Contribution ID: **72** Type: **Presentation**

Secure Zones for Sunet Drive

Wednesday 8 March 2023 11:00 (15 minutes)

Enterprise File Sync and Share (EFSS) systems have become an integral part of every researcher's life, handling an abundance of scientific data for multiple projects. Those projects generally span multiple collaborators and can extend over a significant geographic area. However, there is an inherent conflict when handling research data, between the researcher's need to collaborate and share data with each other and the sensitive nature that that data can sometimes have. Secure Zones for Sunet Drive is a technical implementation of protected data zones in the EFSS system, guarded by step-up authentication. The idea is to only give access to protected data to users that have been properly identified and help those users when handling the data so that they do not give further access to someone they should not, by mistake.

The complexity of multi factor authentication (MFA) can be understood, when one considers all parameters involved in its implementation. Multiple technologies like SMS, TOTP, or FIDO2 devices can be implemented either by the identity provider (IdP), the service provider (SP), or potentially even both. Among other things MFA also requires administration for lost or stolen devices. Identity providers must implement MFA individually and different technologies can be used for different IdPs.

Secure Zones for Sunet Drive have been developed in collaboration with Ponder Source and they implement MFA on the service provider side, with hooks being built into the EFSS solution such that a seamless transition between the general use of data, and corresponding secure zones can be done almost seamlessly. Since many EFSS systems have support for single-sign on via SAML, but no support for Discovery Services (i.e., aggregators of SAML/SSO-logins), Sunet Drive uses SaToSa, a configurable proxy for translating between different authentication protocols and providers. Users can opt to log on to the EFSS directly via their identity provider, with or without MFA and then step-up with MFA at a later point if necessary. The EFSS is made aware whether a user has logged on using MFA and if certain data storage areas of the EFSS should be accessible or not. Users can also control whether certain files or folders will require access via step-up authentication.

Secure Zones are an important technical tool that can be used by organizations and research groups to be compliant with the handling of sensitive data.

Authors: Mr DE JONG, Michiel (Ponder Source); Mr NORDIN, Micke (SUNET)

Co-authors: Mr JOHANSSON, Leif (SUNET); Mr FREITAG, Richard (SUNET)

Presenters: Mr DE JONG, Michiel (Ponder Source); Mr NORDIN, Micke (SUNET)

Session Classification: Security and Authentication

Track Classification: Main session: Technology & Research