Solutions for non-web OAuth 2.0 authorisation at CERN

Authors: Asier Aguado Corman, Jack Henschel, Hannah Short, Sebastian Lopienski

The challenge

CERN is migrating its Authentication and Authorisation Infrastructure to **Keycloak**, which allows us to fully support **OAuth 2.0** (Open Authorisation) as well as SAML (Security Assertion Markup Language).

OAuth 2.0 has become increasingly popular over the past 5 years, and the vast majority of our authenticated applications now rely on OAuth 2.0.

Many workflows at CERN for researchers and engineers are completed on the **command line**. Finding **user friendly**, secure mechanisms to provision OAuth 2.0 tokens on a CLI is essential to **support users** and **avoid insecure workarounds**.

Old approach: Cookies

Cookie-based authentication using a command line tool which logs into the SSO using Kerberos and SPNEGO and saves cookies into a file.

Positives:

- Users only need a Kerberos token (TGT), which is a very common authentication workflow in command line environments.
- No external web browser needed.

Negatives:

- It depends on the SSO website structure: small modifications can break it.
- It doesn't follow authentication standards, can't be reused outside CERN.
- We can't profit from the evolution of new standards and open source tools.
- Web based two-factor authentication protocols can't work.

```
$ kinit
Password for aaguadoc@CERN.CH:
$ auth-get-sso-cookie -u https://the-target-api.cern.ch -o cookies.txt
$ curl -L -b cookies.txt https://the-target-api.cern.ch/foobar
```

New approach: OAuth 2.0 Device Authorization

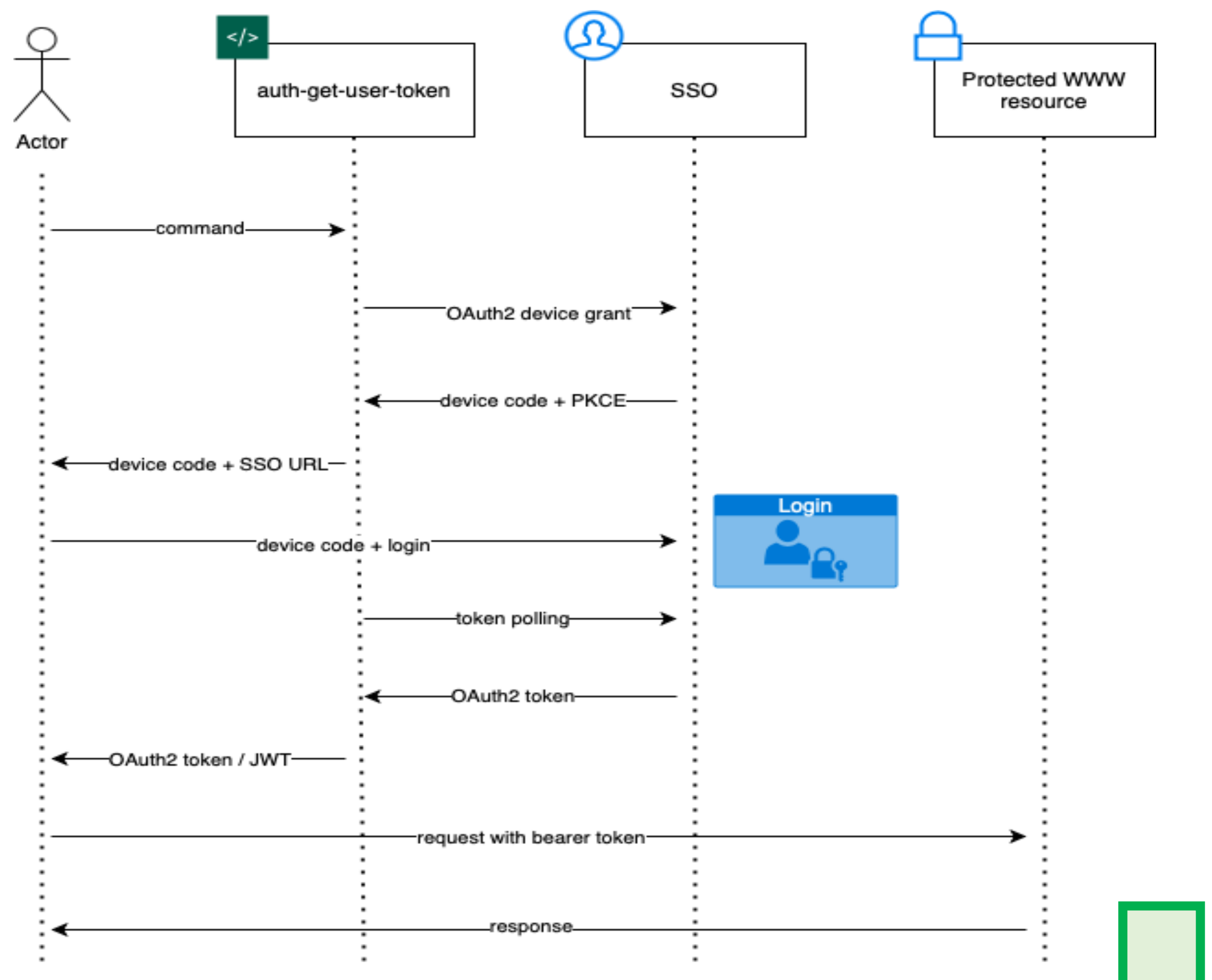
Tools can use the OAuth 2.0 Device Authorization Grant, using a public client and Proof Key for Code Exchange (PKCE).

Positives:

- The use case is fully covered using OAuth 2.0 standards.
- Simple development and testing by using stateless JWT instead of cookies.
- Built-in role based access control (configurable by application managers).
- No dependencies on Kerberos.
- All modern two-factor authentication protocols are compatible.

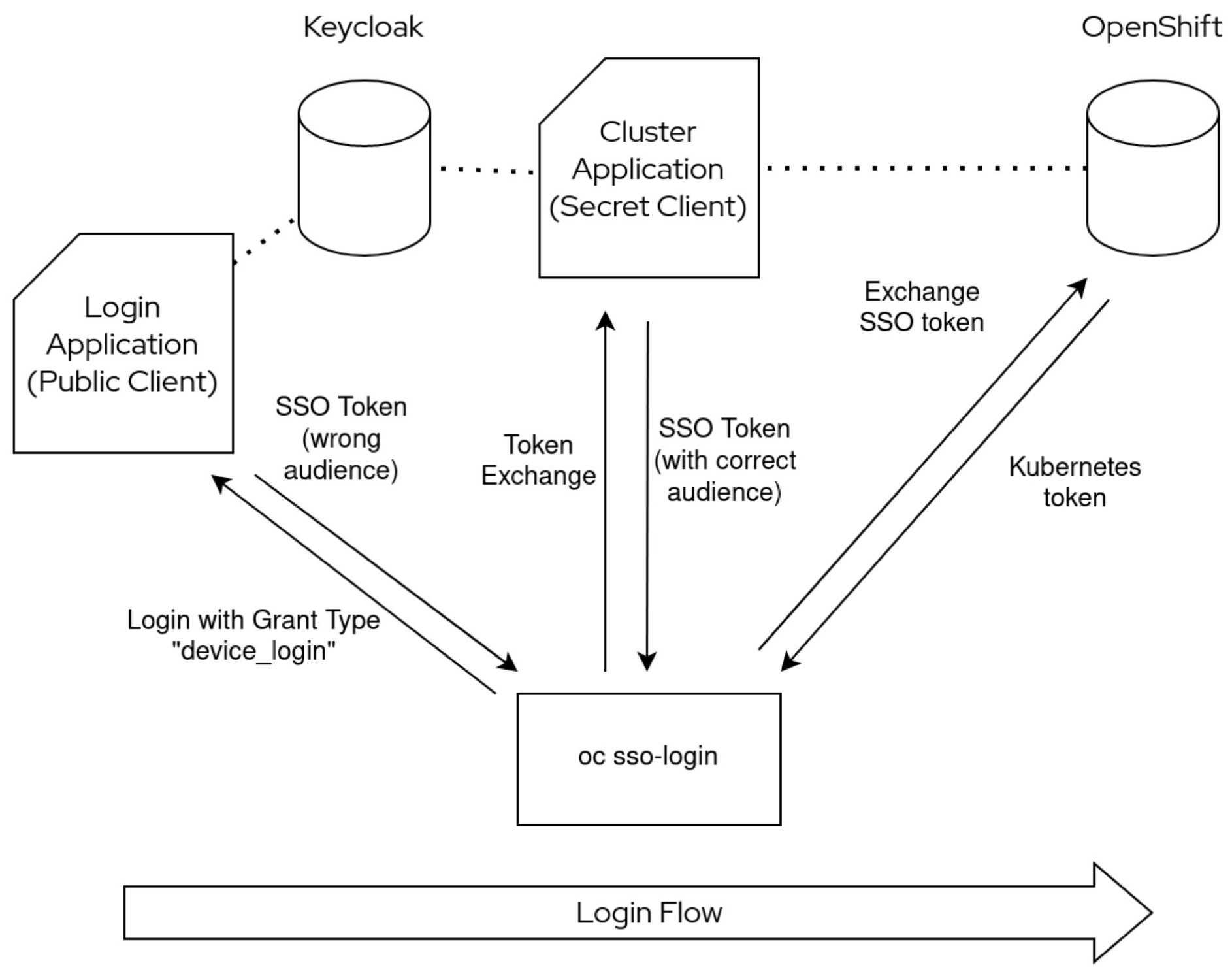
Negatives:

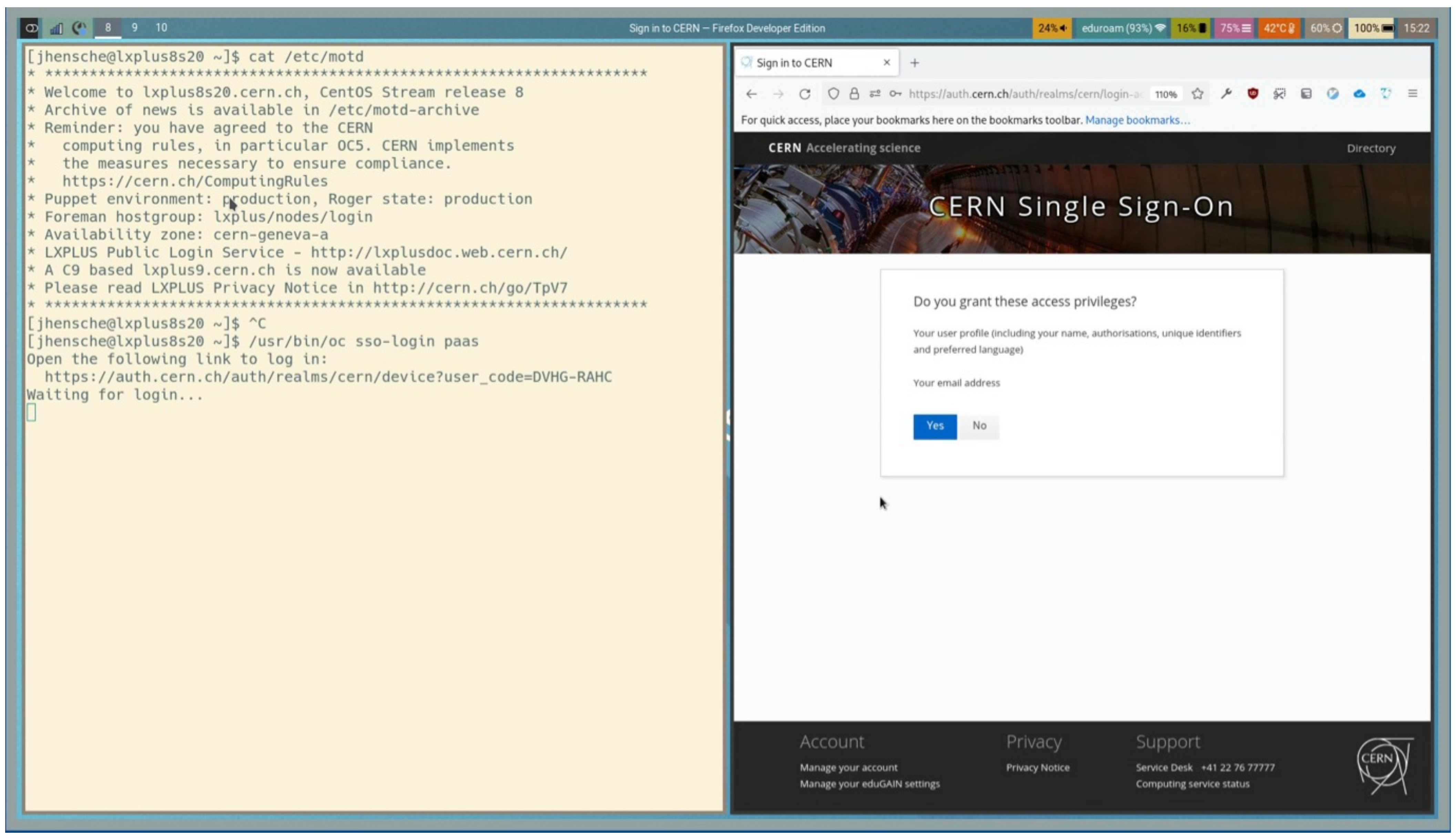
- Users need a web browser window outside the terminal, using the same device or e.g. a mobile phone.
- Double authentication in environments where Kerberos is the main protocol.



Case Study: OpenShift

- Enables CLI authentication to the OpenShift cluster whilst respecting users' 2FA settings
- Authentication happens in the browser (no additional login required if already authenticated). This can be performed on any device.


Keycloak
OpenShift
Cluster Application (Secret Client)
Login Application (Public Client)
SSO Token (wrong audience)
Token Exchange
SSO Token (with correct audience)
Exchange SSO token
Kubernetes token
Login with Grant Type "device_login"
oc sso-login
Login Flow



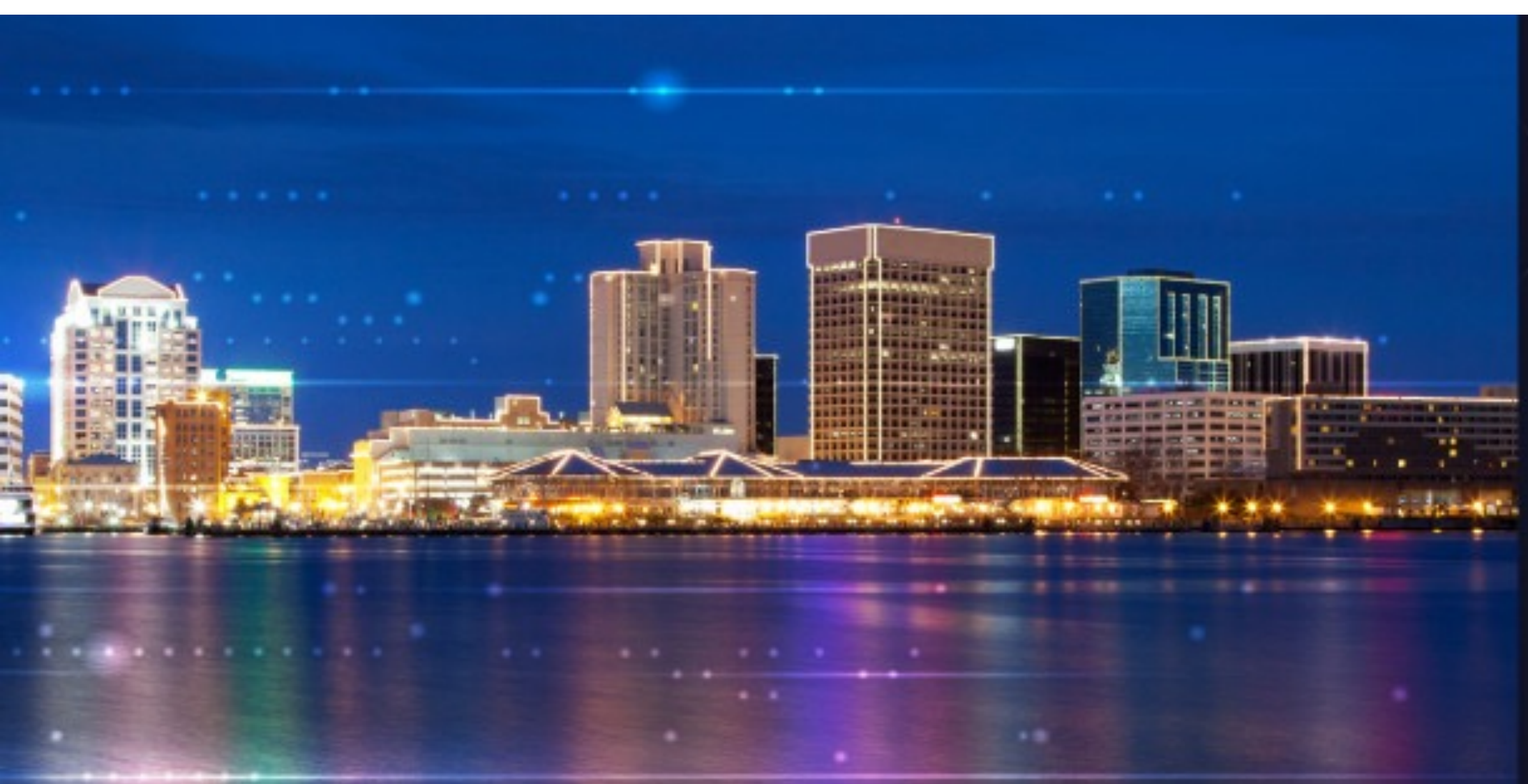
```
[jhensche@lxplus8s20 ~]$ cat /etc/motd
* ********************************************************************
* Welcome to lxplus8s20.cern.ch, CentOS Stream release 8
* Archive of news is available in /etc/motd-archive
* Reminder: you have agreed to the CERN
*   computing rules, in particular OC5. CERN implements
*   the measures necessary to ensure compliance.
*   https://cern.ch/ComputingRules
* Puppet environment: production, Roger state: production
* Foreman hostgroup: lxplus/nodes/login
* Availability zone: cern-geneva-a
* LXPLUS Public Login Service - http://lxplusdoc.web.cern.ch/
* A C9 based lxplus9.cern.ch is now available
* Please read LXPLUS Privacy Notice in http://cern.ch/go/TpV7
* ********************************************************************
[jhensche@lxplus8s20 ~]$ ^C
[jhensche@lxplus8s20 ~]$ /usr/bin/oc sso-login paas
Open the following link to log in:
  https://auth.cern.ch/auth/realms/cern/device?user_code=DVHG-RAHC
Waiting for login...
```

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Do you grant these access privileges?

Your user profile (including your name, authorisations, unique identifiers and preferred language)

Your email address



Norfolk, Virginia, USA • May 8-12, 2023

CHEP 2023

Computing in High Energy & Nuclear Physics

For questions please contact CERN's Authentication team at authzsvc-admins@cern.ch

This poster is presented by Adeel Ahmad (pictured) on behalf of a larger team.