gPlazma2

dCache's new Authentication Module

Dipl.-Inf. Karsten Schwank
(DESY)

Outline

- A short review of gPlazma1
  - Weaknesses
- gPlazma2
  - Architecture
  - Configuration
  - Plug-Ins in 1.9.12 [EMI-1]
- Introducing ARGUS
- Summary

gPlazma1 Review

- Collection of
- Around for several years
- Use-Cases known
- No need for real Plug-Ins
- Monolithic Architecture and Data Structure

gPlazma1 Functionality

- KPWD
- Grid-Mapfile
- VORoleMap
- SAML
- XACML

gPlazma1 Weaknesses

- Inflexible
- New functionality hard to integrate
- More and more work goes into re-factoring
- No easy way to extend by third parties.

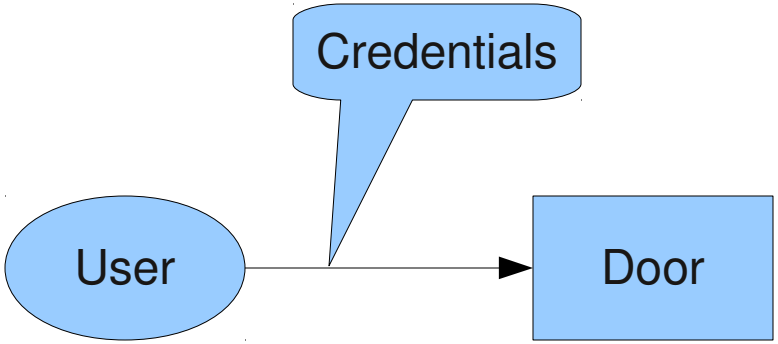
gPlazma2

- Reimplementation
- Modular Architecture
- Flexible Configuration
- Extensible by “real” Plug-Ins
  (possibly by third parties)

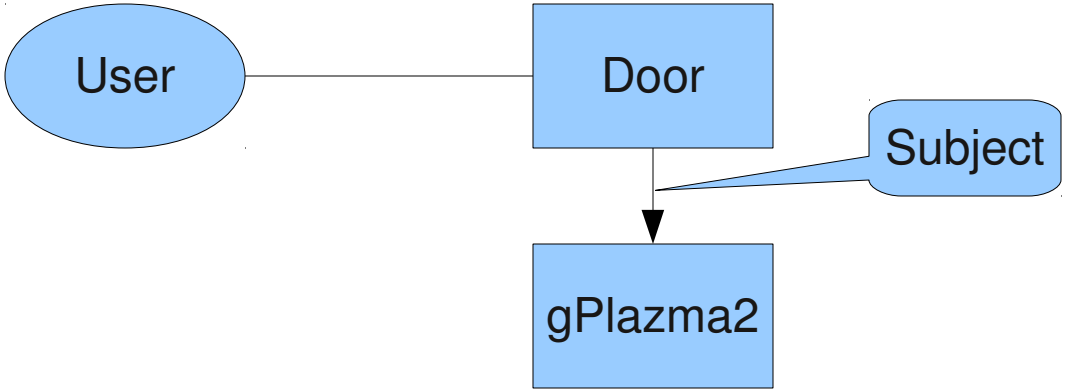
Architecture

- Common interfaces
- Single class, single responsibility
- Separation between 4 different login-steps
- Each login-step is extensible by easy implementable plug-ins.

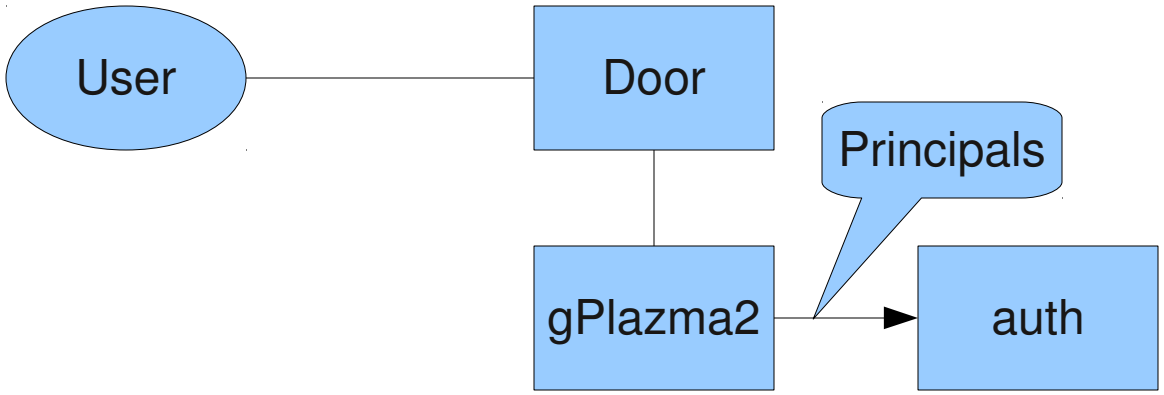
Login Sequence



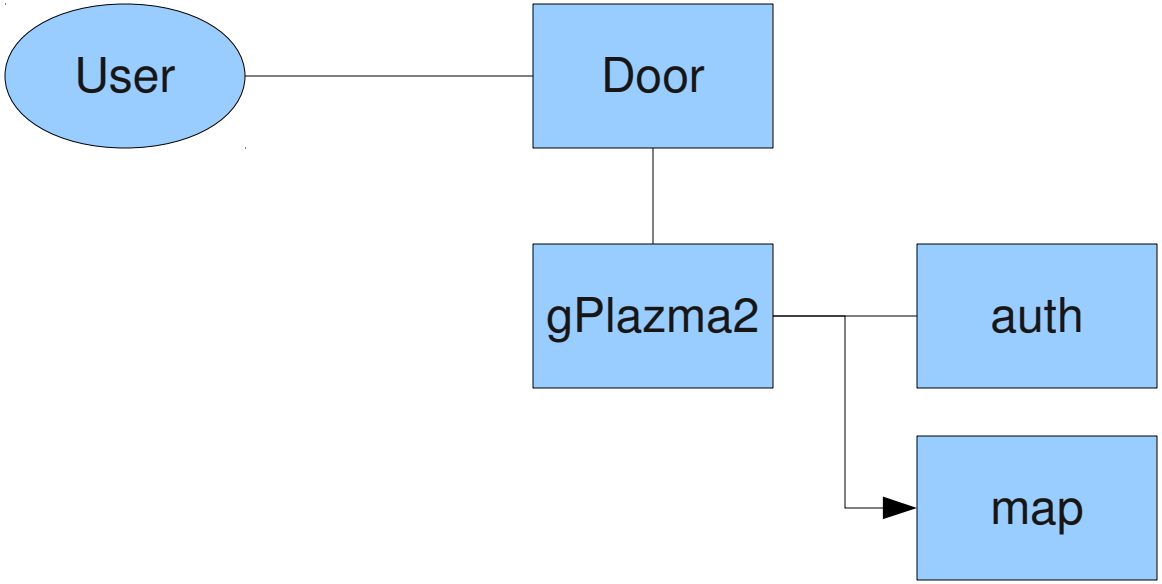
Login Sequence



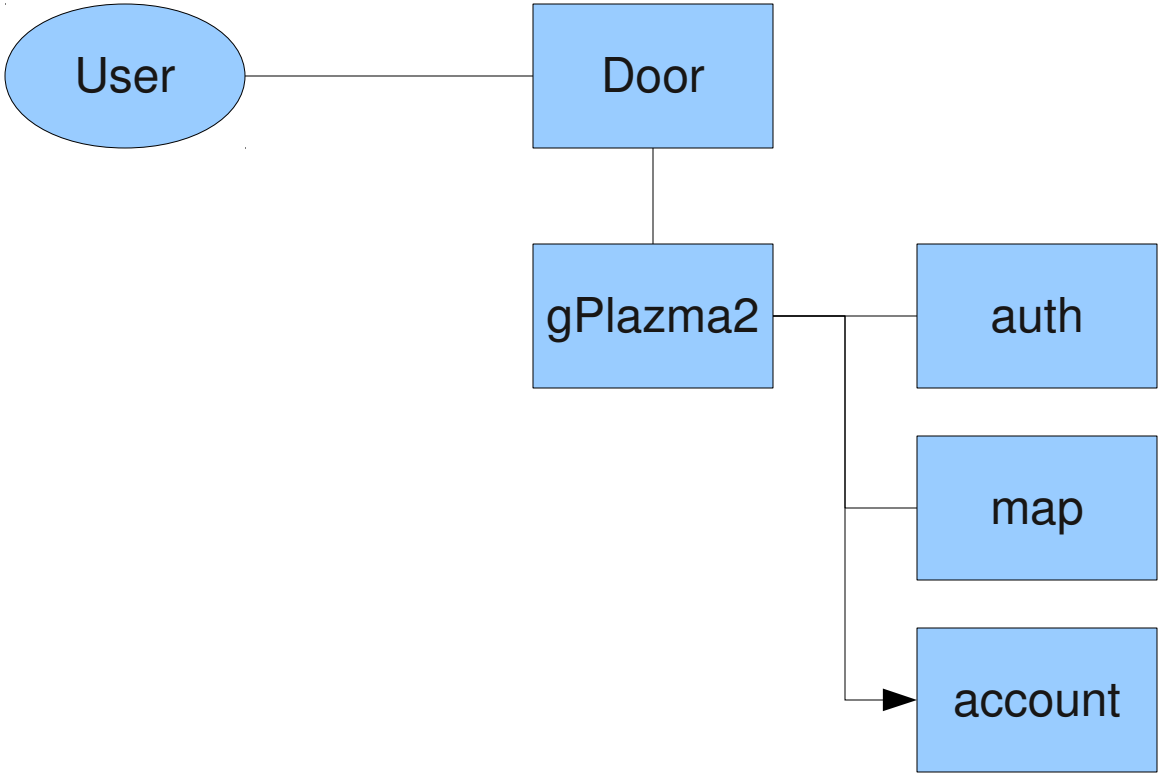
Login Sequence



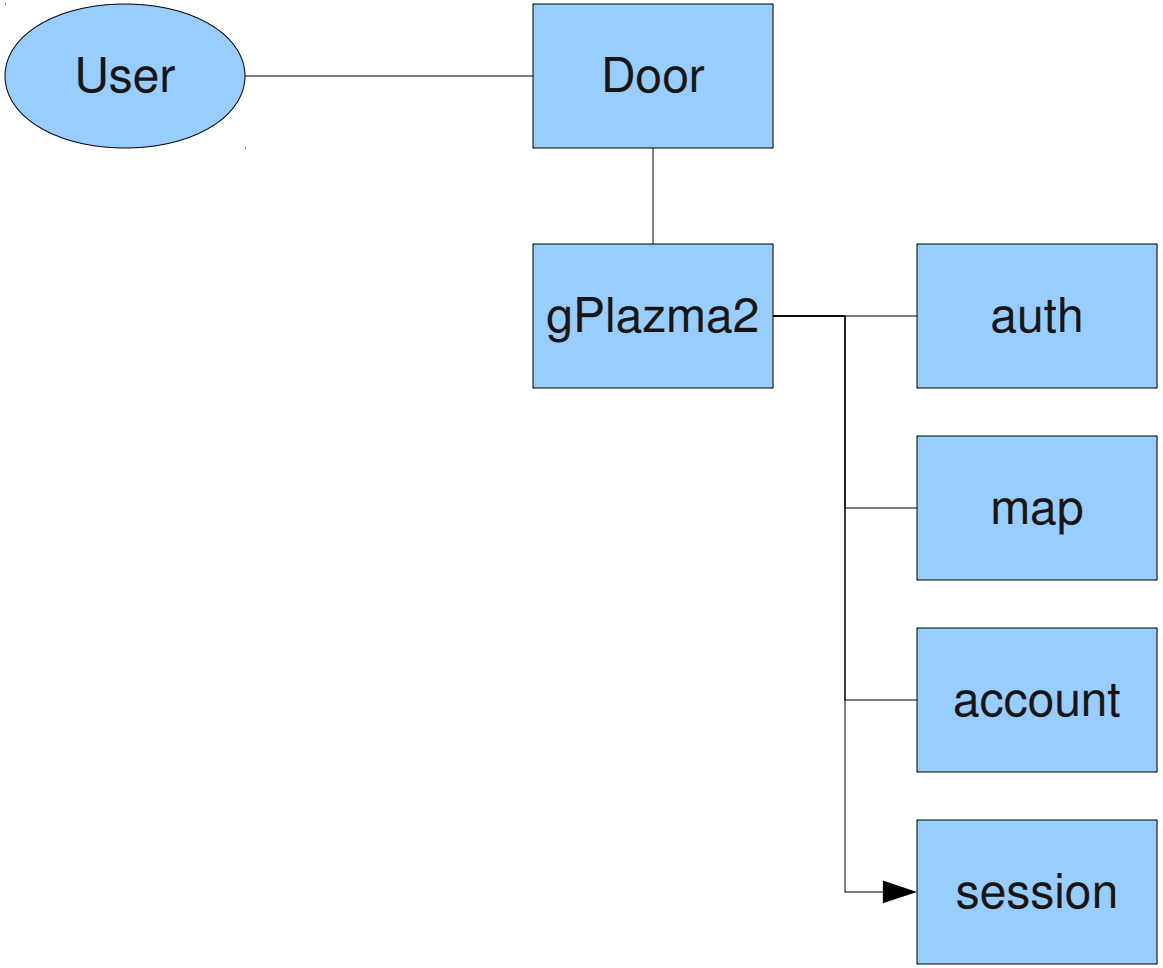
Login Sequence



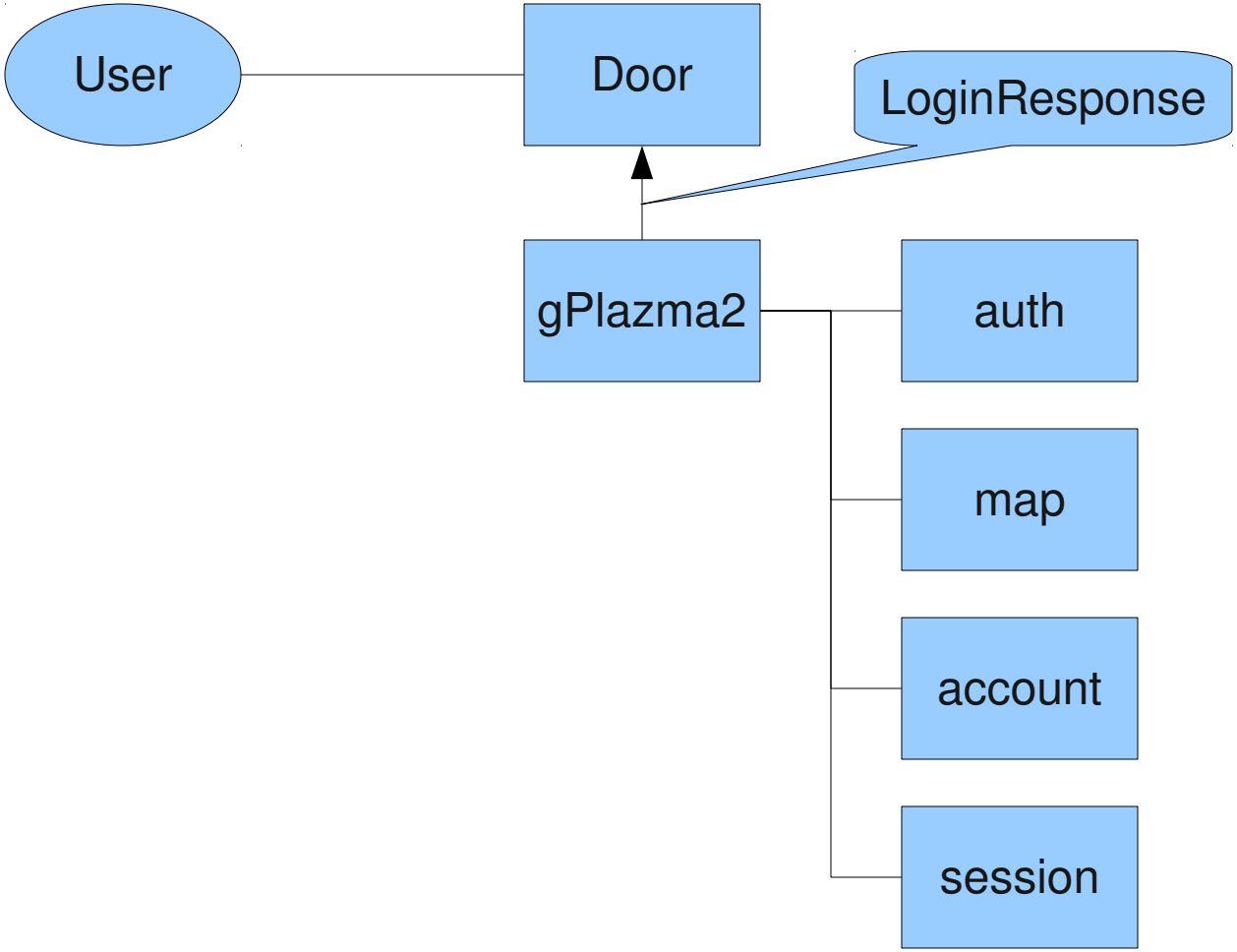
Login Sequence



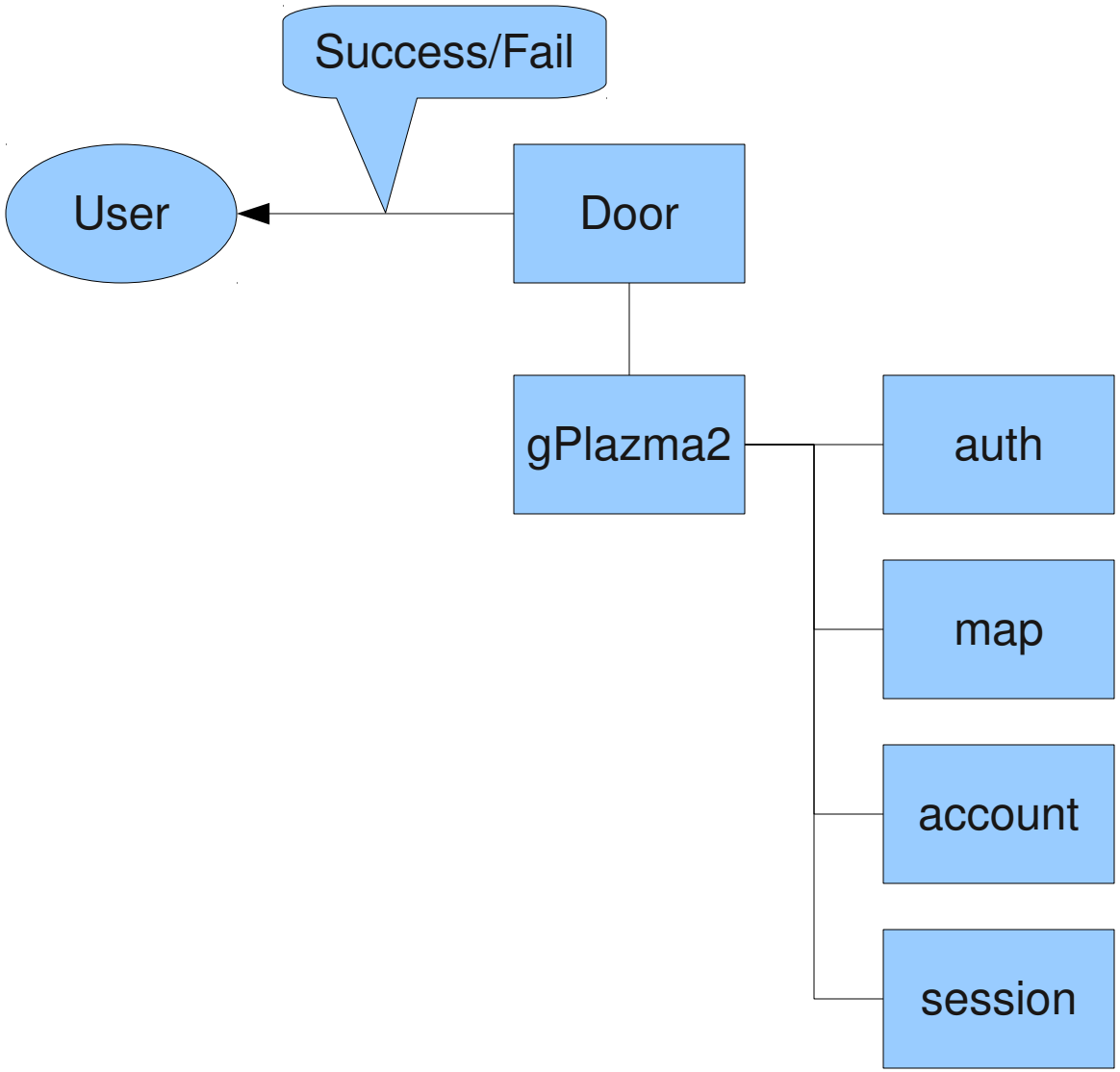
Login Sequence



Login Sequence



Login Sequence



Configuration

- PAM like file `etc/gplazma2.conf`
- 4 columns:
  - Type: auth, map, account, session
  - Modifier: optional, sufficient, required
  - Plug-In name
  - Plug-In parameters

```
<type> <modifier> <name> [<key>=<value>]*
```

Configuration II

- Modifiers:
  - `optional`: Success not critical to login step
  - `sufficient`: Success sufficient for login step to succeed
  - `required`: Success required for login step to succeed
  - `requisite:`on failure the whole login is immediately terminated

Configuration Example

- Required steps:
  - Auth
  - Map
- Optional steps:
  - Account
  - Session

```
# file: gplazma2.conf
auth     requisite   VORoleMap "vorolemap=/etc/vorolemap"
map      sufficient  VORoleMap
account  required    Argus     "PEPEndpoint=https://argus.
```

Plug-Ins in dCache 1.9.12

- KPWD (auth, map)
- VORoleMap (auth, map)
- NIS/LDAP (map)
- ARGUS blacklisting (account)

VORoleMap Plug-In

- Works with existing configuration files
  - vorolemap
  - storage-authzdb
- Functionality
  - Authentication
  - Mapping

KPWD Plug-In

- Works with existing configuration file
  - dcache.kpwd
- Functionality
  - Authentication
  - Mapping

NIS/LDAP Plug-In

- Uses existing site's Directory Service
  - NIS
  - LDAP
- Functionality
  - Mapping

ARGUS Plug-In

- Uses existing site's ARGUS System
- Functionality
  - Account verification by DN
  - Authentication and mapping to come

Near Future Plans

- Plug-In Architecture allows fine grained mapping
  - DN → UID
  - FQAN → GID

Expert Configuration

- Add custom Plug-Ins in `gplazma-plugins.xml`

```
<!-- file: gplazma-plugins.xml -->
<plugins>
  <plugin>
    <name>VORoleMap</name>
    <class>
      org.dcache.gplazma.plugins.GPlazmaVORolePlugin
    </class>
  </plugin>
  <plugin>
    <name>Argus</name>
    <class>
      org.dcache.gplazma.plugins.GPlazmaArgusPlugin
    </class>
  </plugin>
</plugins>
```

gPlazma2 Activation

- Old gPlazma is default.
- To activate gPlazma2 edit gPlazma service section in the layout file:

```
[authDomain]
[authDomain/gPlazma]
gplazma.version = 2
```

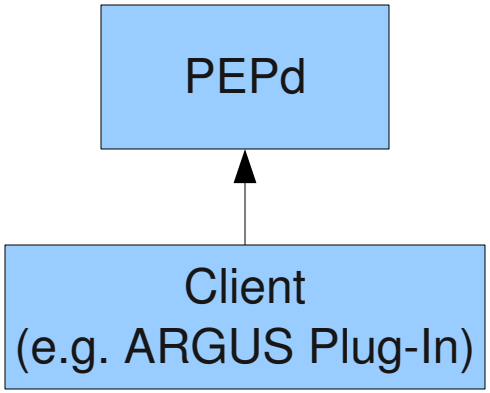
ARGUS

- Component of EMI
- Somewhat similar to SCAS
  - Central authorization
- 3-layers
  - Policy Administration Point (PAP)
  - Policy Decision Point (PDP)
  - Policy Enforcement Point (PEP)

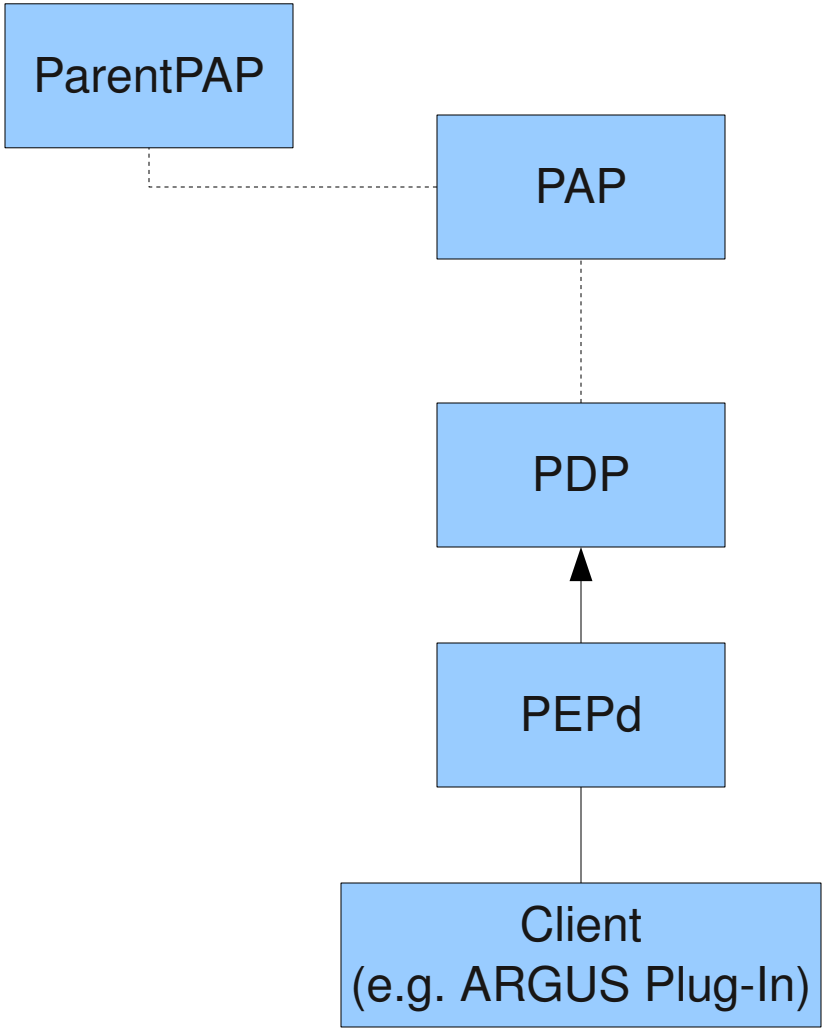
ARGUS Request Sequence

Client
(e.g. ARGUS Plug-In)

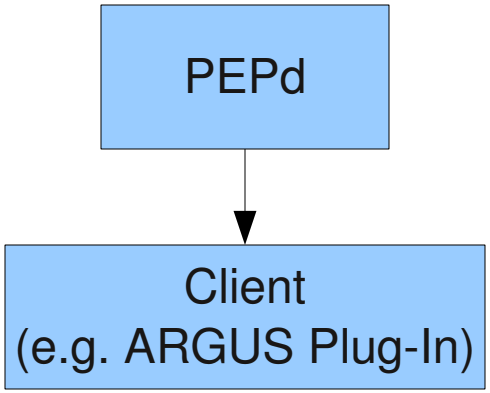
ARGUS Request Sequence



ARGUS Request Sequence



ARGUS Request Sequence



ARGUS Functionality

- Authorization
- Mapping
- Blacklisting

ARGUS Setup

- All three (PAP, PDP, PEPd) come in separate TGZ-Archives

  Unpack e.g. to /opt
- Common directory structure:
  - bin, conf, lib, logs
- Configurable with standard ini-files
- Usable defaults
- `pepd.ini` needs some adjustment for dCache

PEPd Configuration for dCache

- PEPd comes with a good default `pepd/conf/pepd.ini`
  - Enter site specific info (e.g. paths)
  - comment out `pips` and `obligationHandlers` decalaration.

```
[SERVICE]
entityId = https://karsten-vm01.desy.de/pepd
hostname = karsten-vm01.desy.de
port = 8154
adminPort = 8155
adminPassword =

# pips = WHITELIST_PIP GRIDAUTHZPROFILE_PIP
# obligationHandlers = ACCOUNTMAP_OH
```

gPlazma2 Summary

- Clean architecture
- Flexible configuration
- Extensible functionality
- Existing plug-ins compatible with gPlazma1 configuration files
- Additional security via Argus blacklisting

Argus Summary

- Fine grained policy definition
- Central Policy Administration
- Distributed Policy Enforcement
- Authentication, Mapping, Blacklisting

Information and Support

- gPlazma2:

  dcache.org (Manual, Wiki)

  eMail: support@dcache.org

- ARGUS:

  twiki.cern.ch/twiki/bin/view/EMI/Argus

Thank you

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611