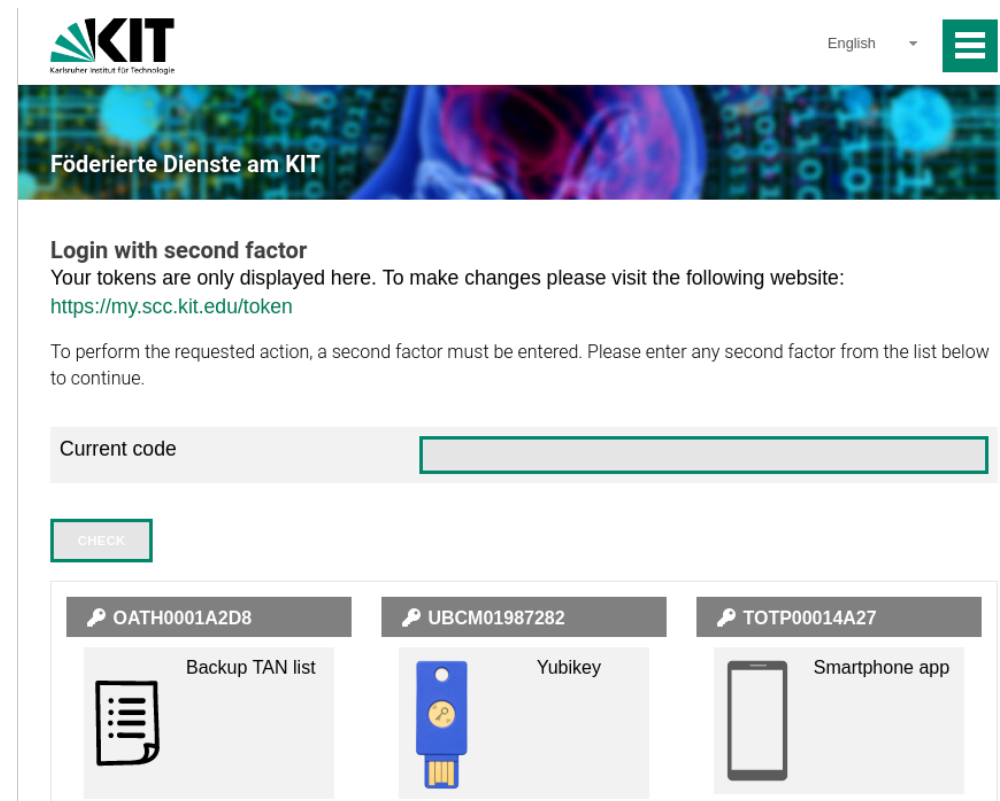




# 2FA + SSH: A Creative Solution for Secure, User-friendly HPC Authentication

Fabian Lingenhöl

# Motivation

- Goal: Prevent unauthorized login with stolen credentials
- Common solution: Multi-factor authentication
  
- Problem: How to integrate with SSH?
  - SSH certificates
  - Local OTP service (e.g. pam\_oath)
  
- Our solution: Remote OTP service









 English 

Föderierte Dienste am KIT

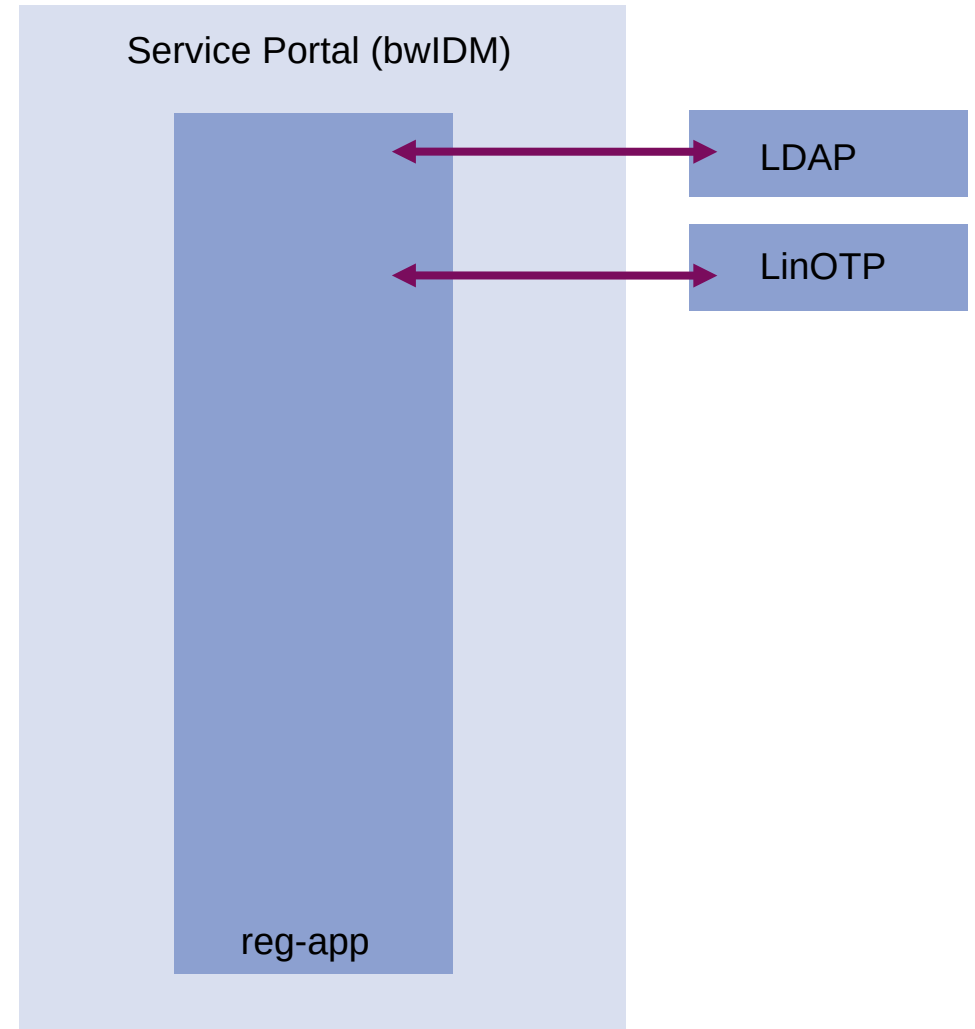
**Login with second factor**  
Your tokens are only displayed here. To make changes please visit the following website:  
<https://my.scc.kit.edu/token>

To perform the requested action, a second factor must be entered. Please enter any second factor from the list below to continue.

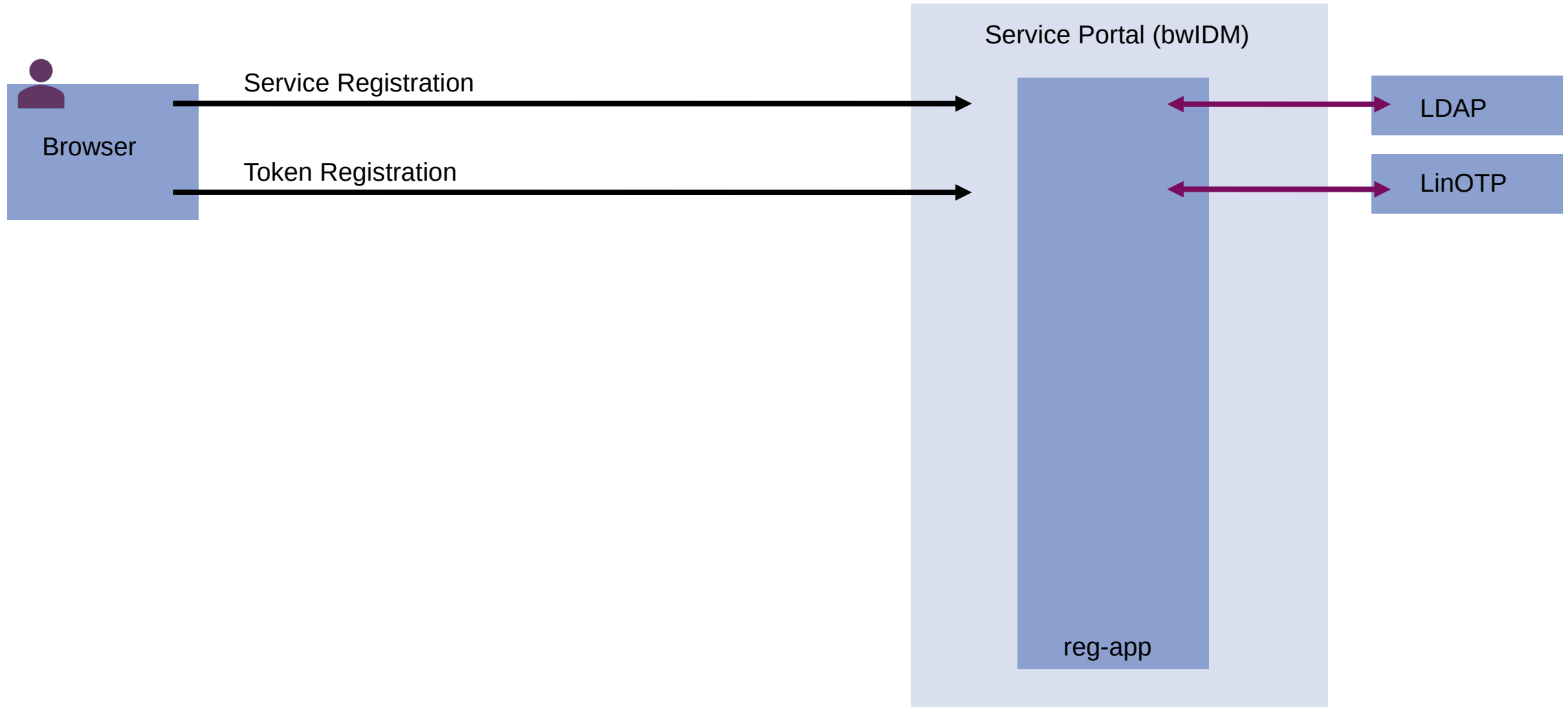
Current code

 OATH0001A2D8	 UBCM01987282	 TOTP00014A27
 Backup TAN list	 Yubikey	 Smartphone app

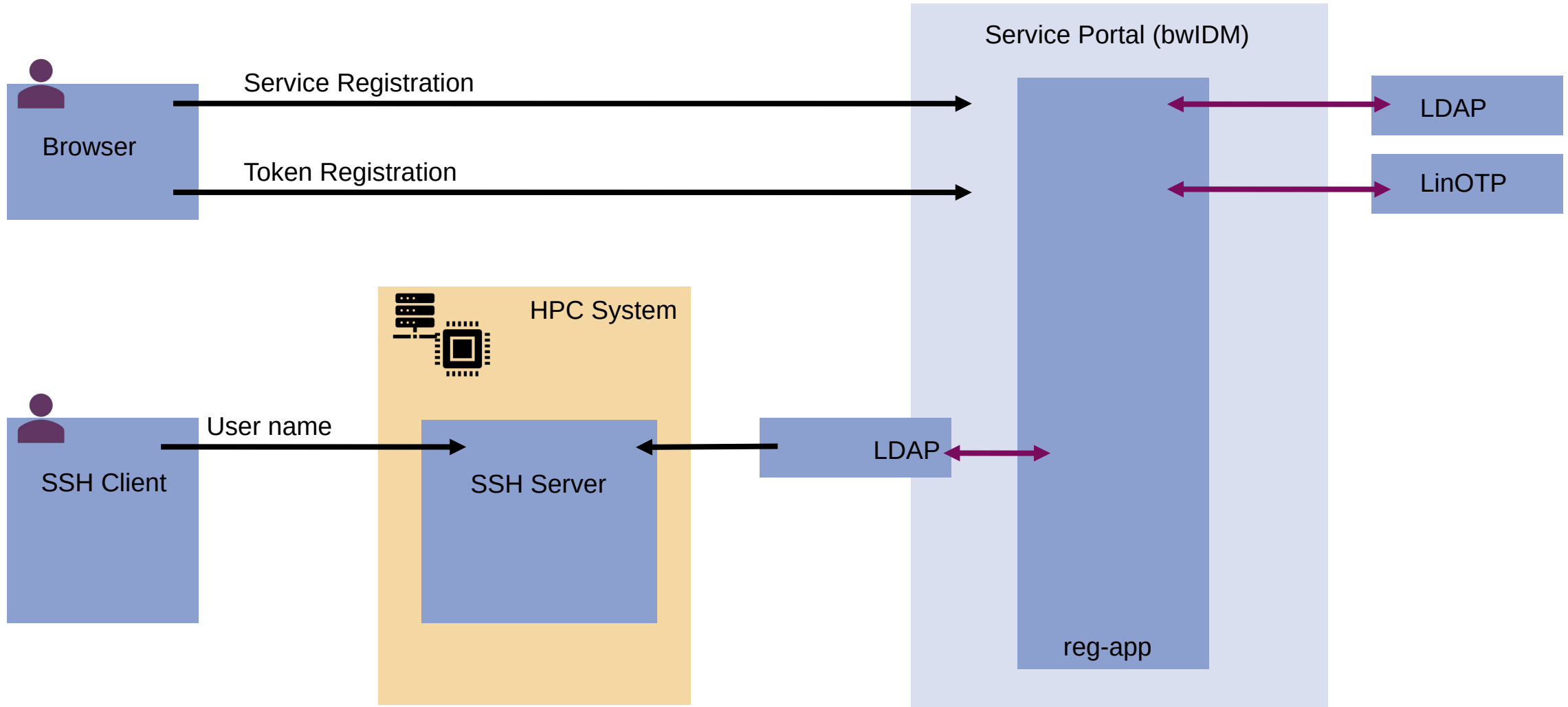
# Integrate 2FA and SSH



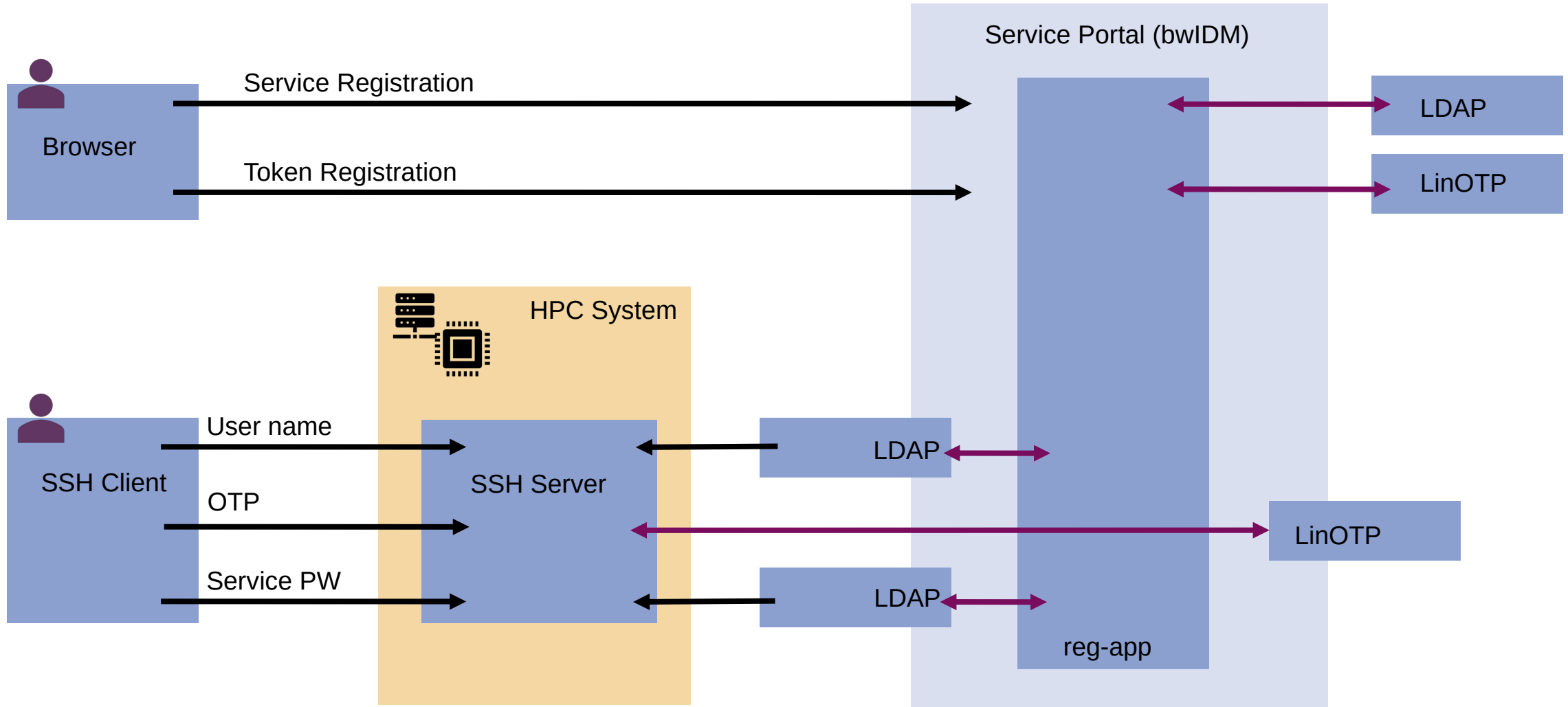
# Integrate 2FA and SSH



# Integrate 2FA and SSH

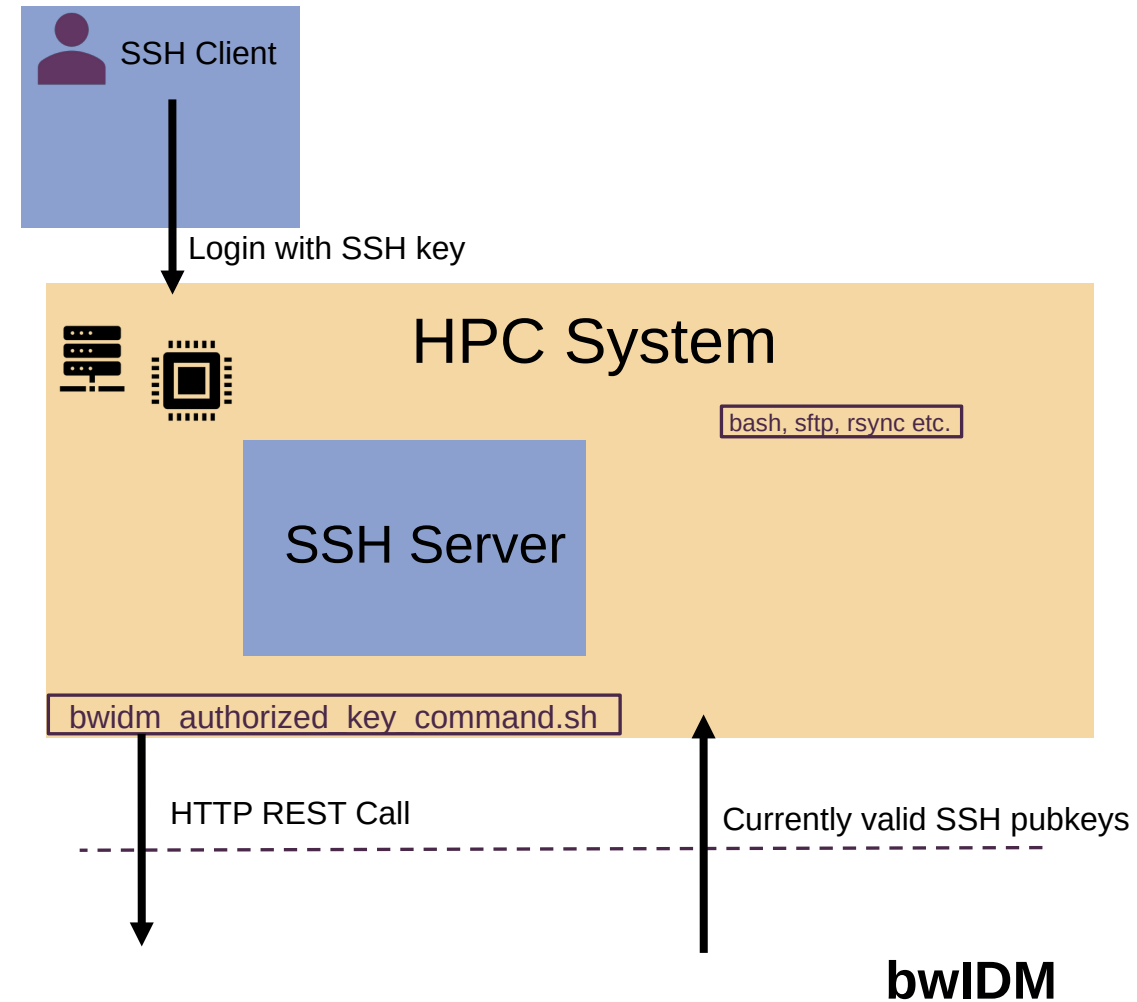


# Integrate 2FA and SSH



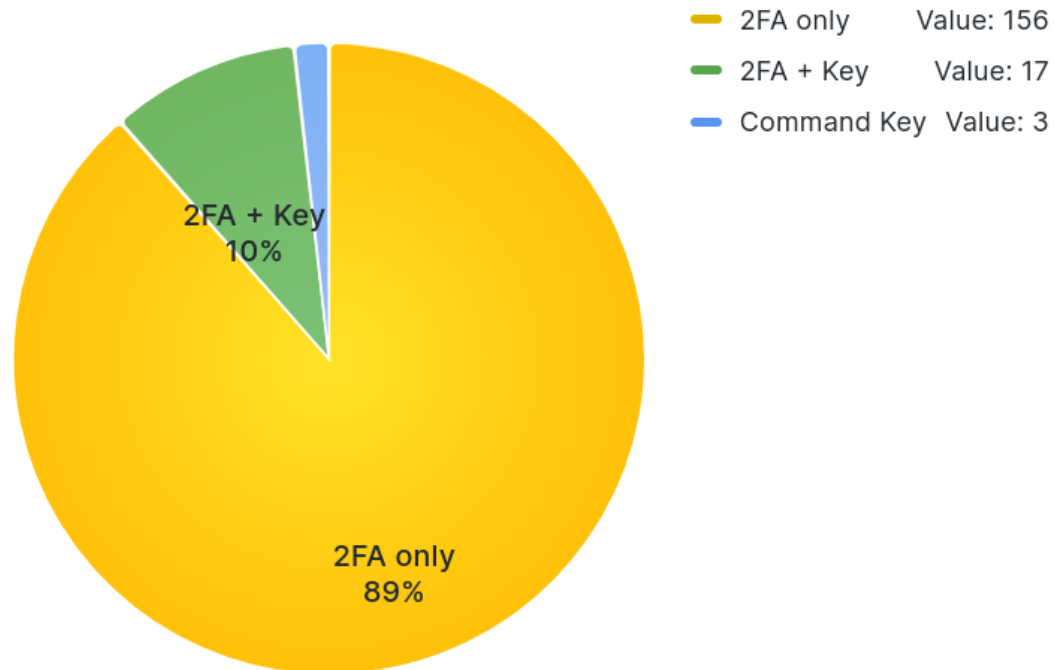
# What about automated workflows?

- So far:
  - Successfully integrated 2FA
  - Separated cluster operation and identity management
- But: Automated workflows often rely on SSH keys
- Dynamic (de-)activation of keys
  - E.g. we unlock „interactive“ SSH keys only if user logged in with 2FA in the past hour
  - Enables automated workflows

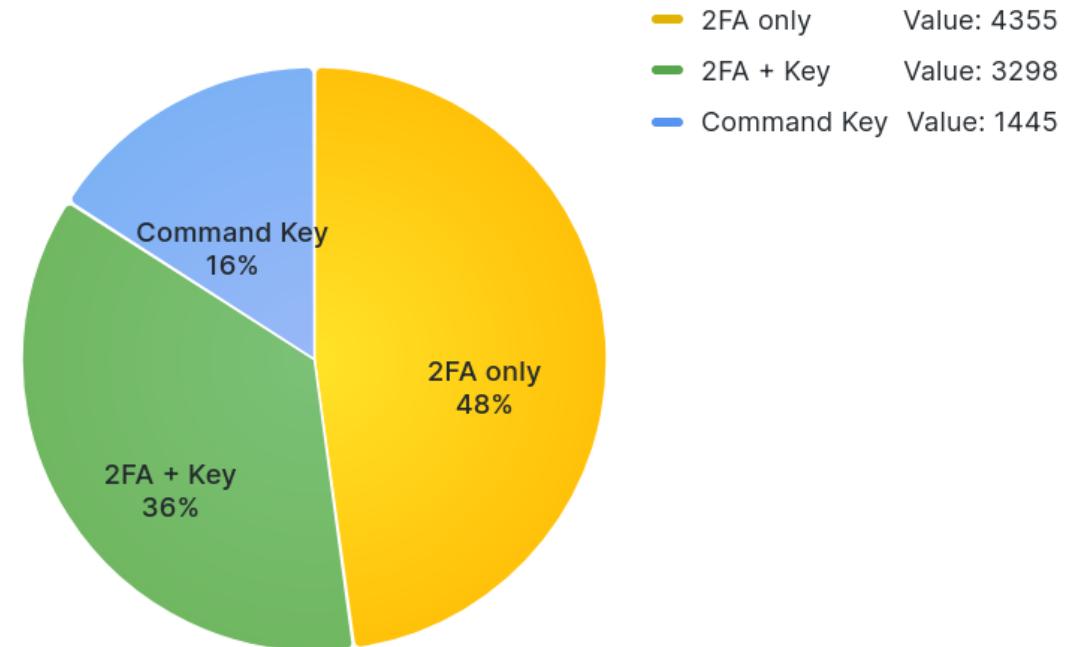


# User Adoption

Login method by number of users



Login method by number of logins



Numbers are for March 2023 on HoreKa