Identity management issues in the gCube framework

Diligent

A DIgital Library Infrastructure on Grid ENabled Technology

Paolo Roccetti

Engineering S.p.A.

Outline

- The gCube environment
- The approach to identity management
- Current implementation
- Credentials flowchart
- Involved Services
- Future directions

The gCube environment

Entities:

- Running instances (RI)
  - Dynamically pop-up in the infrastructure
  - Act autonomously
  - Interact with other services (gCube and gLite ones)
- Users
  - Weakly authenticated (email address, username, pwd)
  - Strongly authenticated (CA)

The approach to identity management

- Each entity should have an identity.
- Uniform the identity management in the infrastructure
  - behind the portal
  - between users and services
- Provide services with valid credentials when they run in the infrastructure
- Administrators liable for RI that autonomously access the grid
  - Analogy with CA rules
- Identities can be shared among entities
  - With rules

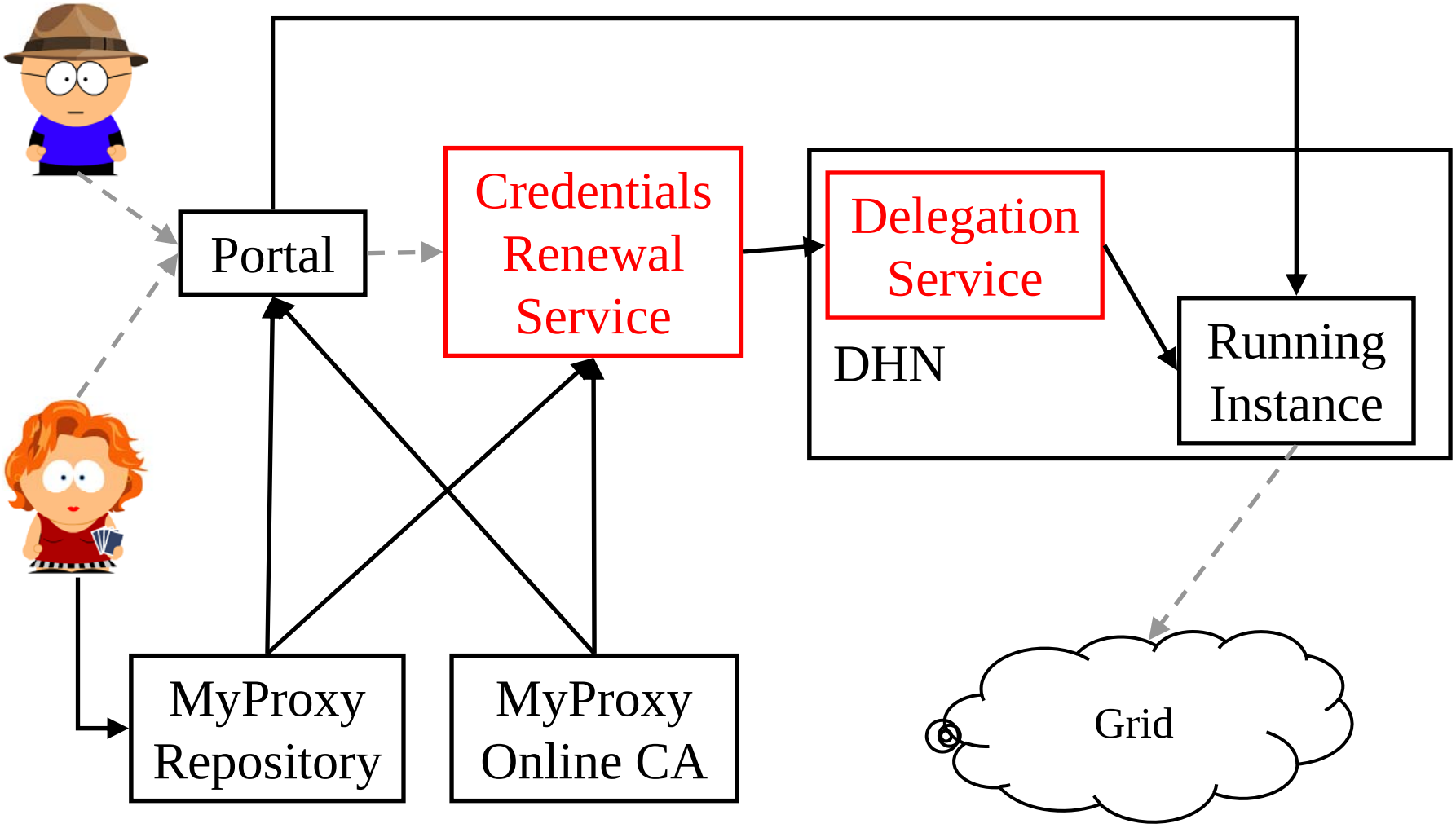
Current implementation

- X.509 certificates to represent identities in the infrastructure

- Credentials are:
  - get from a MyProxy repository or
  - generated on-the-fly by a MyProxy Online CA

  - Transparently loaded by the portal during the session
  - Periodically dispatched to services

Credentials flowchart



Involved services

- Credentials Renewal service
  - Periodically refresh credentials for RI
- Delegation Service
  - Dispatch received credentials to co-hosted RI
- Portal
  - Load user credentials at login (or when needed)
- MyProxy Online CA
  - Create credentials for weakly authenticated users
- MyProxy Repository
  - Store credentials of strongly authenticated users and service administrators

Future directions

- Increase:
  - Scalability
    - CredentialsRenewal service federation
  - Robustness
    - MyProxy-renew functionality
  - Interoperability
    - Shibboleth
- Explore new approaches
  - Identities plugged into AC
    - SAML assertions to identify the user
    - Shibboleth
  - Web of trust
    - OpenPGP