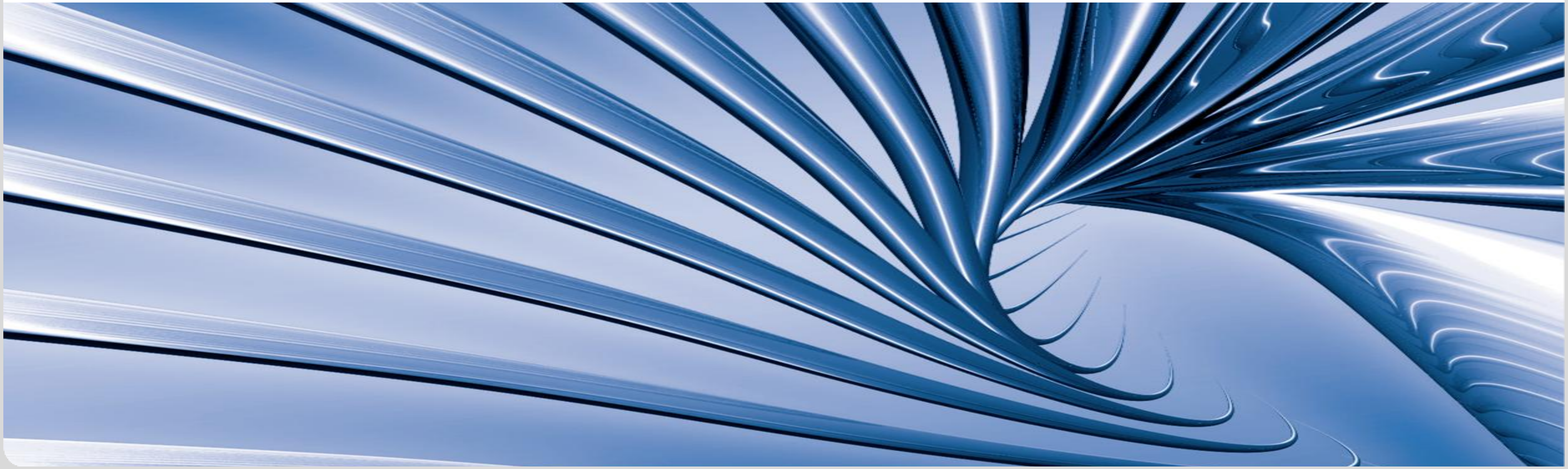
dCache Beginners Course

Access Control

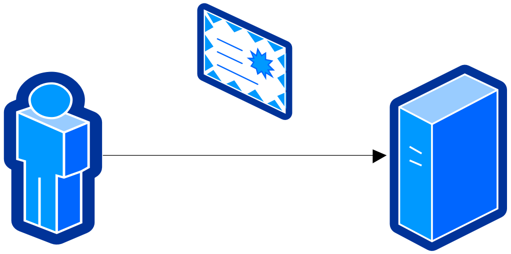
What are the capabilities of dCache for accessing the stored data and admission control?

Karlsruhe Institute of Technology (KIT), Steinbuchcentre for Computing (SCC)



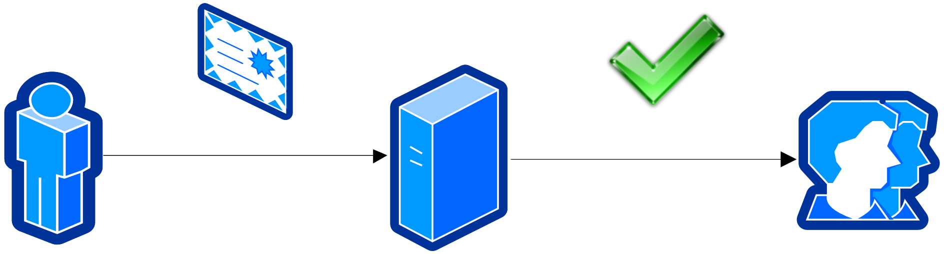
Access Control Systems In dCache

- Access Control in dCache is divided into following steps
  1. If a client is accessing dCache with a secured protocol (*not* DCAP or HTTP) a certificate with the user’s *Distinguished* Name (DN) and optionally one or more *Fully Qualified Attribute Names* (FQANs) must be provided.



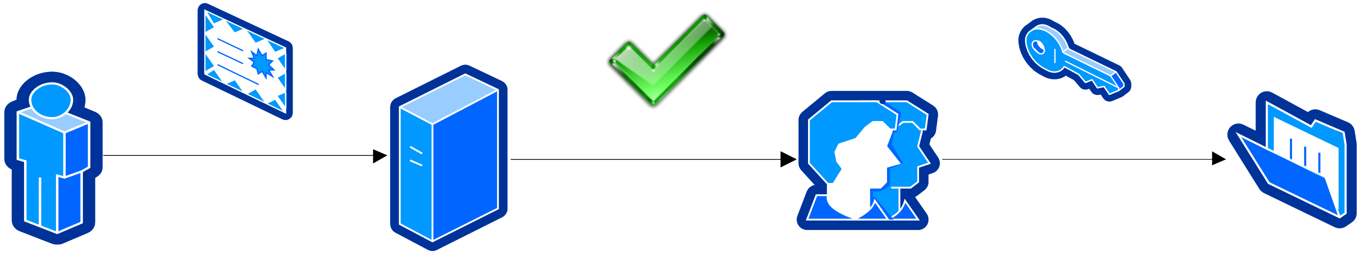
Access Control Systems In dCache

2. In case of successful *authentification* by dCache, the user will be mapped to a virtual, internal user account.



Access Control Systems In dCache

3. Afterwards, this virtual user will be mapped onto actual UNIX user-ID and group-ID(s) specific to the local environment.
4. Using this (final) information, dCache can enforce the configured *authorisation* policy.



Grid Security Infrastructure

- Most services within grids are secured using X.509 certificates, which are used for authentification (and thus indirectly for the authorisation-process), digital signatures and encryption.
- For grid environments, certificates are granted by *Certificate Authorities* (CAs) that are member of the *International Grid Trust Federation* (IGTF).
- A user belonging to a Virtual Organisation (VO) can generate short-living proxy certificates (“grid proxy”) by presenting the grid certificate to the *VO Membership Service* (VOMS).
- The grid proxy may have several attributes like VO role or capabilities attached along with the user’s DN.
- Whenever the user accesses dCache with a (gsi-)secured protocol, a grid proxy is required.

Grid-Aware Pluggable Authorization Management (gPlazma)

- *gPlazma* is the name of the service in dCache that is responsible for authentificating the users.
- As its name indicates, it utilises plugins behind the scenes.
- Tomorrow there will be a session about *gPlazma2*, the successor of gPlazma1.
  - You will learn how to install and configure gPlazma2 tomorrow.
  - For now, we will setup gPlazma1 with very basic configuration.
- The very legacy authentification plugin is *kpwd*, mapping is based solely on the user’s DN.
- The modern plugin is based on VOMS attributes and the plugin is called *gplazmalite-vorole-mapping*.

gplazmalite-vorole-mapping

- Combinations of DN and FQAN are mapped to unique virtual user names.
  - `“DN” [“FQAN”] virtual_user_name`
- The DN can also be set to “`*`”, which serves as a wildcard expression matching any character sequence.
  - This is especially useful when mapping whole VOs.
  - Matches with wildcards are overridden by matches with explicit DNs.
- If the same DN occurs in multiple lines with the same FQAN then only the mapping from the last one is used.
- The same DN can be used multiple times with different FQANs and will be mapped to different virtual user-names respectively.
- If `fqan` is empty or not specified at all, only client-certificates with an empty or no FQAN will match.
- “Disabling entries” (also called “revocation entries”) can be made by using “`-`” as virtual user-name.

Determining Actual User And Group IDs

- gPlazma will test with all enabled plugins to find a valid mapping for the user’s credentials.
  - Only if a plugin does not result in any mapping, the next plugin is applied.
  - Mappings through revocation entries are valid!
- Once the virtual user account is found, dCache will consult the so-called *storage-authzdb*-file.
  - Example:

```
version 2.1
authorize atlas001 read-only  1000 100 / / /
authorize prdatl01 read-write 1001 101 / / /
```

Policies

- dCache can use two different policies, that contain rules on how resources might be accessed.
  1. Traditional POSIX file permissions
  2. Access Control Lists (ACLs)
- ACLs are evaluated in addition to the POSIX file permissions, but supersede them mostly.
- The settings are stored on a per-file basis, managed by Chimera.

Third Chapter Completed!

- Are there any questions?
- If not, try configuring your dCache to allow read-write access for yourself.