ENABLING SEAMLESS ACCESS TO BEAMLINE CONSOLES WITH MOONSHOT AND UMBRELLA ID

PROBLEM STATEMENT

Beamline clients typically use three different set of credentials:

Experiment ID – Shared account used to access beamline console running experiment desktop session

Personal ID – Used for accessing the console using NX

Umbrella ID – Used to access other web-based services

Beamline access can be performed using one of these services:

GDM – Starts a new desktop session, attached to the physical display.

Login console – Starts a new terminal session attached to the chosen TTY.

SSH – Starts a new remote terminal session.

NX – Connects to the existing physical display (can show either GDM or the already started desktop session)

PSI runs the DUO service:

Keeps a mapping of associations between UmbrellaIDs and both, experiment and personal IDs

GOAL

Clients use just their UmbrellaID to connect to the console

Reducing the number of credentials users need to remember and handle

Reducing the management cost associated to these credentials for the IT team

PROPOSED SOLUTION

Enables **federated authentication** for web and non-web services

A single set of credentials can be used to authenticate to all the services

INFRASTRUCTURE REQUIREMENTS (UMBRELLA ID)

- Moonshot IDP
  - FreeRADIUS
  - Authenticates users using EAP-TTLS
    - Uses the same backend (LDAP) than the UmbrellaID SAML IDP (now)
    - Uses a different backend (EduTEAMs)
  - Provides a SAML assertion back to the service for authorisation

INFRASTRUCTURE REQUIREMENTS (PSI)

- Moonshot RPP (Relying Party Proxy)
  - FreeRADIUS
  - Connects on-premise applications with the Moonshot IDP
  - Performs UmbrellaID → local account mapping
  - For PSI, this means using the DUO system to return either the Experiment of Personal account
    - Other Lightsources might use different approaches
    - Install Moonshot at the consoles

INFRASTRUCTURE REQUIREMENTS (PSI)

- Install Moonshot at the consoles
  - Up-to-date repositories for most important GNU/Linux distributions (Debian, Ubuntu, RHEL, Alpine)
  - Configure Moonshot to use our designated RPP (/etc/radsec.conf)
- Configure PAM to use GSS-API authentication
  - Using the pam_gss.so module and add a line to the PAM configuration
- Configure SSH server to use GSS-API authentication
  - Need to use the patched OpenSSH packages from Moonshot (up-to-date with latest OpenSSH version for each distribution)
  - Required because OpenSSH won't accept any GSS-API mechanism other than Kerberos

RESULTS

Users can log into the consoles using their UmbrellaID credentials

SSH, GDM, or Login console → Experiment ID

NX → Personal ID

They can use NX to access the physical display:

No session created previously → Use GDM to create it

Session already created → Access to it

No need for them to know:

Passwords for Experiment or Personal IDs

Not even Experiment or Personal IDs (account names)