dCache.org

Macaroons and dCache

… or delegating in a cloudy world

Patrick Fuhrmann
Paul Millar

On behave of the project team

INDIGO DataCloud

Fermilab NDGF Nordic DataGrid Facility DESY Helmholtz Association Federal Ministry of Education and Research LSDMA

AAI … but

This talk is about the second 'A': **Authorisation**.

Quick recap: which is which?

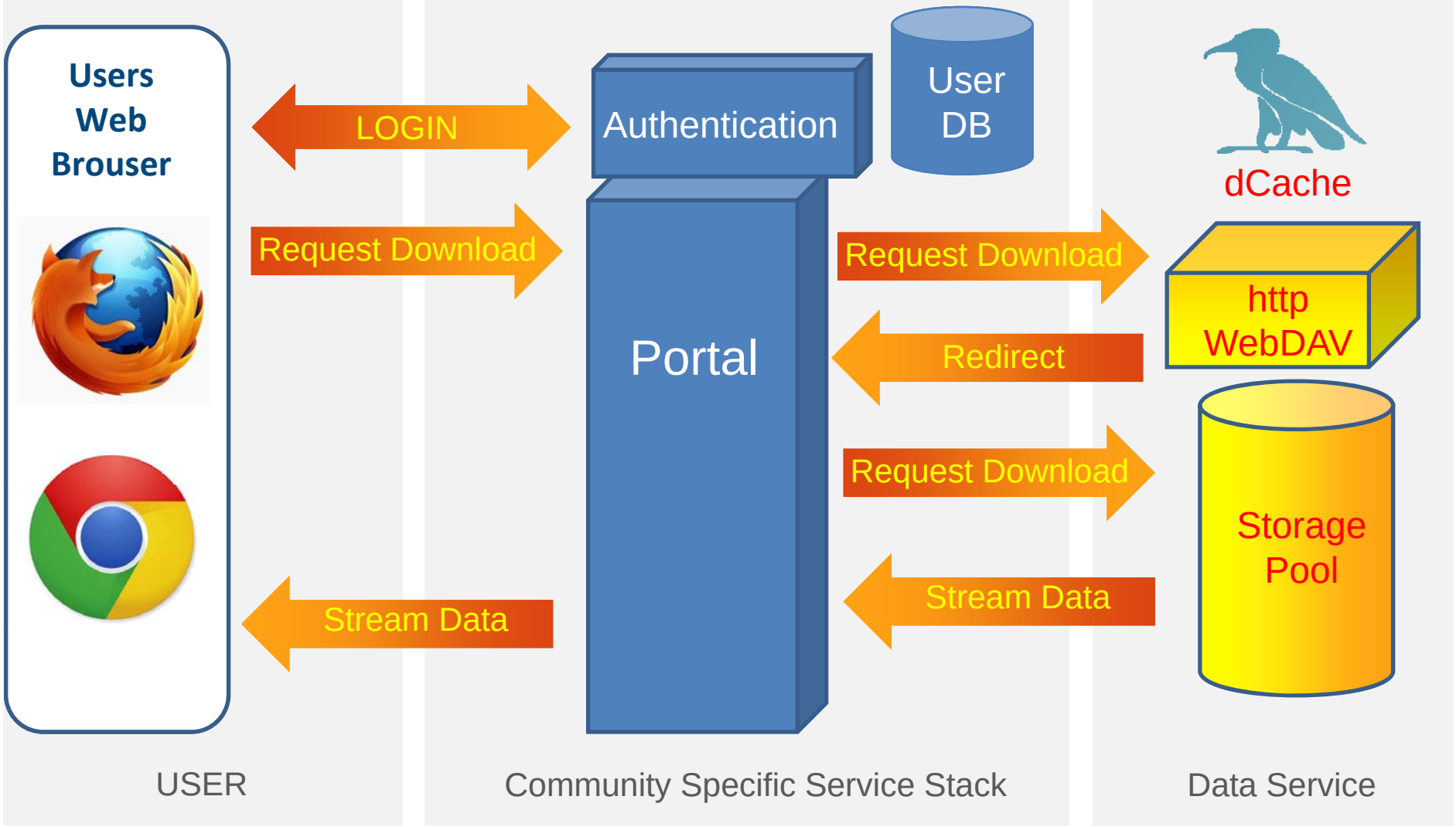
Credential

Authentication

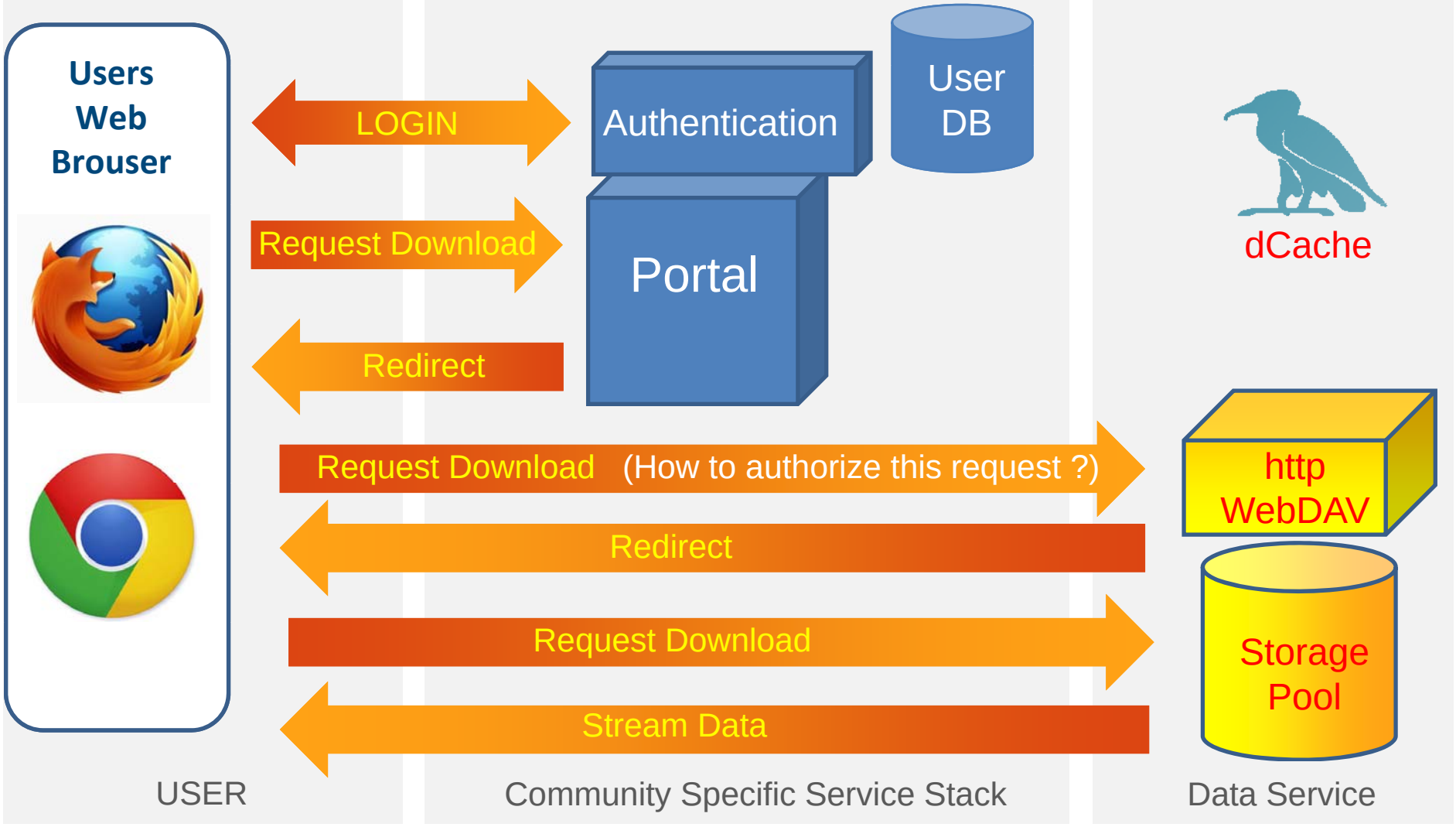
Authorization

Authorisation without authentication?

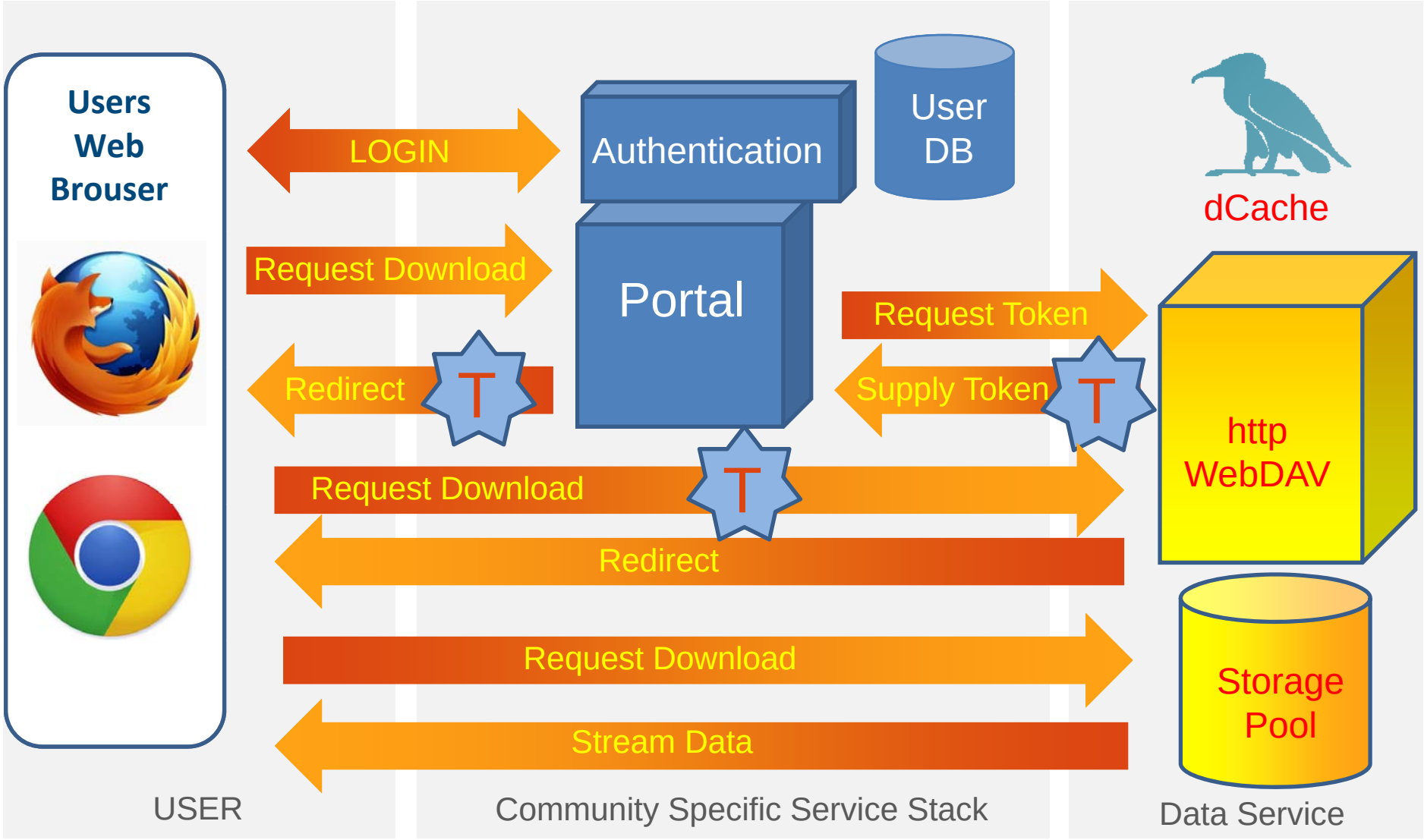
Photon Science portal use-case



Desired: client downloads directly



Desired: client downloads directly



What are bearer tokens?

Bearer token is something the user presents with a request so the server will authorise it. There's no interaction between client and server.

Examples of bearer tokens:

- HTTP BASIC authn, anything stored as a cookies.

Counter-examples:

- X.509 credential,
- SAML,
- Kerberos.

Bearer tokens for download authz

- Redirection should work **without JavaScript**,
- Simple: **embed token** in redirection URL.

http://webdav.example.org/path/to/file?authz=<TOKEN>

(There are nicer ways of embedding the token, but the URL is the only thing we can control)

- **Complete token** always sent with the request.
- What can we do to stop someone **stealing** this token?
- … or make the token useless if they steal it.

Introducing Macaroons