Tokens in dCache

Paul Millar

IAM Workshop 2021

2021-11-08

https://indico.cern.ch/event/876810/

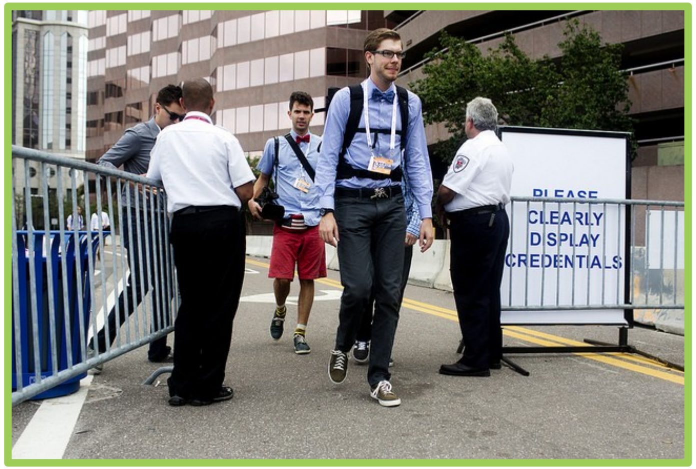
Nordic e-Infrastructure Collaboration

Fermilab

HELMHOLTZ
RESEARCH FOR GRAND CHALLENGES

DESY.

How login works in dCache



Credentials vs principals

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
T22000129
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020
938568
MUSTER
中國人民建設銀行
THE PEOPLE'S CONSTRUCTION BANK OF CHINA
VALID ONLY IN CHINA
VISA
PASE
DIENESTA PASE
EIROPAS SAVIENĪBA LATVIJAS REPUBLIKA
Wile E. Coyote
GENIUS
HAVE BRAIN
WILL TRAVEL

Name: **Wile E. Coyote**

ACME customer ID: **11493**

Passport number: **0008103314**

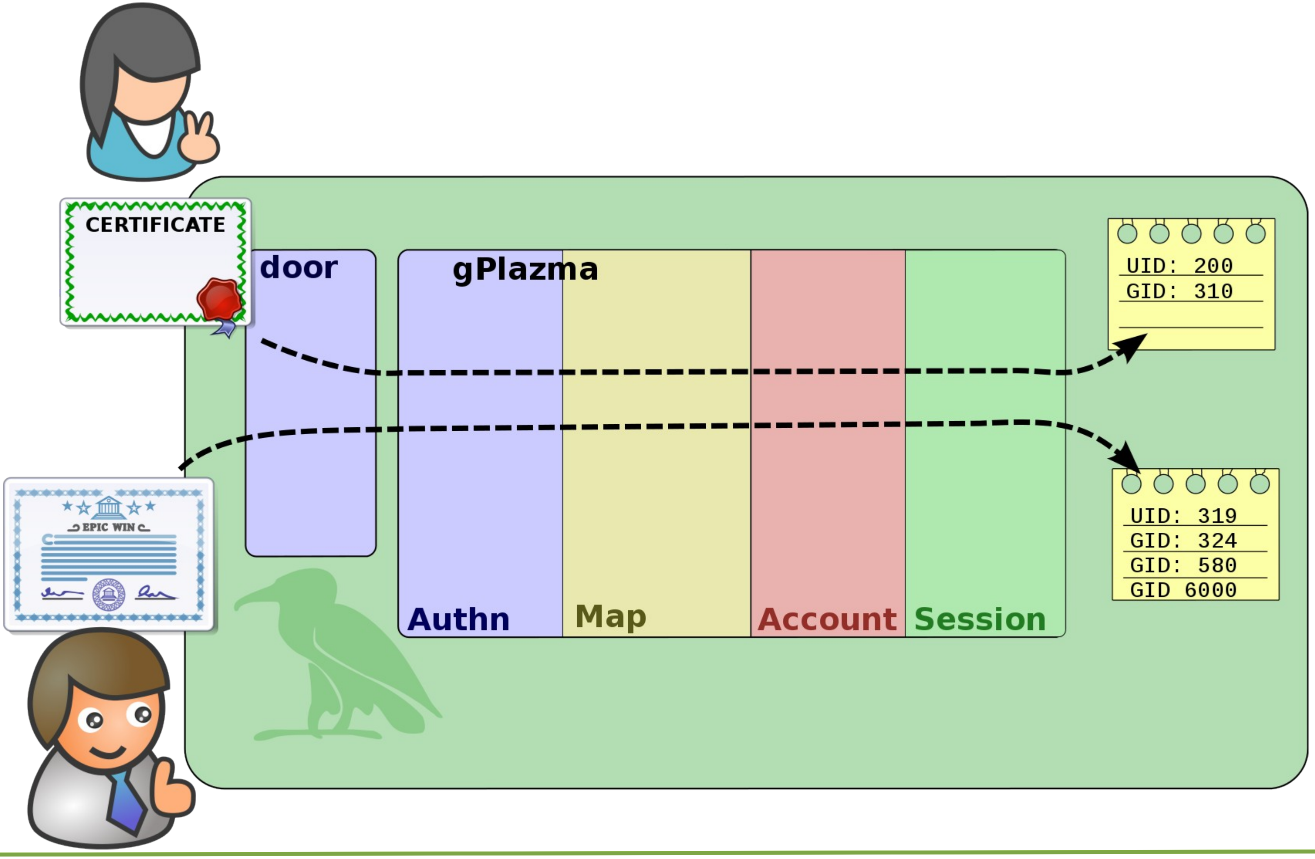
Bank account number: **001213921**
Banks with: **United ACME Bank**

Member-of: **Antagonists Anonymous**

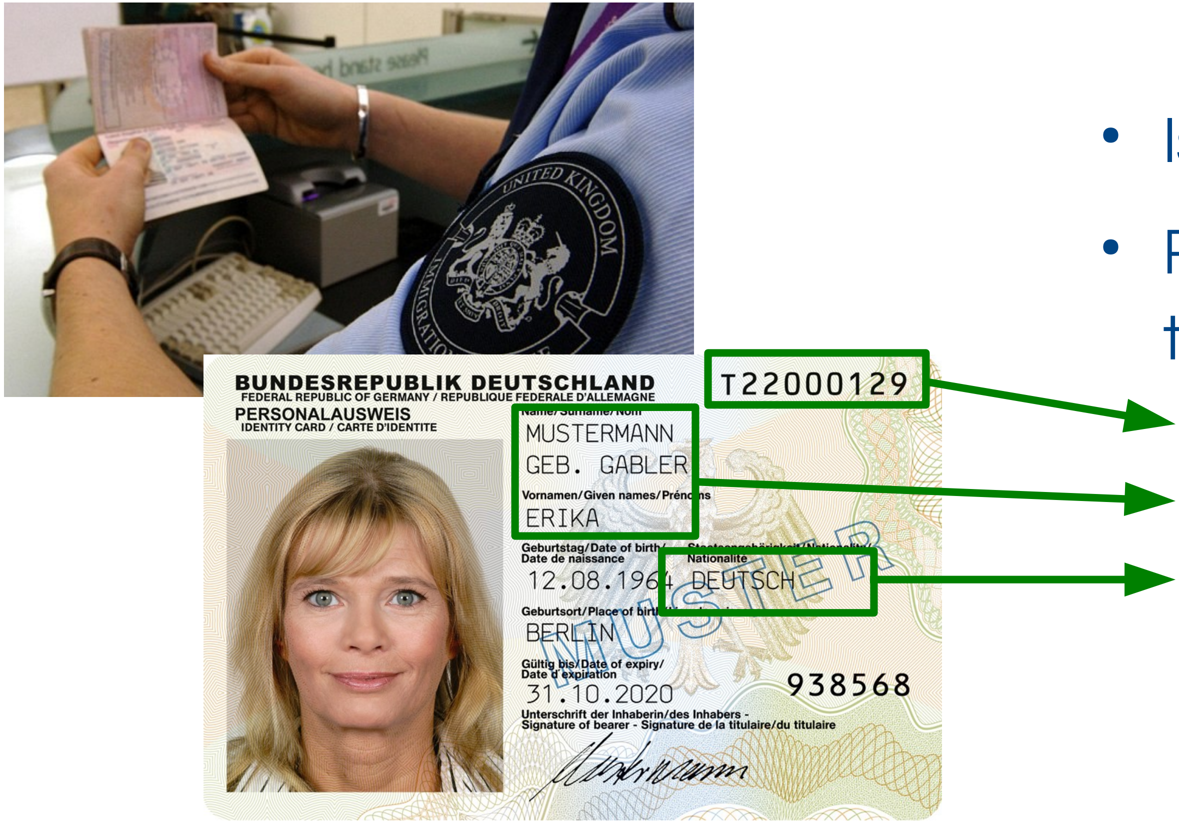
Credentials

Principals

The door and gPlazma



What happens in AuthN phase



BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/
Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/
Nationalite
DEUTSCH

Geburtsort/Place of birth/
BERLIN

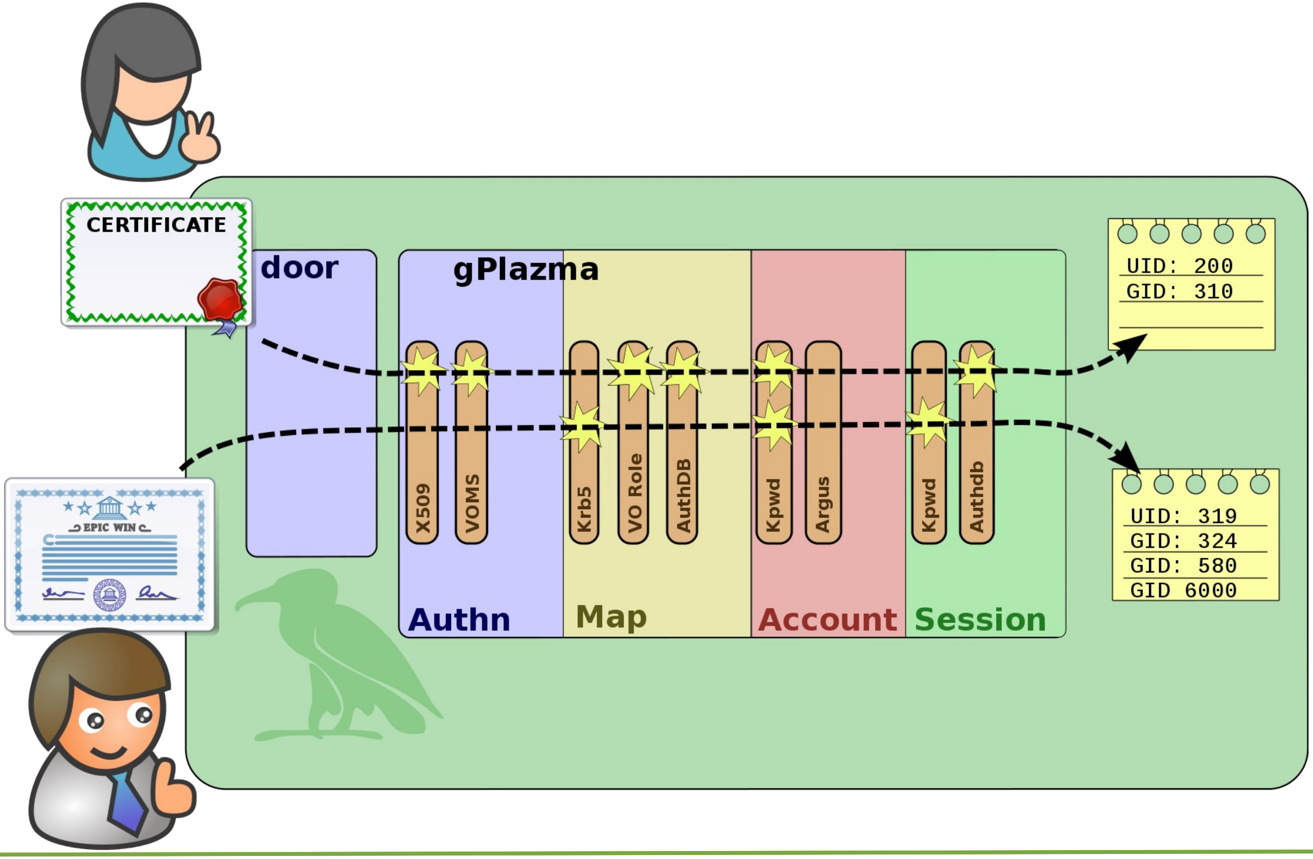
Gültig bis/Date of expiry/
Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers -
Signature of bearer - Signature de la titulaire/du titulaire

- Is the credential valid?
- Pull out information (principals) that describe the person:
  - `Token ID:` **`T22000129`**
  - `Name:` **`ERIKA MUSTERMANN`**
  - `Nationality:` **`German`**

It’s all done with plugins!



dCache and tokens

Protocols supporting bearer tokens

- Underlying **network protocol** needs to (somehow) support bearer tokens:
  - Supporting bearer tokens: **HTTP**, **xroot**.
  - Not supporting bearer tokens: **NFS**, **FTP**.
- dCache **doors** supporting oidc tokens:
  - Using HTTP: **WebDAV**, **SRM**, **REST**.
  - Using xroot: "**xrootd**".

gPlazma support for tokens

- Support is available in the AuthN phase:
  - AuthN phase: Credential → Principals.
  - Subsequent phases use this information.
- There are two AuthN phase plugins to support tokens:
  - **oidc** – identify a person: authentication
  - **scitoken** – identify what bearer is allowed to do: authorisation.
- Either, neither or both tokens may be enabled.
- Compatible with other AuthN (e.g., X.509).

gPlazma support: oidc plugin

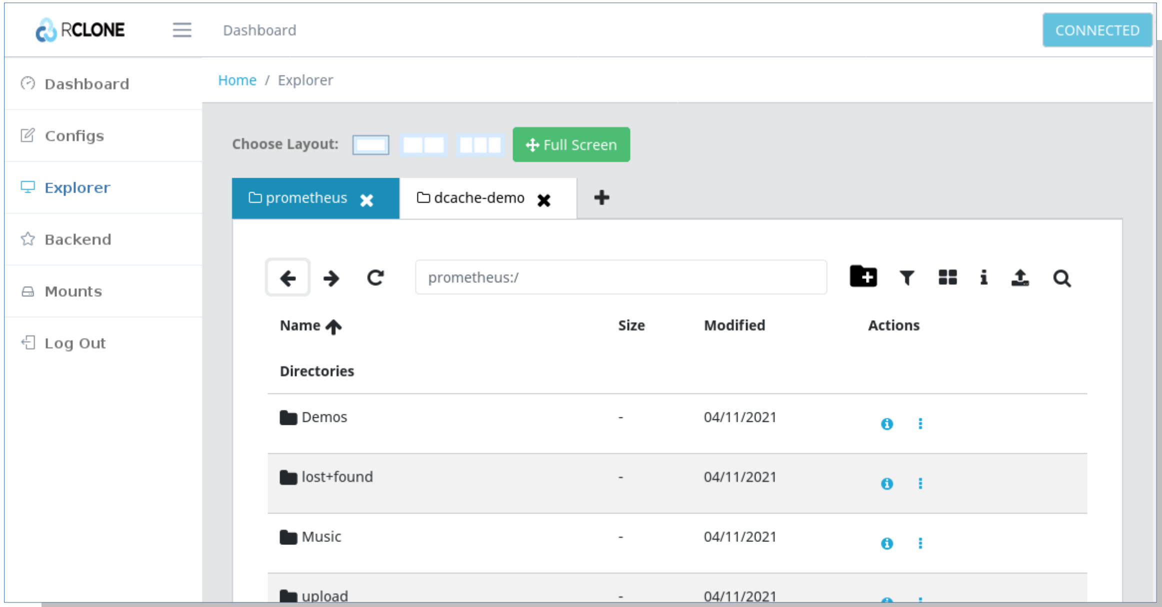
- Calls user-info endpoint to validate token and discover “claims”.
- The OP’s identity → **OauthProviderPrincipal**.
- Maps claims to principals:
  - `sub` → OidcSubjectPrincipal
  - `groups` → OpenIdGroupPrincipal (or GroupNamePrincipal)
  - `eduperson_assurance` → LoAPrincipal
  - `given_name`/`family_name`/`name` → FullNamePrincipal
  - `email` → EmailAddressPrincipal
  - `wlcg.groups` → OpenIdGroupPrincipal
  - `eduperson_entitlement` → EntitlementPrincipal
  - Optionally `preferred_username` → UserNamePrincipal

gPlazma support: scitoken plugin

- Token must be a JWT; uses offline verification.
- Requires token to have either `sub` or `jti` (or both) claims.
- Optional audience protection: based on the `aud` claim.
- Optional replay-attack protection, using `jti`.
- The OP's identity → **OauthProviderPrincipal**
- Maps claims to principals:
  - `sub` → **OidcSubjectPrincipal**
  - `jti` → **JwtJtiPrincipal**
  - `scope` → authorisation information (newer versions override namespace).
- Additional fixed set of principals for this OP (e.g., **GroupNamePrincipal** from VO).

Clients: WebDAV with OIDC tokens

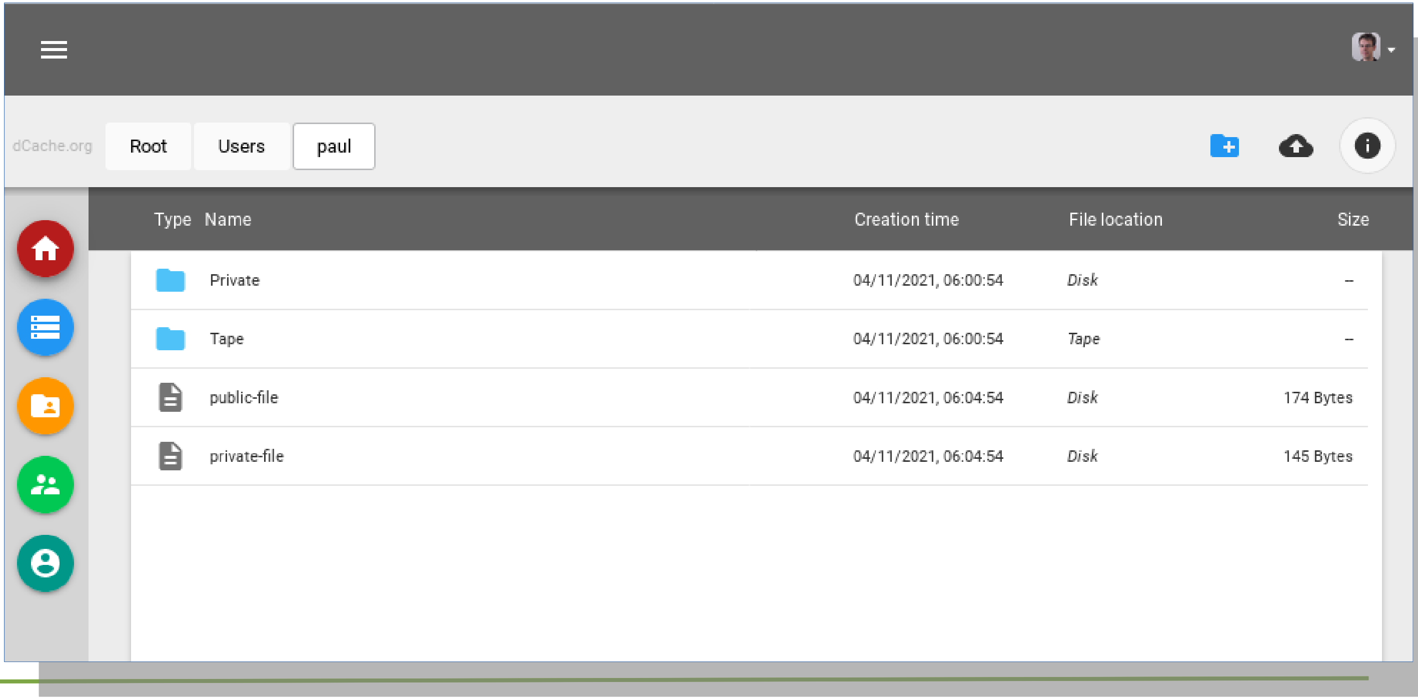
- Our "go to" client here is **rclone**:
  - Supports OIDC via oidc-agent.
- Primarily a **command-line client**, but does provide a web-based GUI.



Name	Size	Modified	Actions
Directories			
Demos	-	04/11/2021	
lost+found	-	04/11/2021	
Music	-	04/11/2021	
upload	-	04/11/2021	

Clients: dCacheView

- JavaScript client shipped with dCache that supports OIDC.
- Uses REST API + WebDAV
- Storage events provide a “live” view of directories.



Type	Name	Creation time	File location	Size
📁	Private	04/11/2021, 06:00:54	*Disk*	–
📁	Tape	04/11/2021, 06:00:54	*Tape*	–
🗎	public-file	04/11/2021, 06:04:54	*Disk*	174 Bytes
🗎	private-file	04/11/2021, 06:04:54	*Disk*	145 Bytes

Future directions

Merging scitoken and oidc plugins

- Not much sense in having two plugins that do (more or less) the same thing.
- Plan to update the `oidc` plugin to support:
  - JWT offline verification;
  - Features of scitoken plugin:

    authorisation (scitoken and WLCG-AuthZ profiles); audience protection; replay-attack protection.
- Support OP-based identity via the OauthProviderPrincipal.

Improved support for Level-of-Assurance

- The **`x509`** and **`oidc`** plugins provide LoA information.
- Currently no dCache-supplied plugins make use of this information.
- In a federated environment, not all authentication mechanisms are the same.
- Use-case: single service hosting resources that require additional "hoops".
- Investigate a "policy" plugin to support enforcing LoA requirements.
- Potential involvement of TFA/MFA ?

Supporting federated environments

- The **HIFIS storage** use-case:
  - Normal activity are through a DESY infrastructure proxy (keycloak) – provides a common service for all on-site services.
  - Also participating as a service in a federated environment: FTS.
- Transfers from FTS use a token from a **community proxy** (!= DESY’s keycloak), but identities are held in the infra proxy.
- Use **token-translation** to convert community-poxy-issued token to a keycloak-issue-token token.

Open questions

Open-question: choosing primary group?

- VOMS (perhaps uniquely) allows a user to **choose** which group is primary.
- In dCache, the primary group is **significant**:
  - Files and directories are group-owned by the primary group.
  - Quota is consumed by primary group.
  - Space consumption uses primary group (sort of).
  - Pins are group-owned based on primary group.
- IAM (like many other OPs) currently don’t support a user choosing which group is their primary group: does this matter?

Open-question: decommissioning accounts?

- Accounts may be **auto-created**:
  - Architecturally, dCache can do this; but we recommend using an infrastructure proxy.
- How does a service **learn** of decommissioned accounts?
  - IAM would first need to discover this.
  - IAM would need to propagate this to dCache.
- Is this problem of interest to IAM?
- Helmholtz is developing an ad-hoc solution – a possibility for standardisation?

The conclusions

(the TL&FA)

Summary

- dCache supports tokens:
  - Both for authentication (OIDC) and authorisation (scitoken/AuthZ) use-cases.
  - It works, but looking at improving it.
  - Also planning to add new features.
- We're also interested in hearing which features people would find useful.

Thanks for listening