Contribution ID: **58** Type: **not specified**

Who Authenticates Linux? Rethinking PAM & NSS in the Age of Cloud Identity

Who authenticates Linux? In the age of Azure Entra ID, Okta, Google Workspace, and beyond, the answer is increasingly "not your local LDAP or Kerberos realm." Modern identity providers rely on OAuth2, device compliance, and custom multi-factor authentication (MFA) flows that are fundamentally browser-centric — which sits at odds with how a Linux login works.

PAM was designed decades ago for direct credential checks (think passwords). It's poorly suited to today's delegated, web-driven identity. Windows gets around this by invoking MFA flows in a desktop context, popping up a browser window for the user. Linux can't now (and arguably shouldn't) run a browser at the login prompt. So how do we integrate modern cloud identity —with MFA, device trust, policy enforcement —into the Linux login experience?

In this talk, I'll demo Himmelblau, an open-source project that glues Azure Entra ID into PAM and NSS. We'll explore the tricky hacks needed to make this work. But this is a bespoke solution for one IdP. Each provider implements their own authentication extensions on top of OAuth2. There's no standard for non-browser-based MFA integration in a PAM/NSS world. Should we start drafting one? Let's discuss what a sane future might look like —and how Linux systems could better support cloud-native identity out of the box.

Primary author: Mr MULDER, David (SUSE)

Presenter: Mr MULDER, David (SUSE)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC