yet again a different look-and-feel) before approving the connection on another webpage and then being redirected to the app.

This flow and the various different designs of the interfaces in this process were not perceived as “professional” and trustworthy by many users³.

The variety of graphical designs were due to the fact that the client apps for the different operating systems were historically developed at different periods and by different developers⁴.

To summarise, the client apps were confusing to end-users as they had to perform two kinds of discovery, eduVPN instance discovery (“which instance do I want to / can I use?”) and identity provider discovery (“where am I from?”), which was further compounded by the different look-and-feel between the apps.

The main issue with the flow was that it was assumed and necessary that end-users knew which use they wanted to make of eduVPN as well as what they were entitled to use.

2.2 New Apps

2.2.1 Similar Look-and-Feel

It was decided to impose the same look-and-feel and graphical identity for all new apps as well as the website and the different screens that an end-user interacts with.

In order to do this, a style guide was adopted⁵.



Figure 2.3: Style guide for eduVPN developers

A guide was also made available to developers giving clear design indications on how the apps should look [[README](#)].

³ As revealed during the interviews and workshops with end-users conducted during the D4S project.

⁴ See here for a list of the apps <https://app.eduvpn.org> and links to the app stores.

⁵ <https://github.com/eduvpn/artwork/blob/master/Styleguide/eduVPN-styleguide-v1.0.pdf>

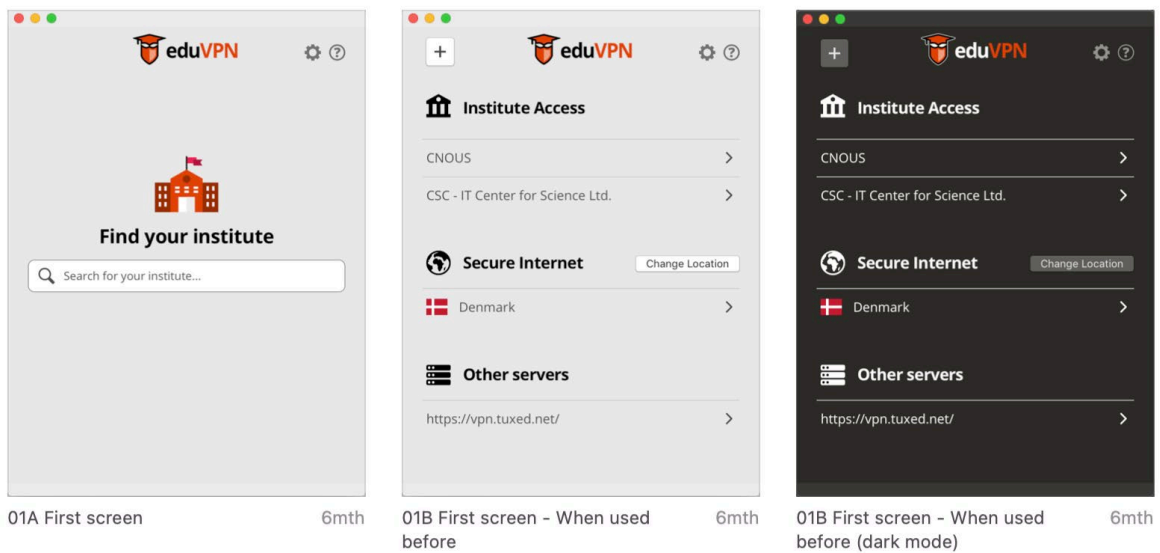
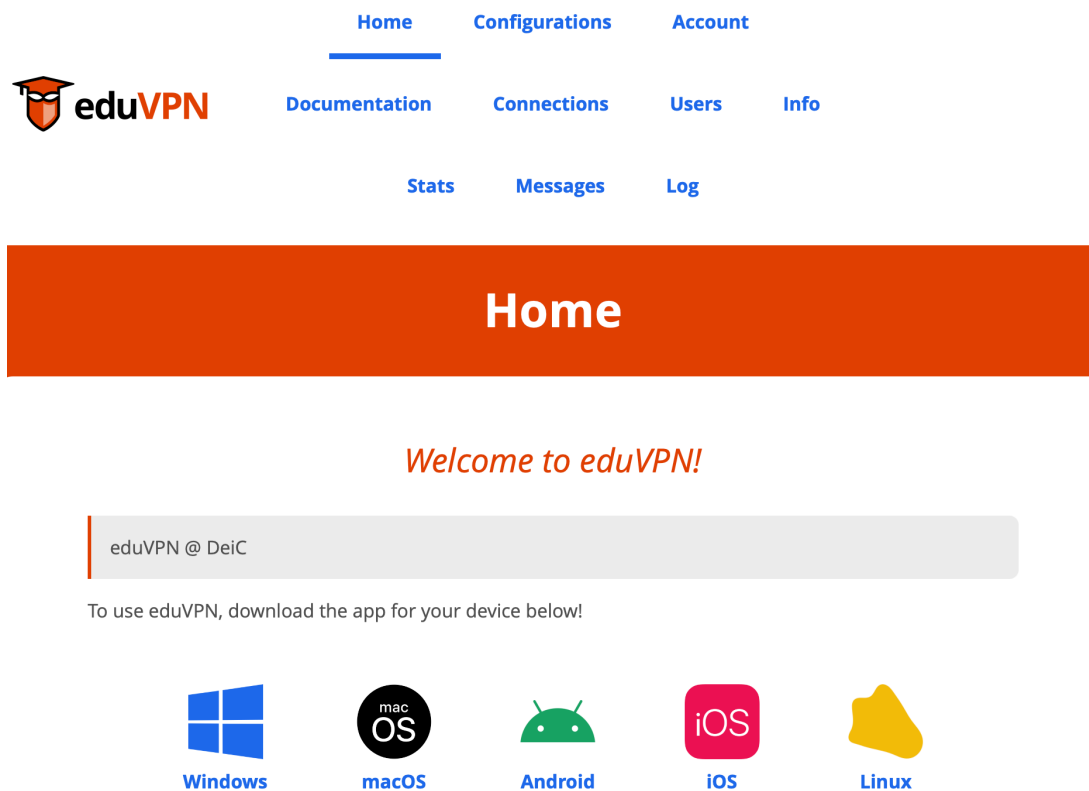


Figure 2.4: Guidelines for the successive screens in the different apps

There is now continuity between the website, the web-portal of each instance and the apps, given by the homogeneity of the look-and-feel.



On your "Account" page you can block access to the VPN in case you lose a device. On the "Configurations" page, advanced users can manually download VPN configurations.

Figure 2.5: Example of an instance web-portal

Deliverable D8.3
 eduVPN v2.0
 Document ID: GN4-3-21-406E3D

Another new feature is that most of the user journey now happens in-app and that navigation to different webpages in the flow is limited. In particular, all the discovery is done within the client app and the only non-homogeneous page is the login page at the user's Identity Provider.

2.2.2 New Flow: Prioritising Identity Provider Discovery

A variety of possible flow optimisations were initially considered that address the problems described in section 2.1 above⁶:

1. Ask the user first for their "Identity Provider"(IdP), i.e., "Organisation" before showing them any VPN instances to connect to (Solution 1).
2. Modify the application in such a way that users cannot 'get stuck' (e.g., the user goes through the app flow, authenticates at the wrong identity provider and experiences the app as not working) (Solution 2).

The problem with Solution 1 is that it is not possible to define which method will be used for user authentication, which could be SAML, RADIUS, LDAP or a local user database. This problem becomes especially clear when "Organisations" have access to *multiple* eduVPN instances. For this to work, a (global unique) way to identify an organisation is needed. Unfortunately, eduGAIN, the higher education and research inter-federation, cannot be leveraged for this purpose as not all organisations have their IdP in eduGAIN. To ensure a single unique way to identify an organisation, a dedicated registry of organisations would have to be created that links these to services while at the same time guaranteeing that all server operators coordinate with all organisations that have access to any eduVPN instance.

In order to create such a registry, the help of European NRENs would have to be enlisted, as they are in a position to ensure that this is properly managed in their "jurisdiction" (e.g. their country). With the help of the NRENs, the registry could cover the whole globe. This registry approach was discussed with a few NRENs, who reacted positively.

Solution 2 is implementable when the identity service provider of an organisation is only integrated with a single identity federation or confederation. In practice, this is the case anywhere in Europe. This means searching for the organisation would only result in a single hit.

After some analysis, a "hybrid" Solution 3 was devised, where for "Institute Access" the user chooses their *eduVPN instance* from a list, such as the 1st generation of the eduVPN applications, but for "Secure Internet" they choose their *organisation* instead.

This solves both the organisational problem of requiring unique mappings of organisations on the NREN level, as there is no longer the risk of duplication, *and* prevents users from getting stuck by choosing the wrong country.

⁶ This section reflects work done mostly within the D4S project.

2.2.3 Release Dates and Change Log

The release dates of the different client apps integrating the new flow and design are shown in the table below. All apps are listed on the eduVPN apps page [[eduVPN Apps](#)].

OS	Link to app	Change Log	Release Date
Android	https://play.google.com/store/apps/details?id=nl.eduvpn.app	https://github.com/eduvpn/android/blob/master/CHANGES.md	05-10-2020 in Google Play Store
macOS	https://apps.apple.com/app/eduvpn-client/id1317704208?mt=12	https://github.com/eduvpn/apple/blob/master/CHANGES.md	October 2020 in Mac App Store
iOS	https://apps.apple.com/app/eduvpn-client/id1292557340	https://github.com/eduvpn/apple/blob/master/CHANGES.md	November 2020 in App Store
Windows	https://app.eduvpn.org	https://github.com/Amebis/eduVPN/blob/master/CHANGES.md	February 2021 ⁷
Linux	https://app.eduvpn.org	https://github.com/eduvpn/python-eduvpn-client/projects/1 and https://github.com/eduvpn/python-eduvpn-client/pull/228	April 2021 ⁸

Table 2.1: Release dates and change logs for second generation eduVPN apps

2.2.4 IPR and Licensing

All apps are open source. They are released under a GNU GPLv3 (or higher) license.

The Copyright is owned by the eduVPN programme under The Commons Conservancy [[TCC](#)].

eduVPN is a registered EU trademark.

⁷ The new version of this app is being finalised at the time of writing and will shortly be available here: <https://github.com/Amebis/eduVPN/blob/master/CHANGES.md>

⁸ The current app which can be found here <https://python-eduvpn-client.readthedocs.io/en/master/> has to be modified to integrate the new GUI. A new Linux app for Let's Connect! Is available.

3 Conclusions

During the design of the apps, several questions were raised regarding:

- Use of federated identity in apps and how to design satisfying flows between apps and the web.
- Use of the same client apps by multiple identity providers and service providers and how to hide this complexity from end users.

It is hoped that the solutions presented here will provide an improved user experience for the new eduVPN apps.

The new generation of eduVPN client apps should thus also help drive growth in the number of eduVPN deployments and users. Their development has required the involvement of stakeholders outside the NREN community, in particular when testing assumptions about user groups in the context of the NGI TRUST-funded project D4S.

In the coming months, the app developers will be working on WireGuard support as well as other features, such as importing OpenVPN configuration files.

References

[D4S]	D4S stands for “Design 4 Security – Making VPNs easy” and it is a third-party project that has received funding from the NGI Trust, the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 825618. The partners in D4S were the Technical University of Denmark, The Royal Danish Academy (KADK) and Commons Caretakers. The project included user consultation (interviews, workshops)
[eduVPN]	https://github.com/eduvpn
[eduVPN_Apps]	https://app.eduvpn.org
[eduVPN_Docs]	https://github.com/eduvpn/documentation
[NGI TRUST]	https://www.ngi.eu/ngi-projects/ngi-trust/
[README]	https://github.com/eduvpn/artwork/blob/master/App/README.md
[TCC]	https://commonsconservancy.org/

Glossary

D4S	Design for Security
IdP	Identity Provider
IPR	Intellectual Property Rights
LDAP	Lightweight Directory Access Protocol
NGI	Next Generation Internet
NREN	National Research and Education Network
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
VPN	Virtual Private Network