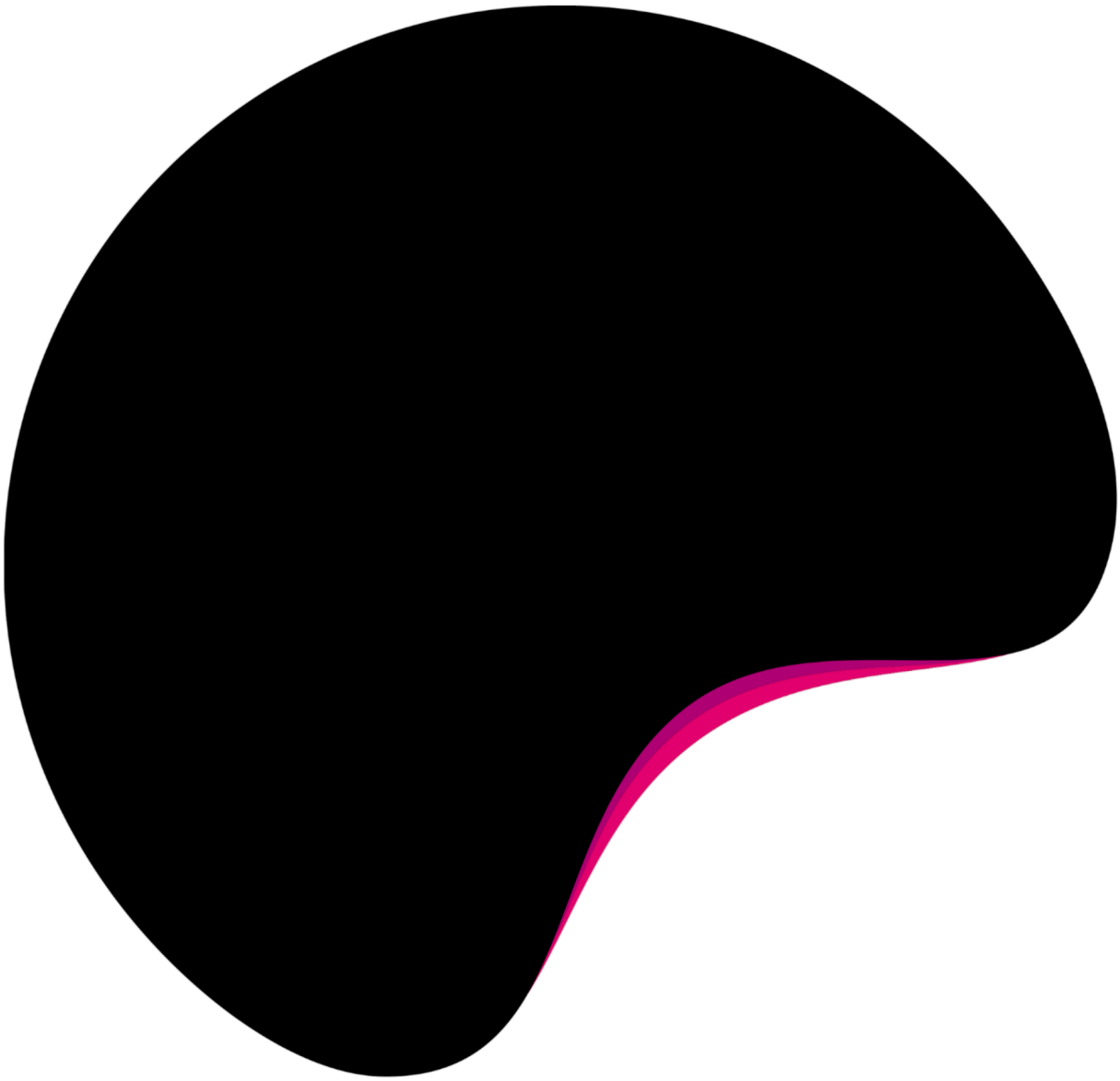

Proposal for changing the OST Auth solution

Striving for a more open educational environment

Author

Georgiy Chirokikh Shevoroshkin

Contributors

Fynn Gächter, Marco Kuoni, Ramon Bister

Outline

Context

The OST Auth Solution currently relies on EntraID (SAMLv2) for services such as the Confluence wiki , "Unterricht" webservice and Cisco SSL-VPN. EntraID, developed by Microsoft, provides identity management and facilitates integration with the broader Microsoft ecosystem.

Argumentation

Universities can play an exemplary role by using and contributing to FOSS through advisory, analytical, and evaluative activities. They possess unique forms of expertise and a degree of independence that can add significant value. These activities can indeed foster learning and improvement in the spirit of the Humboldtian educational ideal. Collaboration with the wider FOSS community is essential to ensure genuine openness, mutual learning, and innovation. In addition, sovereignty, data security, and inclusion should be key priorities. Educational institutions are key in providing information in a neutral and non-discriminatory manner, thereby establishing a standard for OER , open research and the free exchange of information [1] . This responsibility can only be fulfilled when accessibility for all is guaranteed through the implementation of FOSS [2] .

While the management of identities via EntraID may offer conveniences, the reliance on a multi-trillion-dollar corporation’s closed-source software presents a multitude of risks and worries particularily in, but not limited to, educational and research contexts. These risks encompass:

- Vendor Lock-In: Dependency on proprietary platforms limits flexibility and adaptability. [3]
- Incompatibility with Legacy Hardware: Potential exclusion of users employing older technologies. [4]
- Security Concerns: Heightened risks associated with centralized control and data management. [5]
- Licensing Costs: Ongoing fees may strain institutional budgets and resources. [1], [5]
- Ethical Considerations: Dependence on commercial entities raises questions about corporate governance in educational settings. [6]

Moreover, the monopolistic behavior and tracking practices associated with global corporations, in this case Microsoft, pose significant risks to security [7] , privacy [8] and democratic ideals [9] . Past incidents have highlighted the potential ramifications of these behaviors in both individual and institutional contexts. Through the usage of EntraID the administrators are forced to supply each student with a Microsoft account, thus contributing to the data harvest and monopoly position of the corporation.

The adoption of on-premise and open-source software solutions ensures the sovereignty and security of end-user data. Users are more likely to develop advanced technical skills and engage in collaborative learning, as well as a heightened awareness of ethical software practices and responsible IT behaviors. Moreover, the organizing body gains comprehensive control over its data and infrastructure, enabling the development of tailored solutions. This approach enhances risk management and fosters an environment of active development, ultimately benefiting the broader open-source ecosystem and the solutions built upon it [1] .

To showcase a positive example, the Microsoft Authenticator app is not required for client authentication, though it is recommended [10] . This flexibility enables the use of provider- and device-agnostic OTP software, promoting inclusivity for individuals who choose FOSS out of ethical or personal reasons. However, several aspects of the current OST infrastructure still restrict this possibility, notably in areas such as email and authentication. By integrating additional authentication options, one can reduce dependency on proprietary technologies and mitigate the associated risks. This effort not only promotes ethical practices but also empowers users to engage with the services in a manner that respects their preferences and needs.

Proposal

Transitioning the entire Microsoft-based ecosystem at OST University to a fully open-source model is undoubtedly a monumental undertaking. However, introducing the capability to connect to services like the VPN or wiki through alternative authentication methods beyond EntraID SSO would represent a significant first step in the right direction. This change would align with the institution's commitment to openness and accessibility and create a path for an independent and inclusive future.

As an initial step, it is feasible to implement authorization through open-source access management solutions such as Keycloak [11] in conjunction with OpenID Connect [12] (based on OAuth 2.0 [13]) without altering the existing identity infrastructure. This integration has already been successfully executed in the Network Garden Lab environment . A depiction of the user accessing a service using this method is illustrated in Figure 1 .

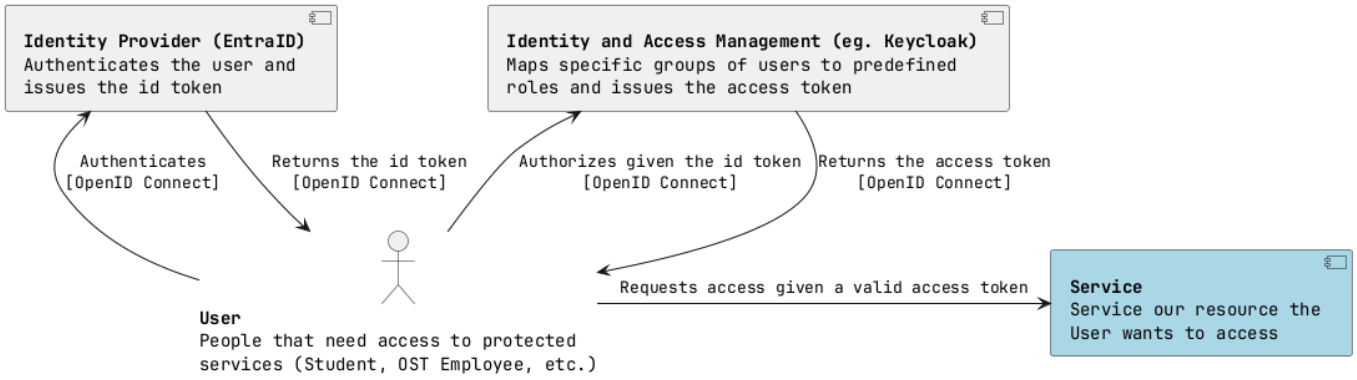

Figure 1: Service access and auth process

Although alternative open-source IAM projects like Shibboleth [14] or Gluu [15] exist, Keycloak provides an all-in-one solution, proving to be versatile enough for large organizations with complex access management schemes. Furthermore, the knowledge gained from implementing keycloak in the aforementioned Lab environment can be leveraged in creating an overarching and standardized auth solution for the multitude of services which OST provides.

Future considerations

Once the services requiring authentication and authorization are configured to utilize an open source IAM framework like Keycloak, the full identity management process can be more easily taken over from EntraID by said framework. Further steps would include data migration, policy configuration, testing, monitoring and finally decomissioning EntraID.

Glossary

OSS	Open Source Software
OER	Open Educational Resources
OTP	One Time Password
FOSS	Free and Open Source Software
SSO	Single Sign-On
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)
IAM	Identity and Access Management
IT	Information Technology

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] B. O. S. Bildung, “Strukturfonds für kritische Bildungsinfrastruktur.” Accessed: Oct. 10, 2025. [Online]. Available: https://opensource-bildung.de/proposal-strukturfonds-fur-kritische-bildungsinfrastruktur/

[2] F. Hartwagner, “Förderung von Open Source Software (OSS) an den Schulen.” Accessed: Oct. 10, 2025. [Online]. Available: https://www.educa.ch/sites/default/files/2020-11/whitepaper-open-source.pdf

[3] F. Kelch and S. Kaufmann, “Öffentliches Geld – Öffentliches Gut!: Warum Schulen und Freie Software gut zusammenpassen,” *Netzpolitik.org*, Aug. 2024, Accessed: Oct. 10, 2025. [Online]. Available: https://netzpolitik.org/2024/oeffentliches-geld-oeffentliches-gut-warum-schulen-und-freie-software-gut-zusammenpassen/

[4] bildung.digital, “Wege zur digitalen Schule II - Open Source,” *bildung.digital*, Dec. 2023, Accessed: Oct. 10, 2025. [Online]. Available: https://www.bildung.digital/artikel/wege-zur-digitalen-schule-ii-open-source

[5] S. Bandyopadhyay and S. S. Thakur, “ ICT in Education: Open Source Software and its Impact on Teachers and Students ,” *International Journal of Computer Applications*, vol. 151, no. 6, pp. 19–24, 2016, doi: 10.5120/ijca2016911915 Add to Citavi project by DOI .

[6] T. Pudelko, “Der Open-Source-Gedanke als ein Aspekt digitaler Nachhaltigkeit in der Sozialen Arbeit,” in *Nachhaltigkeit in Nonprofit-Organisationen: Transdisziplinäre Perspektiven für ein zukunftsfähiges Management*, J. Hilgers-Sekowsky, N. Richter, and N. Ermel, Eds., Wiesbaden: Springer Fachmedien Wiesbaden, 2023, pp. 135–148. doi: 10.1007/978-3-658-40659-2_10 .

[7] M. X. Heiligenstein, “Microsoft Data Breaches: Full Timeline Through 2024,” *firewalltimes*, Feb. 2024, Accessed: Oct. 25, 2025. [Online]. Available: https://firewalltimes.com/microsoft-data-breach-timeline/

[8] Office of Public Affairs, “Microsoft Agrees to Pay $20 Million Civil Penalty for Alleged Violations of Children’s Privacy Laws,” 2023, Accessed: Oct. 25, 2025. [Online]. Available: https://www.justice.gov/archives/opa/pr/microsoft-agrees-pay-20-million-civil-penalty-alleged-violations-childrens-privacy-laws

[9] A. Bokhari, “How Microsoft Helped Build The Censorship Industry,” *foundationforfreedomonline*, Jan. 2025, Accessed: Oct. 25, 2025. [Online]. Available: https://foundationforfreedomonline.com/microsoft-government-censorship-industry-revolving-door/

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

[11] Keycloak Authors, “Open Source Identity and Access Management.” Accessed: Nov. 01, 2025. [Online]. Available: https://www.keycloak.org/

[12] OpenID Foundation, “How OpenID Connect Works.” Accessed: Oct. 28, 2025. [Online]. Available: https://openid.net/developers/how-connect-works/

[13] D. Hardt, “The OAuth 2.0 Authorization Framework,” RFC Editor, 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6749.html

[14] Shibboleth, “The Shibboleth Project.” Accessed: Nov. 02, 2025. [Online]. Available: https://www.shibboleth.net/about-us/the-shibboleth-project/

[15] Open Source Identity and Access Management, “Gluu.” Accessed: Nov. 02, 2025. [Online]. Available: https://gluu.org/

Illustrations

Tables