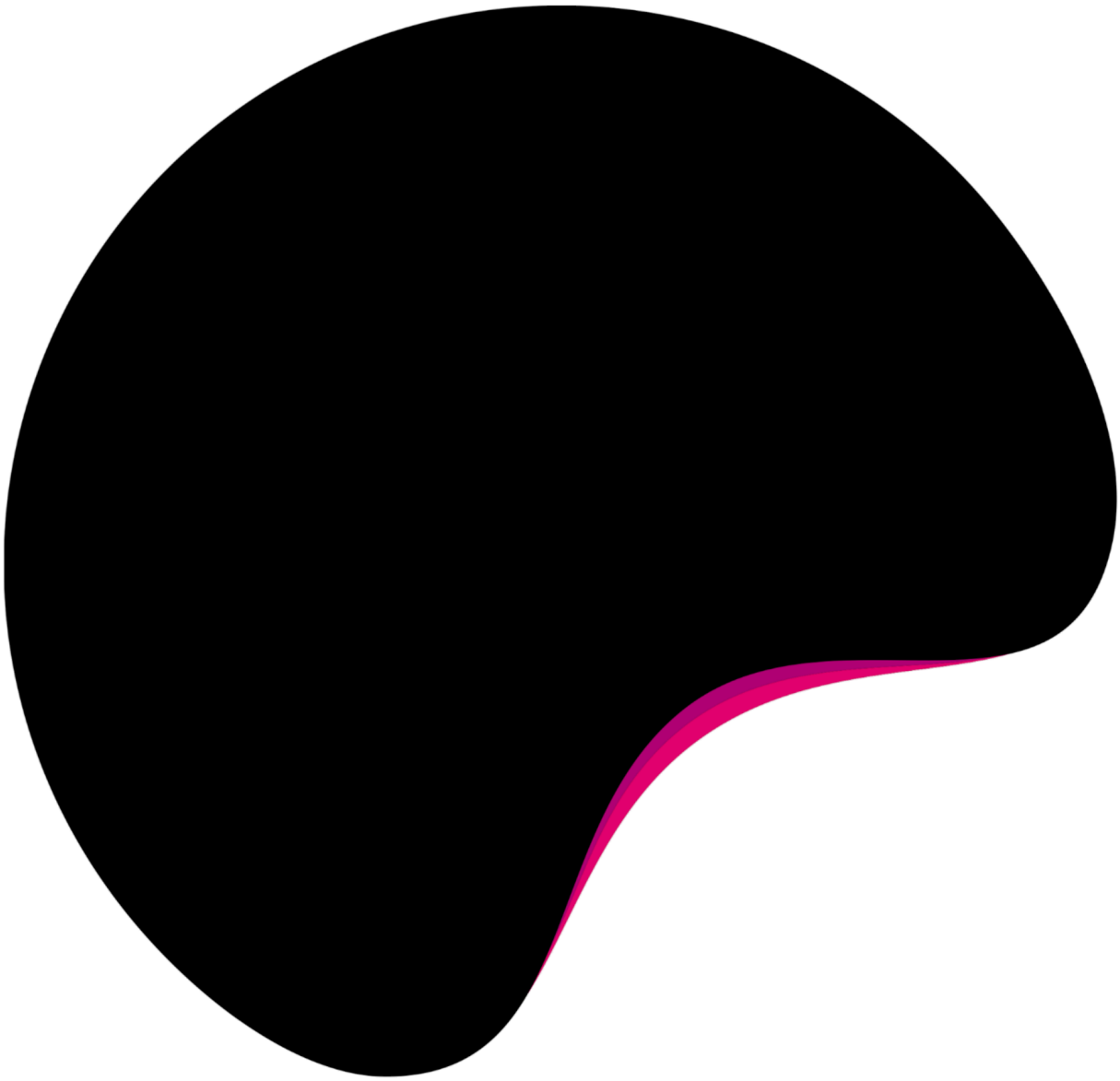

Proposal for changing the OST VPN

Striving for a more open educational environment

Author

Georgiy Chirokikh Shevoroshkin

Contributors

Fynn Gächter, Marco Kuoni, Ramon Bister

Outline

Context

This Proposal is based on the Proposal for changing the OST Auth solution . Consequently, all points regarding open-source and closed-source software (e.g. lower cost of ownership, flexibility, data sovereignty) remain applicable to the arguments supporting an alternative VPN implementation.

The OST-VPN Solution currently utilizes EntraID (SAMLv2) authentication for Cisco SSL-VPN. Users can connect to the VPN through the recommended cisco secure client [1] or any compatible client supporting the AnyConnect protocol, such as openconnect [2] .

There have been multiple requests from students and faculty for an OSS solution. Notably, Andreas Steffen, the creator of StrongSwan [3] , has suggested its implementation for the OST VPN. Raphael Das Gupta also had inquired about an open-source alternative to Microsoft Authenticator [4] .

Proposal

In addition to providing privacy-compliant and non-discriminatory remote access to the OST Network, an alternative solution may enhance both performance and security. StrongSwan presents itself as a compelling alternative, having been developed by Andreas Steffen, a former Professor at OST. The internal knowledge base can be effectively leveraged to facilitate this implementation. Moreover, StrongSwan offers a high degree of customizability and custom plugins, so that the requirements of complex environments can be met.

Furthermore, the IKEv2/IPSec Protocol demonstrates superior performance in high-traffic situations compared to alternative solutions such as OpenVPN [5] or Wireguard [6] as evaluated by C. T. J. Xiang [7] and F. Pohl [8] .

StrongSwan’s use of IKEv2/IPSec also offers robust encryption and integrity checks, providing better data protection compared to SSL-based protocols. Its open-source nature allows for third-party audits and transparency, ensuring there are no undisclosed vulnerabilities. In contrast, Cisco’s proprietary system limits visibility into the underlying security mechanisms.

Glossary

OSS	Open Source Software
SAMLv2	Security Assertion Markup Language 2.0
SSL	Secure Sockets Layer
VPN	Virtual Private Network
EntraID	Microsoft Entra ID (formerly known as Microsoft Azure Active Directory or Azure AD)
IKEv2/IPSec	VPN protocol combination of Internet Key Exchange version 2 and Internet Protocol Security

Supporters

Many thanks go out to all of the honorable supporters of this project, which include

Name	***Email***
Carina Schmitt	carina.schmitt@ost.ch
Claude Bregenzer	claude.bregenzer@ost.ch
Edoardo Balsamo	edoardo.balsamo@ost.ch
Elia Schenker	elia.schenker@ost.ch
Florian Bruhin	florian.bruhin@ost.ch
Fynn Gächter	fynn.gaechter@ost.ch
Gioele Petrillo	gioele.petrillo@ost.ch
Giuliano Gianola	giuliano.gianola@ost.ch
Jasmin Fässler	jasmin.faessler@ost.ch
Lukas Hunziker	lukas.hunziker@ost.ch
Marco Kuoni	marco.kuoni@ost.ch
Nathanael Fässler	nathanael.faessler@ost.ch
Nico Michael Rudolph	nico.rudolph@ost.ch
Oliver Clerc	oliver.clerc@ost.ch
Ramon Bister	ramon.bister@ost.ch
Raphael Das Gupta	raphael.dasgupta@ost.ch
Samuel Meuli	samuel.meuli@ost.ch
Simon Böni	simon.boeni@ost.ch
Stefan F. Keller	stefan.keller@ost.ch
Timon Erhart	timon.erhart@ost.ch
Yannick Ott	yannick.ott@ost.ch

Table 1: Supporters

Bibliography

[1] D. Tobler, “VPN OST.” Accessed: Oct. 25, 2025. [Online]. Available: https://wiki.ost.ch/display/public/IOW/VPN+OST

[2] C. Lubomir, “Openconnect.” Accessed: Oct. 25, 2025. [Online]. Available: https://github.com/openconnect

[3] The strongSwan Team, “Strongswan.” Accessed: Nov. 03, 2025. [Online]. Available: https://strongswan.org/

[4] R. D. Gupta, “OST wiki Comment: Microsoft Authenticator Alternative.” Accessed: Nov. 03, 2025. [Online]. Available: https://wiki.ost.ch/display/public/IOW/Multi-Faktor-Authentifizierung+mit+Microsoft+Authenticator#comment-section-title

[5] OpenVPN, “Self-Hosted VPN: Access Server | OpenVPN.” Accessed: Nov. 03, 2025. [Online]. Available: https://openvpn.net/access-server/

[6] J. A. Donenfeld, “WireGuard: fast, modern, secure VPN tunnel.” Accessed: Nov. 03, 2025. [Online]. Available: https://duckduckgo.com/?q=wireguard&ia=web

[7] C. T. J. Xiang, S. Aslam, and A. Tan, “Performance Evaluation of VPN Protocols in Live and Dynamic Network Environments,” in *Selected Proceedings from the 2nd International Conference on Intelligent Manufacturing and Robotics, ICIMR 2024, 22-23 August, Suzhou, China*, W. Chen, A. PP Abdul Majeed, A. H. Ping Tan, F. Zhang, Y. Yan, Y. Luo, L. Huang, C. Liu, and Y. Zhu, Eds., Singapore: Springer Nature Singapore, 2025, pp. 420–429.

[8] F. Pohl and H. D. Schotten, “Secure and Scalable Remote Access Tunnels for the IIoT: An Assessment of openVPN and IPsec Performance,” in *Service-Oriented and Cloud Computing*, F. De Paoli, S. Schulte, and E. Broch Johnsen, Eds., Cham: Springer International Publishing, 2017, pp. 83–90.

Illustrations

Tables