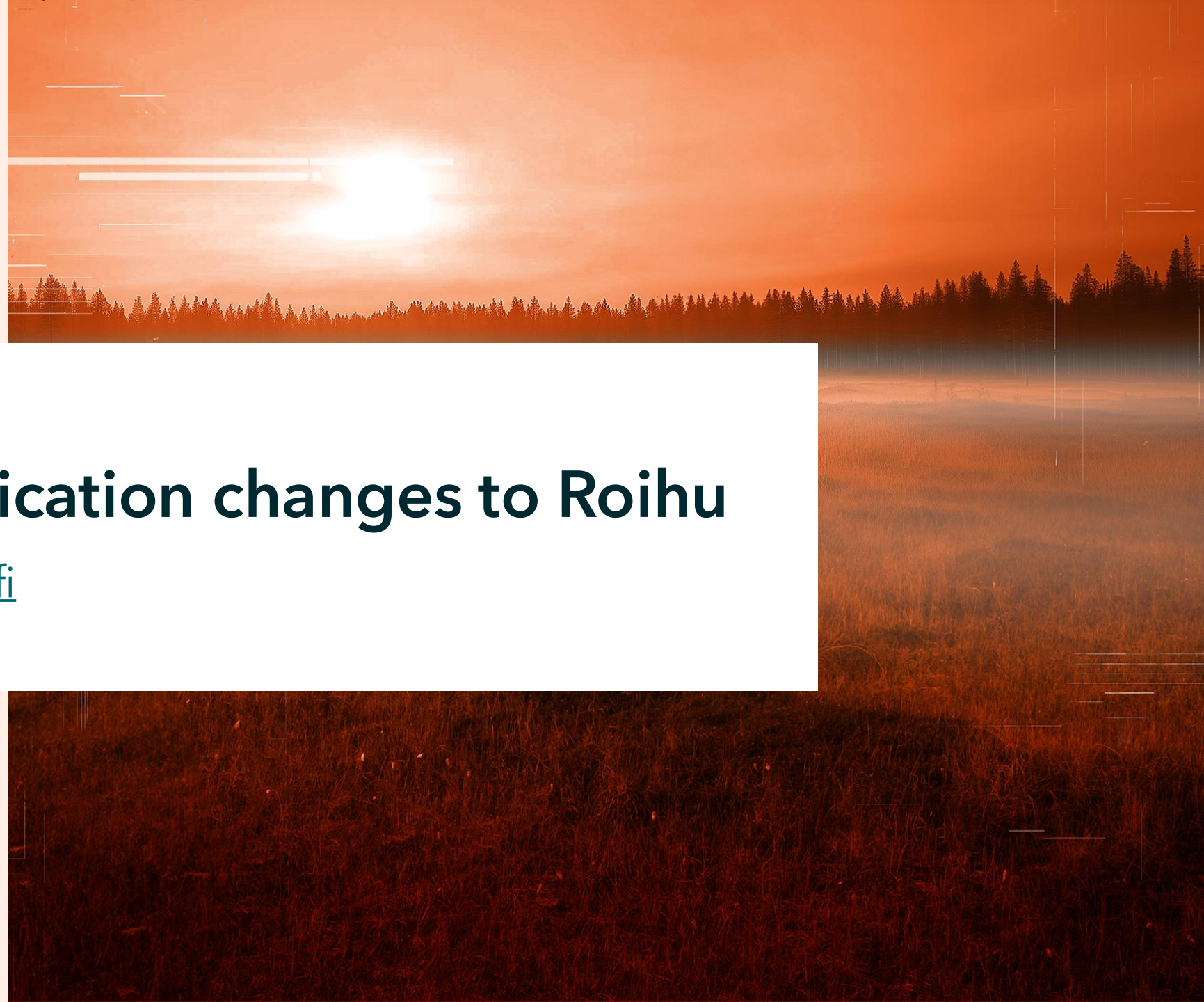

SSH authentication changes to Roihu

juha.nyholm@csc.fi

OpenSSH keys → Short-lived OpenSSH certificates

Core Concept

• Issue **short-lived** (24 hours) **SSH certificates** to users by leveraging **federated login** (e.g. Haka login) and enforcing **Multi-Factor Authentication (MFA).**

Enhances Security Posture by:

• **Reducing unauthorized access** risk with SSH certificates that automatically expire.

• **Limiting the impact of stolen SSH private keys** by requiring MFA during certificate issuance.

• **Improves research security** by preventing accounts that have been locked at their home organization from authenticating to CSC services (federated login).

How to obtain a short-lived SSH certificate?

Two options:

- **Via web browser**
  - Sign in to **MyCSC**.
  - Upload your SSH public key (if needed) and request signing.
  - Download the signed SSH certificate and configure your SSH client.
- **Using a "certificate helper script"**
  - https://github.com/CSCfi/certificate-helper-tool/
  - Run the script and authenticate.
  - The script retrieves the signed SSH certificate and configures your SSH client automatically.

DEMO: SSH certificate-based authentication

Follow us

LinkedIn

Instagram

Facebook

YouTube

csc.fi