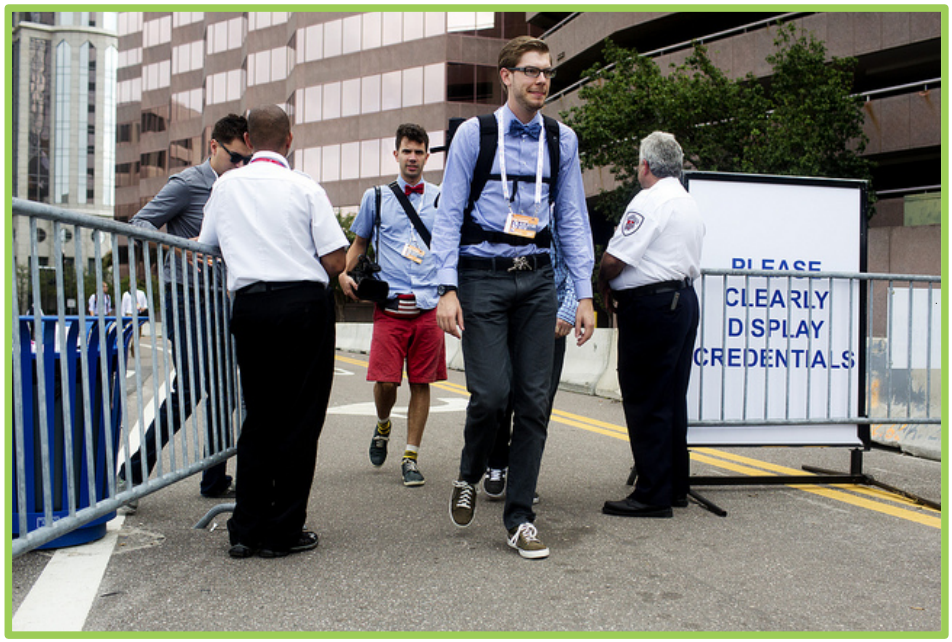
dCache.org

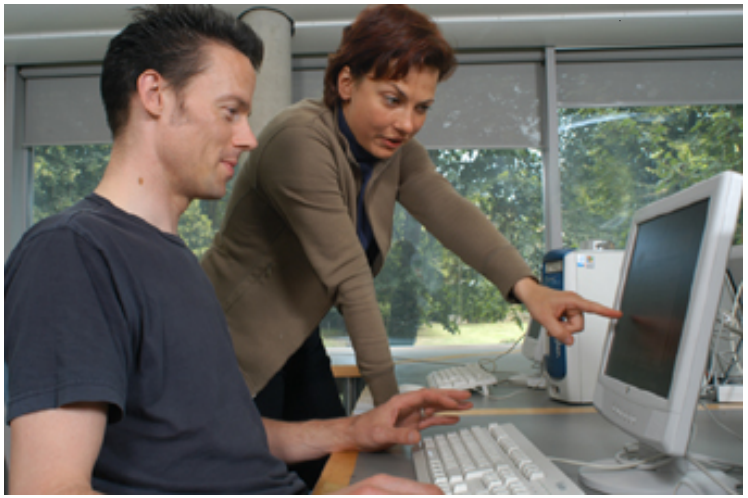
Federated Identity

Paul Millar
DESY, 2014-05-15

Fermilab NDGF Nordic DataGrid Facility DESY HELMHOLTZ ASSOCIATION LSDMA

A gentle introduction...





Can read a file?

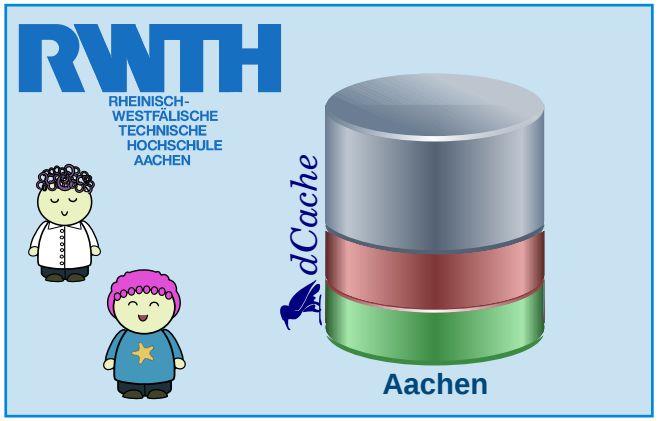
Can write a file?

Can delete a file?

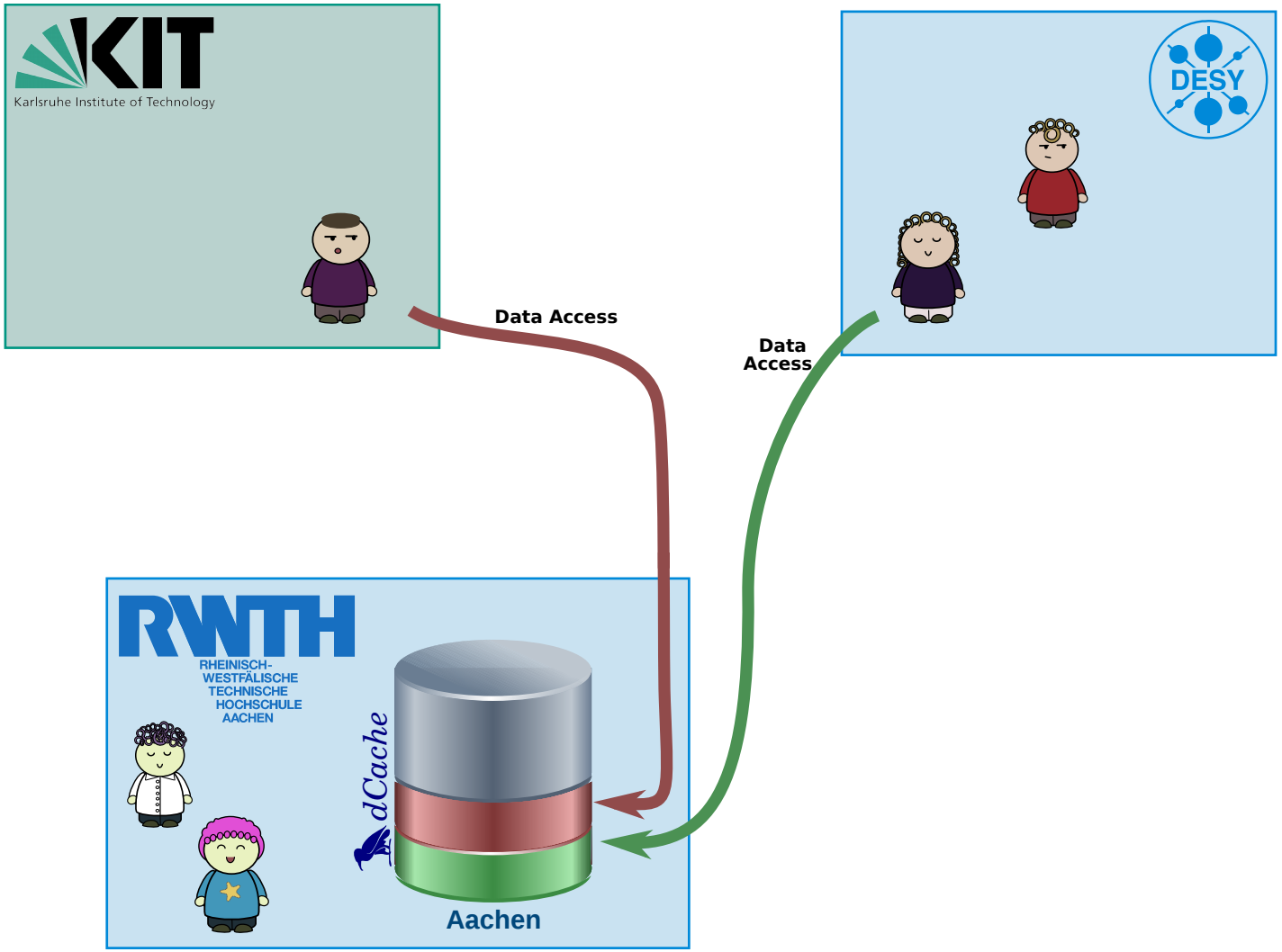
Stage file from tape?

Can create directory?

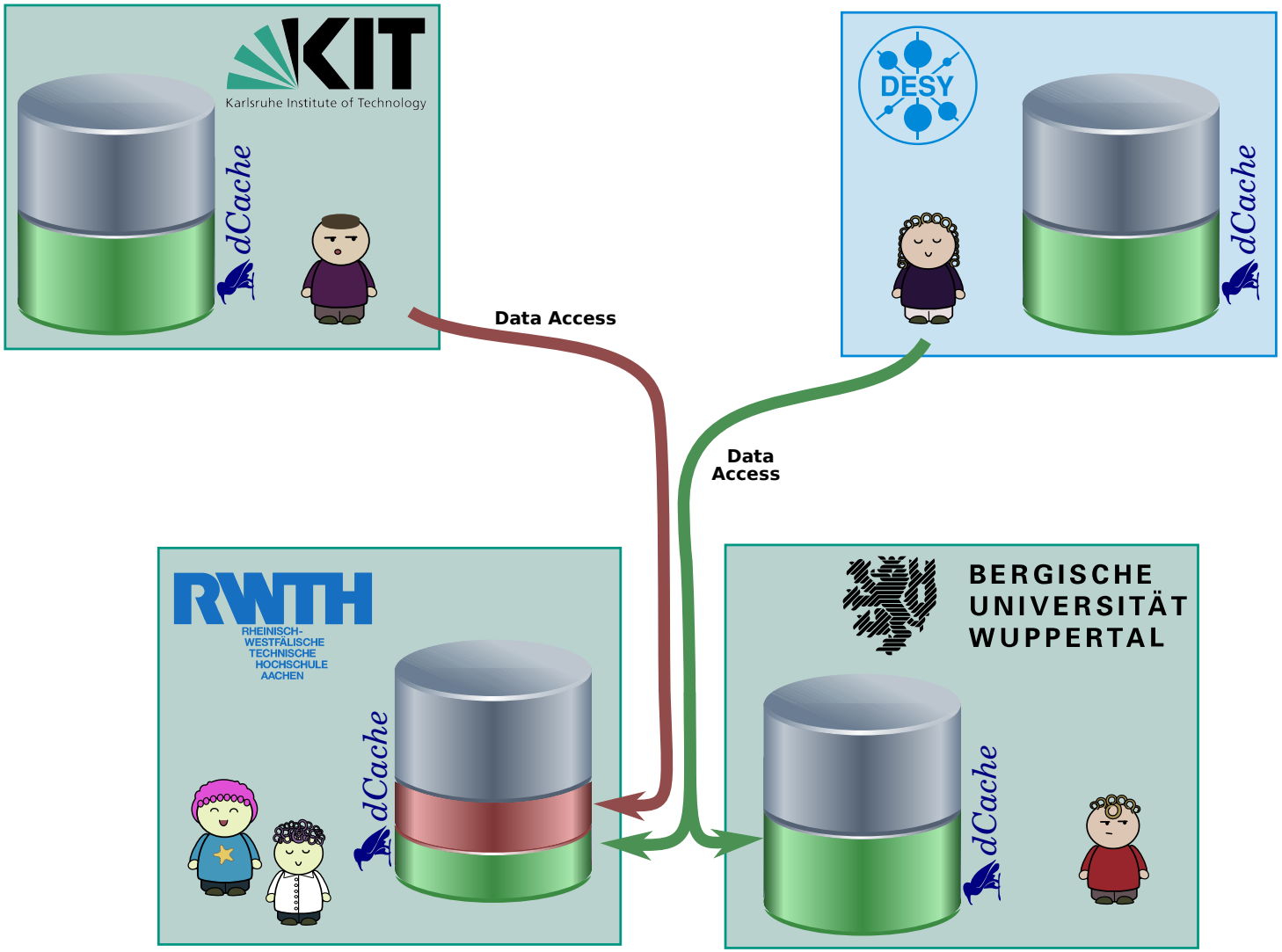
So, what's the problem?



So, what's the problem?



So, what's the problem?



Not new... steps already taken

- There are "single sign-on" ("SSO") solutions,

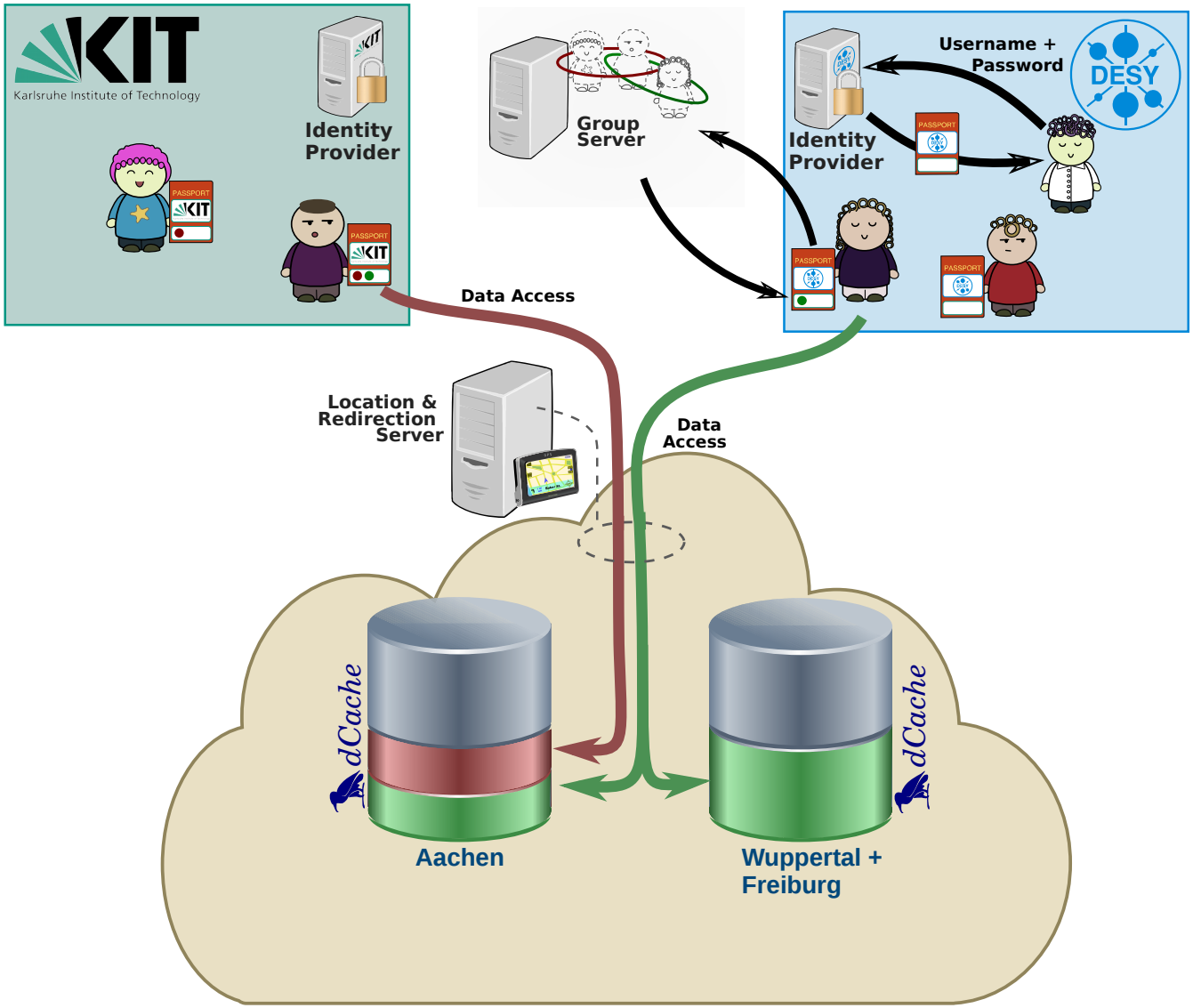
  type in a password once and the system remembers this (for a while) – a sufficient but not necessary solution.

  - The big player is Kerberos
- Another solution: X.509 certificates

  Yes, in theory an excellent solution

  Currently caught in a "vicious cycle"

Other approaches? Federated Identity



Quick check: Grid credentials

- SP: 'DESY ATLAS dCache instance'
- IdP: the 'GermanGrid CA'
- The SP authenticates users from many IdPs.

  Tick: DESY ATLAS dCache instance accepts ATLAS users from many CAs, including GermanGrid CA
- The IdP is accepted by many SPs.

  Tick: people with a GermanGrid CA issued certificate can authenticate with any grid resources, including DESY ATLAS dCache instance

Grid X.509 authentication provides federated identity.

Quick check: OpenID

- SP: Flickr
- IdP: Yahoo
- The SP authenticates users from many IdPs.

  Tick: can also login with Facebook and Google accounts.
- The IdP is accepted by many SPs.

  Tick: many sites provide OpenID authentication with Yahoo

OpenID authentication provides federated identity.

Quick check: Kerberos

- SP: dCache NFS server
- IdP: DESY KDC
- The SP authenticates users from many IdPs.

  No! (not impossible, but hard)
- The IdP is accepted by many SPs.

  Tick (in DESY), No! outside.

(almost all) Kerberos installations are not Federated Identity systems.

The not-a-web-browser problem

- All Fed-Identity systems shown so far assume the user is using a web-browser.

  can make a pretty web-page (in HTML); use anything a web-browser supports for authentication

- Data transfer clients for protocols like

  WebDAV, NFS, FTP, SMB/CIFS, CDMI

  are (almost always) ***not*** a web-browser

- Huston, we have a problem!

Solutions to the not-a-web-browser problem

- Use the web-browser as the transfer agent

  (i.e., dCache's HTTP web-browser interface)

- Use a web portal to manage data transfers:

  "translates" an SAML token to an X.509 credential

  (e.g., Globus Online, web based work-flow engine)

- Fix the clients to "speak Fed-Identity"

  (SAML ECP, Project Moonshot/AbFab)

When are these coming?

- Adding Fed-Identity support to dCache web-browser interface

  Relatively simple, but slated for after 2.10

- Using a web portals

  Already possible (just need to trust the portal's CA)

- Fixing the clients

  Both solutions (AbFab/Moonshot & ECP) are development projects. Both require rolling out of infrastructure, which (in a federated world) means coordinating.

Summary

- Fed-Identity allows your users to use dCache with their existing credentials,
- It's already possible with a web-portal solution (with some limitations)
- We plan to:
  - Add more features to the web interface.
  - Investigate auto-enrolment for creating new users.
  - Engage with others to support fed-identity clients.

Thanks for listening

Backup Slides

The trust problem: SPs trusting the IdP

- They always identify the same person

  don't reuse identifiers, password database isn't compromised, ...

- Information is reliable

  checked a passport to know the name, ...

- Inform them if an identity has been compromised

  “how” is a good question.

The trust problem: IdPs trusting the SP

- Don't pass on personal information to others

  don't leak/sell information to spammers, news papers, ...

- Don't track their users habits

  knowing the activity of a Nobel Laureate for Medicine may have commercial value

- Will report suspicious activity

  “how” is another good question

Solutions to the trust problem

- For SAML, people are building federations to solve these problems
  - Set of rules so people know what to expect.
  - Taking the pragmatic approach: trust + real-world → contract.

    Makes joining a federation hard
  - Makes inter-federation (federations of federations) also hard ("weakest link")
- Everything else, it's a Wild West:

  The IdP-trusting-SP problems are less because (typically) less information is shared

  The SP-trusting-IdP problems are not dealt with.

The split-personality problem

- A user many have **many ways** of authenticating:

  Kerberos, X.509, SAML, OpenID, ssh pub/priv keys

- Most people agree that authorisation decisions should be against a **person**
- A service need to "merge" these identities
  - Currently, **gPlazma works**, but requires manual configuration
  - Outside of dCache, there's no good, general solution :-/

The account life-cycle problem

- Some student from the University of Baden-Baden uses your dCache for the first time

  "Easy" some enrolment process takes place, either automatic or requires users to register themselves
- User stores data in dCache
- Later, the student leaves the University of Baden-Baden
- What should happen?
  - First, how does your dCache know the user has left?
  - Second, what should dCache do now?