EUROPEAN MIDDLEWARE INITIATIVE

Gplazma2

dCache's new Authentication Module

Dipl.-Inf. Karsten Schwank
(DESY)

Outline

- A short review of gPlazma1
  - Weaknesses
- gPlazma2
  - Architecture
  - Plug-Ins in 1.9.12 [EMI-1]
- Introducing ARGUS
- Future Plans
- Questions/Ideas

gPlazma1 Review

- Around since 200?
- Use-Cases known and fixed
- No need for real Plug-Ins
- Monolithic Architecture and Data Structure

gPlazma1 “Plug-Ins”

- KPWD
- Grid-Mapfile
- VORoleMap
- SAML/GUMS
- XACML

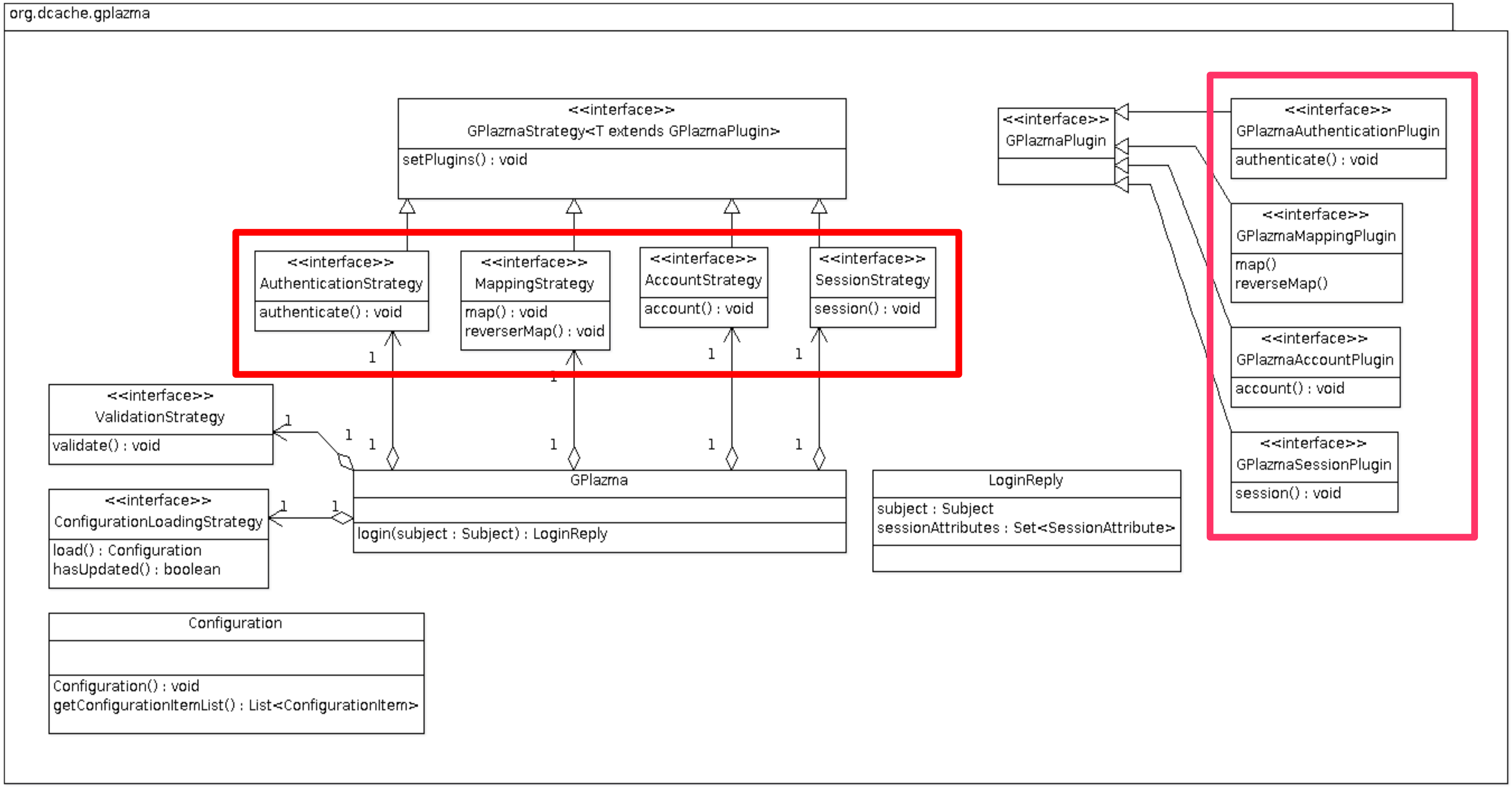
gPlazma1 Weaknesses

- 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)

gPlazma2 in UML



org.dcache.gplazma

<<interface>>
GPlazmaStrategy<T extends GPlazmaPlugin>
setPlugins() : void

<<interface>>
AuthenticationStrategy
authenticate() : void

<<interface>>
MappingStrategy
map() : void
reverserMap() : void

<<interface>>
AccountStrategy
account() : void

<<interface>>
SessionStrategy
session() : void

<<interface>>
ValidationStrategy
validate() : void

<<interface>>
ConfigurationLoadingStrategy
load() : Configuration
hasUpdated() : boolean

GPlazma
login(subject : Subject) : LoginReply

LoginReply
subject : Subject
sessionAttributes : Set<SessionAttribute>

Configuration
Configuration() : void
getConfigurationItemList() : List<ConfigurationItem>

<<interface>>
GPlazmaPlugin

<<interface>>
GPlazmaAuthenticationPlugin
authenticate() : void

<<interface>>
GPlazmaMappingPlugin
map()
reverseMap()

<<interface>>
GPlazmaAccountPlugin
account() : void

<<interface>>
GPlazmaSessionPlugin
session() : void

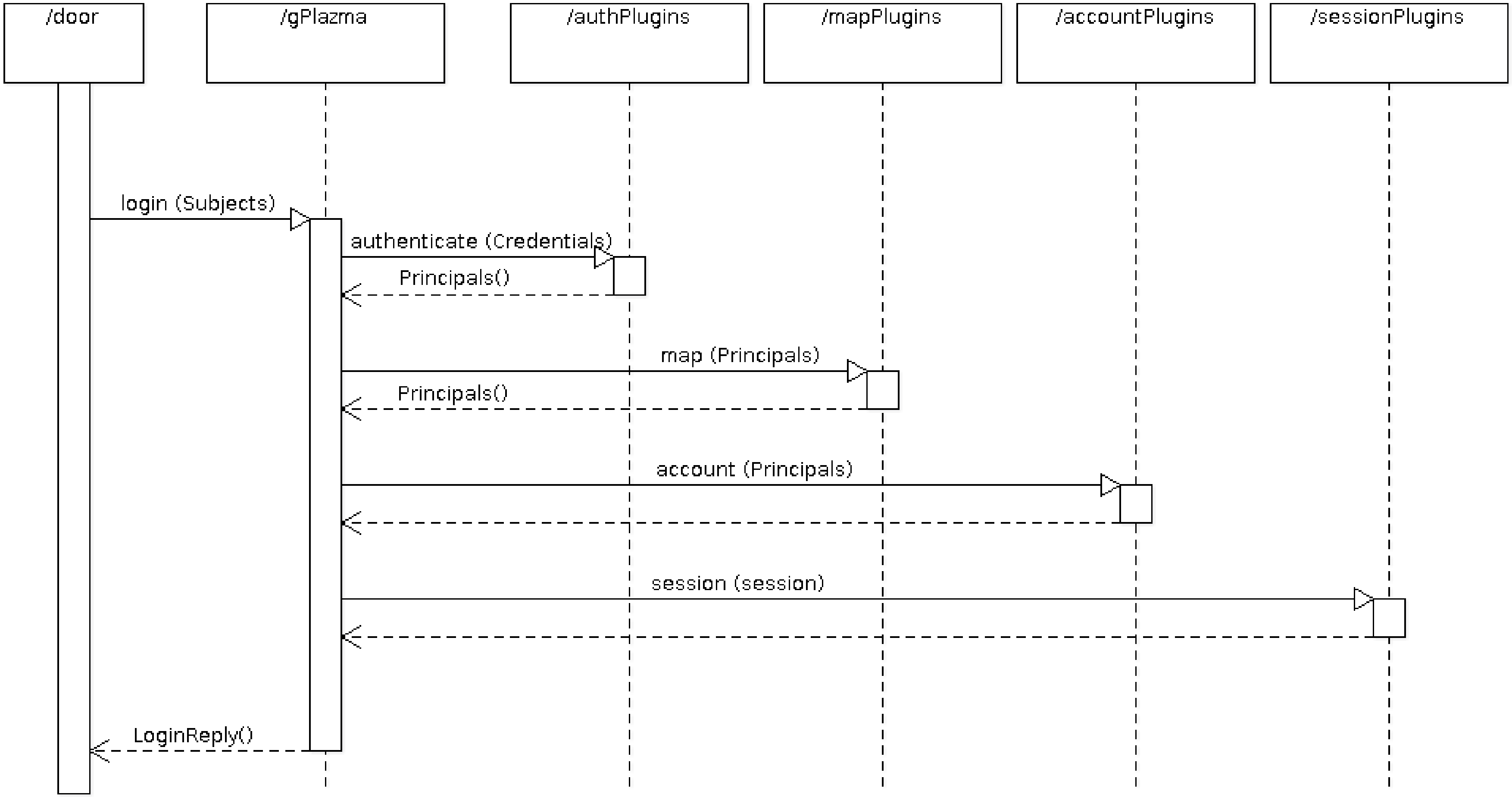
gPlazma2

- 4-Step Authorization
  - Authentication
  - Mapping
  - Account Verification
  - Session Verification

Login

- User accesses door
- Door collects credentials and creates Subject
- Door sends Subject to gPlazma
- gPlazma calls plug-ins:
  - authenticate
  - map
  - account
  - session
- gPlazma returns LoginReply to door
- Door allows/disallows entry

Login: Sequence Diagram



Configuration

- PAM like file format:

```
# file: /opt/d-cache/etc/gplazma2.conf
auth    sufficient    VORoleMap              "vorolemap=/etc/grid-security/vorole
auth    optional      KpwdUsernamePassword   "kpwdfile=/opt/d-cache/etc/dcache.kp
map     sufficient    VORoleMap
map     optional      KpwdUsernamePassword
account required      Argus                  "PEPEndpoint=https://example.org:815
```

- Configurable Plug-Ins:

```
<!-- 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>
```

Plugins in dCache 1.9.12

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

VORoleMap Plugin

- Works with existing files
  - vorolemap
  - storage-authzdb
- Authentication: DN/FQAN → Name
- Mapping: Name → UID/GID

KPWD Plug-In

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

NIS/LDAP Plugin

- Uses NIS or LDAP Server for authentication

ARGUS Plug-In

- ARGUS Authentication Service
  - Centralised configuration for distributed systems
  - Supports blacklisting by DN
  - And more... in the future

ARGUS

- Centralized but distributed
- PAP, PDP, PEP
- Authorization
- Mapping
- Blacklisting

ARGUS

European Middleware Initiative

EMI INFSO-RI-261611

EUROPEAN MIDDLEWARE INITIATIVE

Thank you

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