Authentication, Authorisation and Accounting

Marco Leonardi
Albrecht Schmidt

20/05/2016

Issue/Revision: 1.0
Reference: EMSS-EOPG-HO-16-021
Status: Draft

Summary

- Authentication and Authorisation
- Accounting
- Federated End-to-end use case for Thematic Exploitation Platform (TEP)
- Workplan

Authentication and Authorisation (1)

- Assumptions:
  - The user has a digital identity he can use in order to access services
  - The user's digital identity can be provided by several entities like the user's Organization or (in the future) the user's country government; legal implications to be considered about EU directives for digital identities
  - The user is able to access local and federated services via an authentication process and to use them after an authorization process implemented by the services
  - The user's digital identity is associated with a set of attributes related to the user that allow the services to authorize user's requests and to provide the proper service level

Authentication and Authorisation (2)

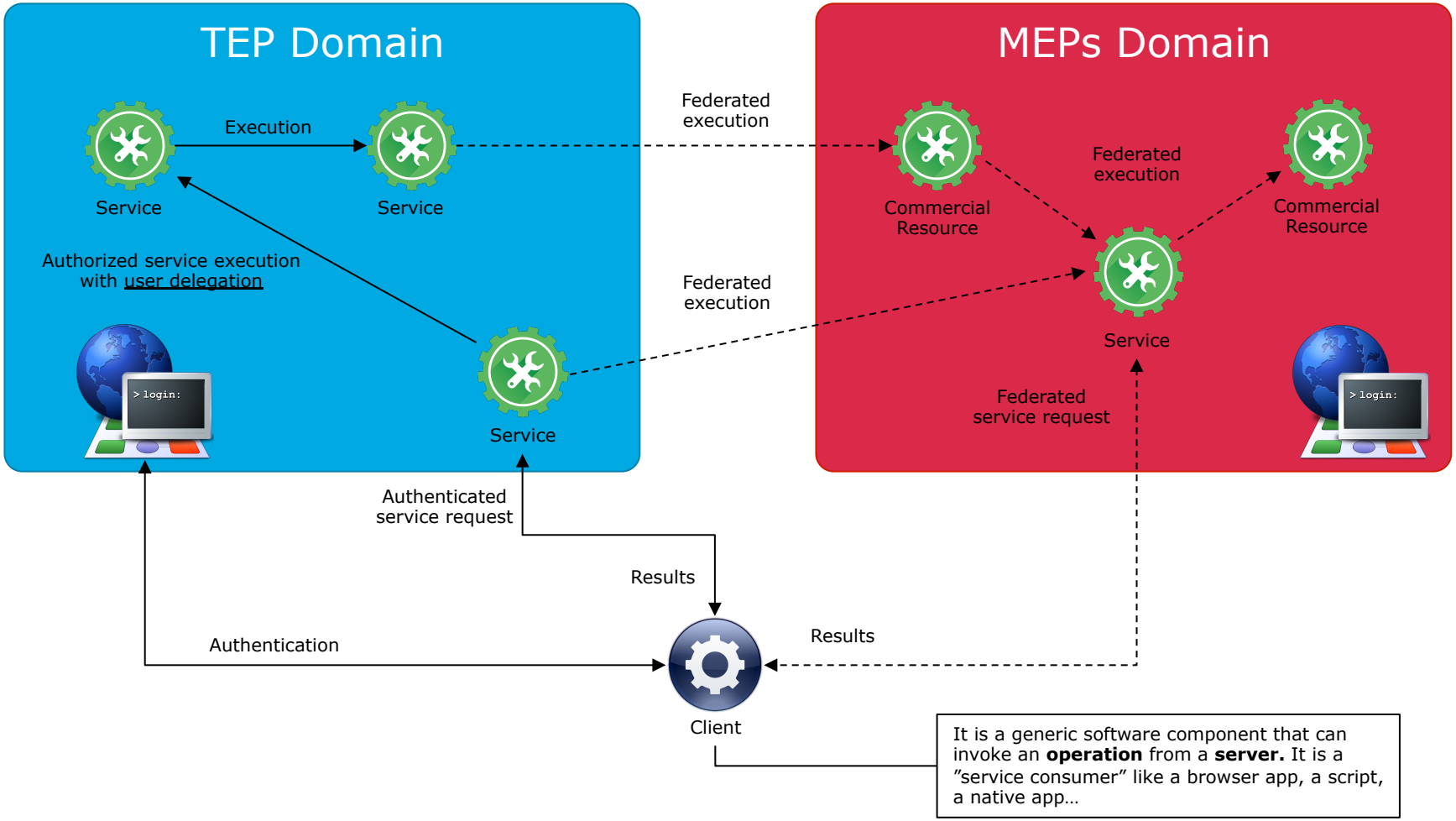
- The Exploitation Platform, as a distributed/federated service, needs to be able to:
  - Support general authentication mechanism
  - Allow authenticated users to access the services in a ”consumer to business - C2B” manner
  - Support user’s service request execution according to the rights derived from a chained/distributed authorisation process and independently from the domain the user’s digital identity belongs to
  - Allow authorized users to submit service requests involving several chained/distributed services (like Mission Exploitation Platforms - MEPs - or commercial providers) in a ”business to business – B2B” manner even crossing the boundaries of the user’s Organization domain
  - Access resources on behalf of the user (including delegation)

- Standards and technologies: WS-Trust, WS-Security, SAML, (OpenID Connect, Oauth2, x509 certificates, kerberos, …), XACML, geoXACML

Accounting

- Definition: *"Accounting is the systematic and comprehensive measurement of the resources a user consumes during access"*
- The Exploitation platform needs to be able to:
  - Provide all the (expected) measures about the resources consumption related to the execution of an authorized user's request
  - Implement accounting mechanisms for different kind of needs like users' session statistics, general usage information, auditing, billing, …
  - Use auditing measure for implementing revenue-share requirements of commercial providers involved in the process
- Standards and technologies: No actual standards, APEL solution (EGI, Indigo)

Federated End-to-end use case for Thematic Exploitation Platform (1)



Federated End-to-end use case for Thematic Exploitation Platform (2)

- Involved Services and Resources collect accounting information that can be elaborated locally and at end-to-end level
- Services can act on behalf of the user (delegation mechanism)
- The user does not need to maintain his login session during the workflow execution
- ESA: Currently available a local STS implementation for TEPs
- ESA: Ongoing activity with GARR for the provisioning of a Federated access to Sentinel-2 data (for selected users) in eduGAIN via IPT Poland infrastructure
- Other initiatives: Indigo data cloud implementation of interoperable federated cloud services (TRL to be checked, verified)

Possible workplan

Priority	
High	• Various pathfinder projects (Sentinel-2 federated data provisioning, pay-per-use services) • STS solutions for TEP
Medium	• Evolution of existing MultiMission and CDS User management infrastructures towards federation • Mainstreaming current implementation towards best practices in IT
Low	• Research into accounting solutions • Compatibility with current industrial best practices in addition to the research community/academia/government

QUESTIONS?