

EOEPCA Phi-Week event

User Management:
Authentication, Authorisation, Accounting

Overview of User Management

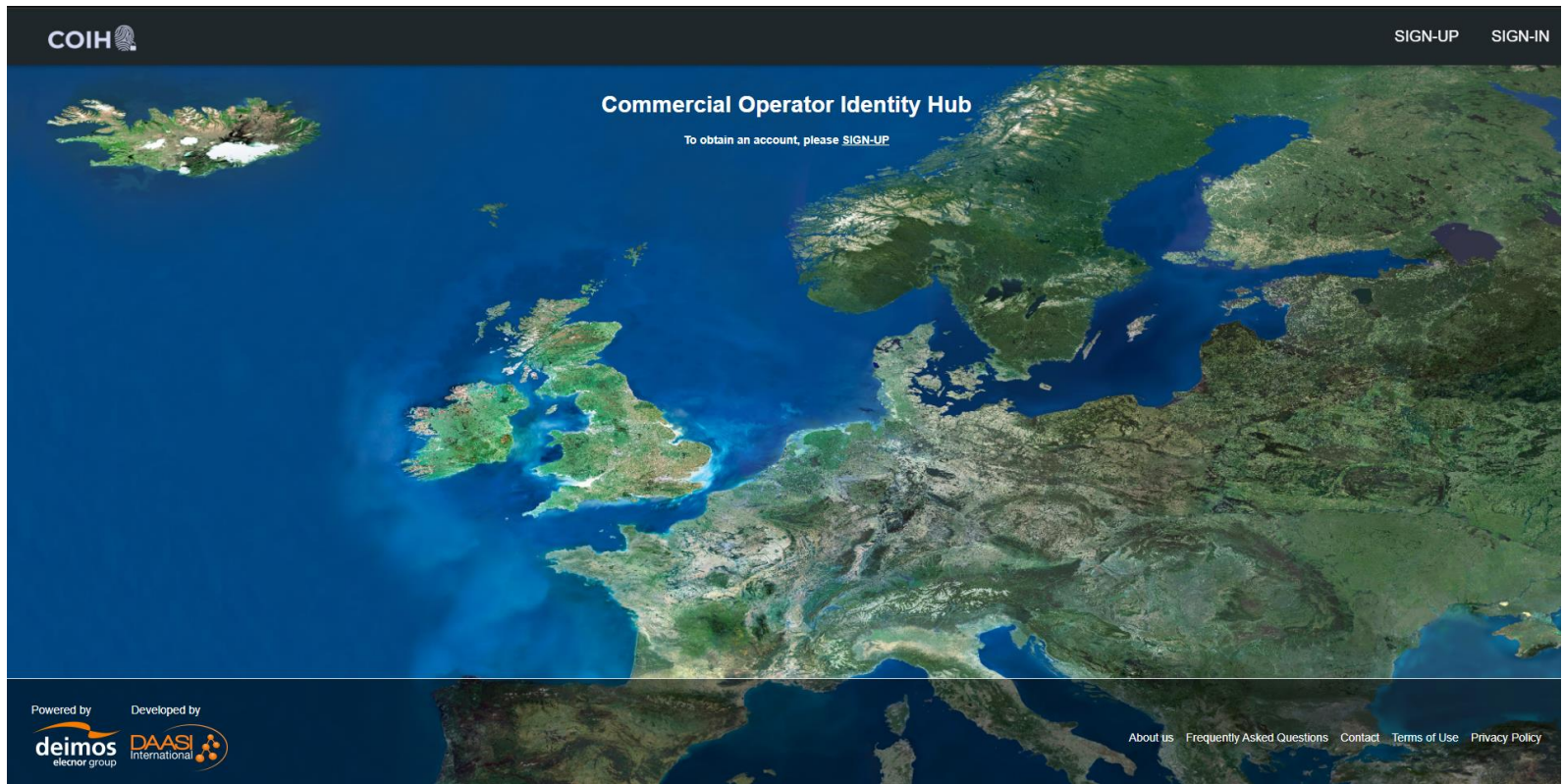
- To provide an easy-to-use Identity Management system
- To provide Single Sign-On facilities across federated (common) systems
- To ensure Attribute Based Access Control, via usage of access policies, Authorization and Authentication
- User Profiles for licensing management

Overview of User Management

Main concepts to keep in mind:

- **Commercial Operator Identity Hub (COIH): serves as an external identity provider. It is a deployed, free service. Reference at <https://coih.org/>**
- Triple-A: A deployed, paid service, that provides Federated Identity Management functions over registered services (i.e. client, applications) and resources. Commercial contact point david.garcia.perez@deimos.com.pt
- EOEPKA: technology development and architectural demonstration

Overview of User Management



Commercial Operator Identity Hub (COIH: <https://coih.org/>)

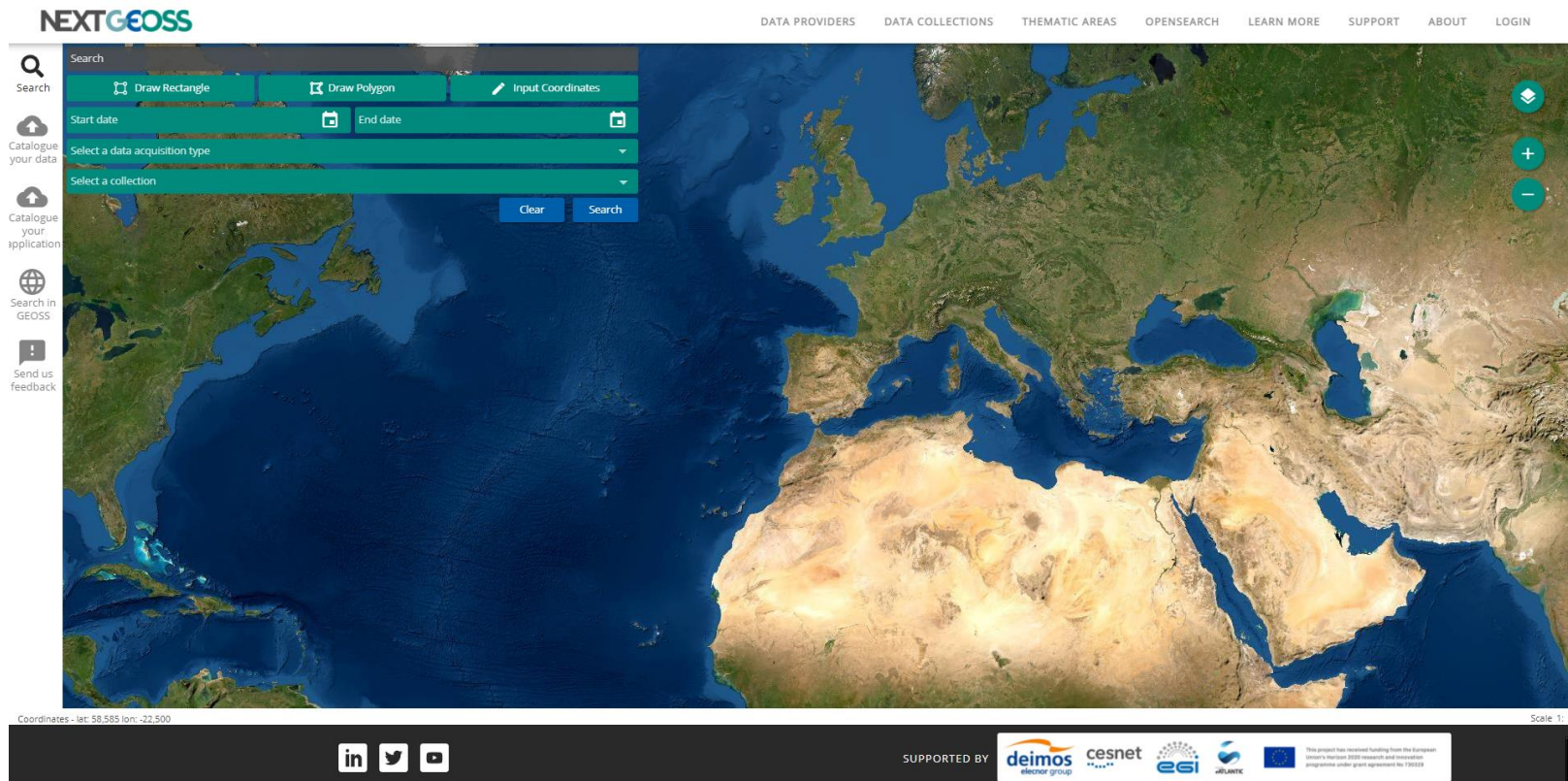
Trademarks "Elecnor Deimos", "Deimos" and the logo of Deimos (Elecnor Group) encompass Elecnor Group's companies of Aerospace, Technology and Information Systems: **Deimos Space S.L.U.** (Tres Cantos, Madrid, Spain), **Deimos Engineering and Systems S.L.U.** (Puertollano, Ciudad Real, Spain), **Deimos Engenharia S.A.** (Lisbon, Portugal), **Deimos Space UK Ltd.** (Harwell, Oxford, United Kingdom), **Deimos Space S.R.L.** (Bucharest, Romania).

Overview of User Management

Main concepts to keep in mind:

- Commercial Operator Identity Hub (COIH): serves as an external identity provider. It is a deployed, free service. Reference at <https://coih.org/>
- **Triple-A: A deployed, paid service, that provides Federated Identity Management functions over registered services (i.e. client, applications) and resources. Commercial contact point david.garcia.perez@deimos.com.pt**
- EOEPKA: technology development and architectural demonstration

Overview of User Management



NextGEOSS Catalogue (backed by Triple-A)

Trademarks "Elecnor Deimos", "Deimos" and the logo of **Deimos (Elecnor Group)** encompass Elecnor Group's companies of Aerospace, Technology and Information Systems: **Deimos Space S.L.U.** (Tres Cantos, Madrid, Spain), **Deimos Engineering and Systems S.L.U.** (Puertollano, Ciudad Real, Spain), **Deimos Engenharia S.A.** (Lisbon, Portugal), **Deimos Space UK Ltd.** (Harwell, Oxford, United Kingdom), **Deimos Space S.R.L.** (Bucharest, Romania).

Overview of User Management

Main concepts to keep in mind:

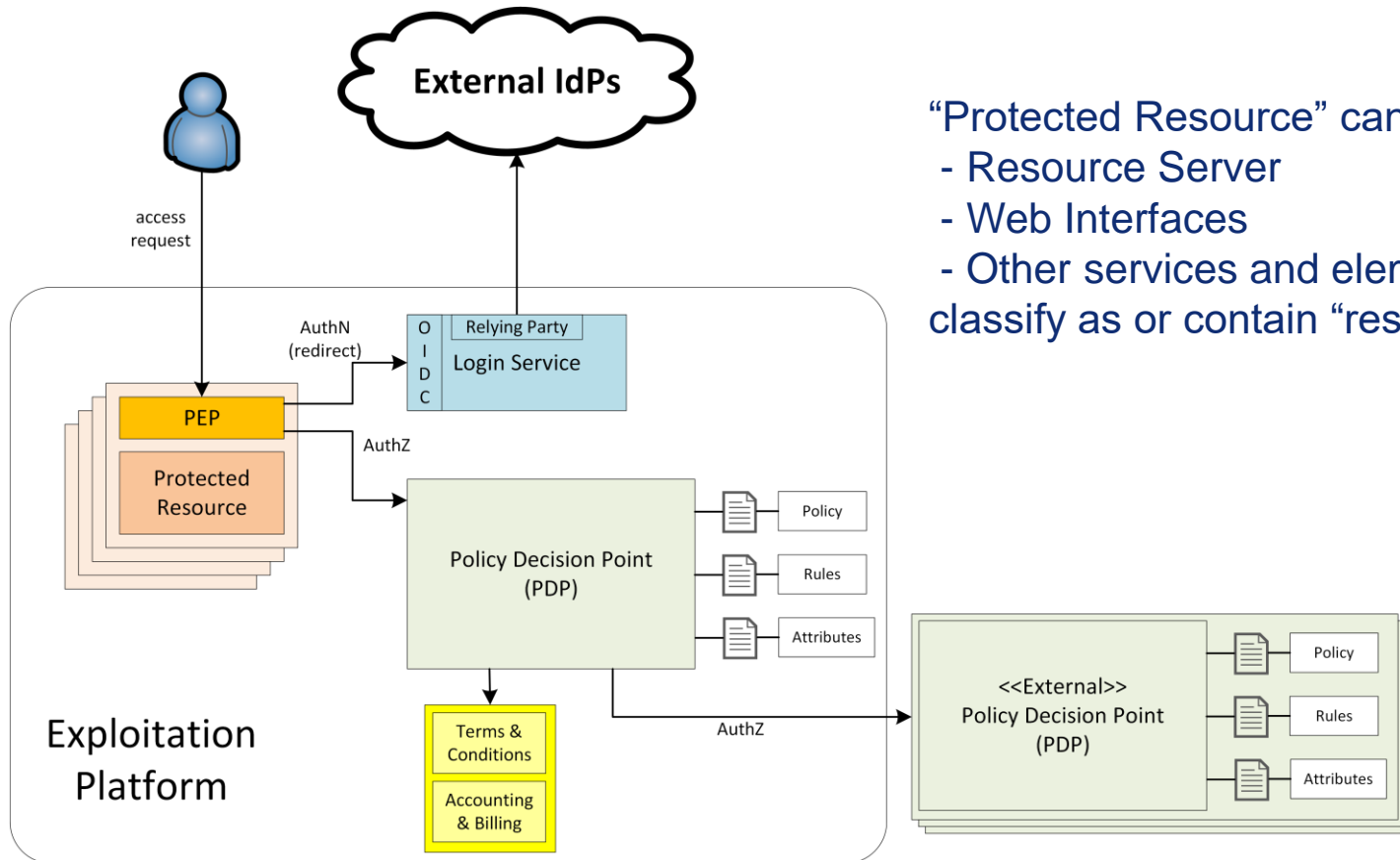
- Commercial Operator Identity Hub (COIH): serves as an external identity provider. It is a deployed, free service. Reference at <https://coih.org/>
- Triple-A: A deployed, paid service, that provides Federated Identity Management functions over registered services (i.e. client, applications) and resources. Commercial contact point david.garcia.perez@deimos.com.pt
- **EOEPCA: technology development and architectural demonstration**

Overview of User Management

- Current version composed of 4 Building Blocks:
 - Login Service: Identity repository and management, Authentication point
 - User Profile: user and licensing management
 - Policy Enforcement Point: Entry point to solution, can interface with different proxy solutions (one is provided by default) and allows for resource management by Resource Servers
 - Policy Decision Point: Authorization point, can be externally delegated

Trademarks "Elecnor Deimos", "Deimos" and the logo of Deimos (Elecnor Group) encompass Elecnor Group's companies of Aerospace, Technology and Information Systems: **Deimos Space S.L.U.** (Tres Cantos, Madrid, Spain), **Deimos Engineering and Systems S.L.U.** (Puertollano, Ciudad Real, Spain), **Deimos Engenharia S.A.** (Lisbon, Portugal), **Deimos Space UK Ltd.** (Harwell, Oxford, United Kingdom), **Deimos Space S.R.L.** (Bucharest, Romania).

Overview of User Management



“Protected Resource” can be:

- Resource Server
- Web Interfaces
- Other services and elements that classify as or contain “resources”

Login Service use cases

Resource registration

- For access protection and control

Dynamic client registration

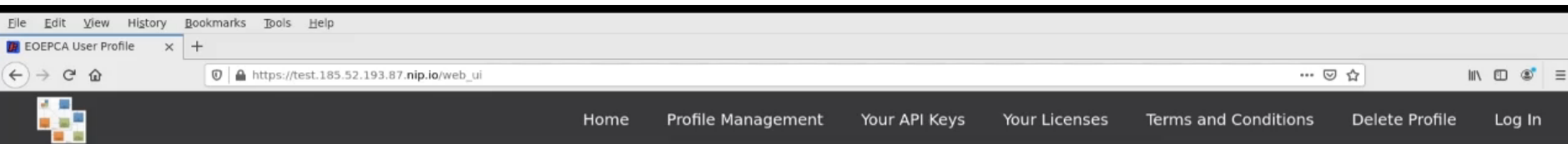
- For automation of platform deployment, using OAuth 2.0 standards

Propagation of User Identity by usage of JWT

Login Service use cases

Login with external IdP:

- Delegates user authentication on external Identity Providers



User Profile use cases

Interface for external IdP Logins

Profile edits

Account deletion

Policy Decision Point use cases

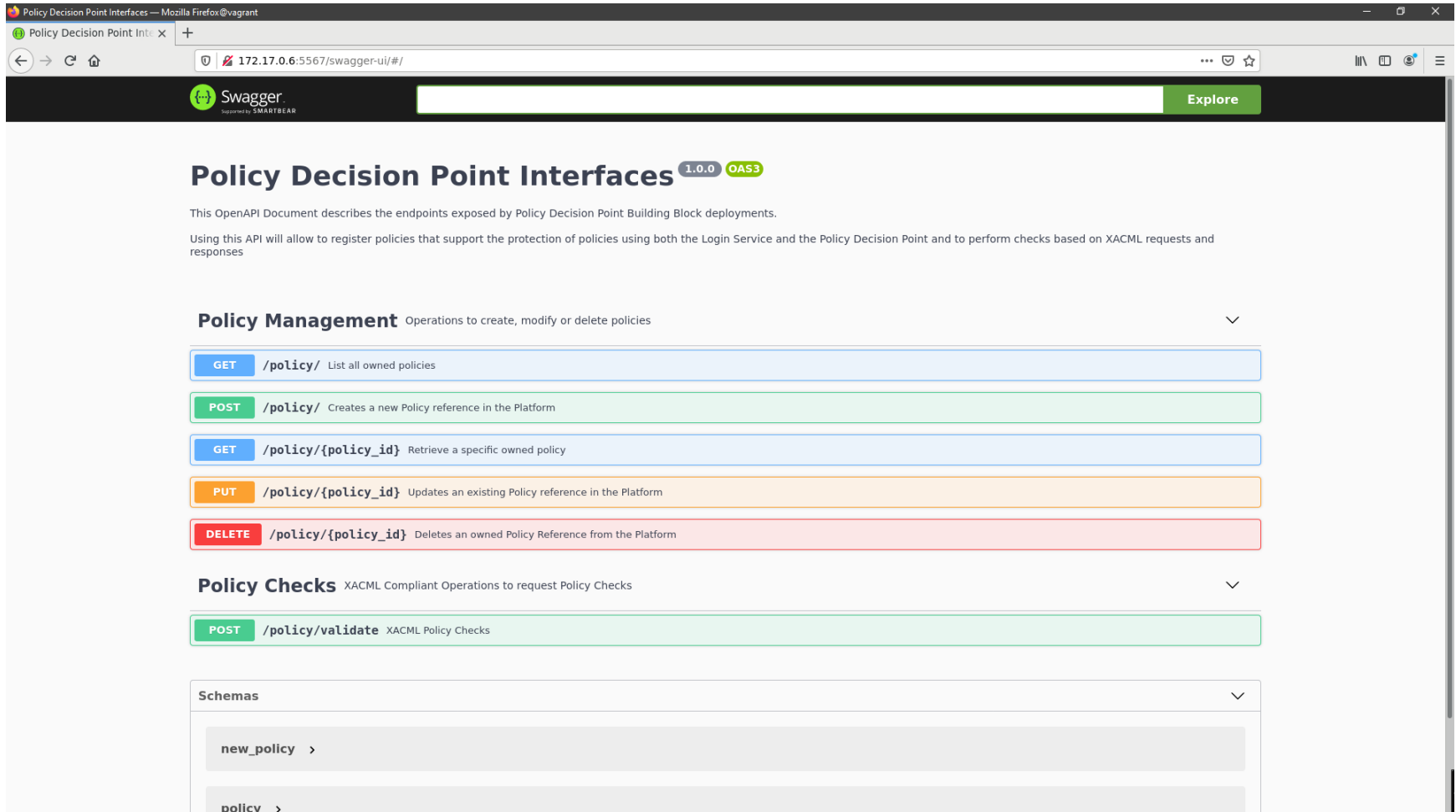
- Authorization decisions
- Policy CRUD operations
- Policy delegation to external PDP

Policy Enforcement Point use cases

- Reverse proxy functions (default)
- Traffic forwarding to Resource Server
- UMA 2.0 implementation
- Resource path lookup
- Resource CRUD operations

Policy Enforcement/Decision Point

- OpenAPI webpage



Policy Decision Point Interfaces — Mozilla Firefox@vagrant

Policy Decision Point Int... x +

172.17.0.6:5567/swagger-ui/#/ Explore

Policy Decision Point Interfaces ^{1.0.0} ^{OAS3}

This OpenAPI Document describes the endpoints exposed by Policy Decision Point Building Block deployments.

Using this API will allow to register policies that support the protection of policies using both the Login Service and the Policy Decision Point and to perform checks based on XACML requests and responses

Policy Management Operations to create, modify or delete policies

- GET** `/policy/` List all owned policies
- POST** `/policy/` Creates a new Policy reference in the Platform
- GET** `/policy/{policy_id}` Retrieve a specific owned policy
- PUT** `/policy/{policy_id}` Updates an existing Policy reference in the Platform
- DELETE** `/policy/{policy_id}` Deletes an owned Policy Reference from the Platform

Policy Checks XACML Compliant Operations to request Policy Checks

- POST** `/policy/validate` XACML Policy Checks

Schemas

- `new_policy` >
- `policy` >

Overview of User Management

- Planned Features:
 - Accounting & Billing services
 - Pricing Engine: rates & prices calculations, can be called as a consultant for the PDP on Authorization phase, helper for Billing Service
 - Billing Service: receives and processes Billing Events from external components (using Pricing Engine), establishes associations with Billing Identities, generates Billing Reports
 - License Manager: link between license constraints and end-users, constraint verifications when paired with the PDP



Thank you

www.elecnor-deimos.com

Trademarks "**Elecnor Deimos**", "**Deimos**" and the logo of **Deimos (Elecnor Group)** encompass Elecnor Group's companies of Aerospace, Technology and Information Systems: **Deimos Space S.L.U.** (Tres Cantos, Madrid, Spain), **Deimos Engineering and Systems S.L.U.** (Puertollano, Ciudad Real, Spain), **Deimos Engenharia S.A.** (Lisbon, Portugal), **Deimos Space UK Ltd.** (Harwell, Oxford, United Kingdom), **Deimos Space S.R.L.** (Bucharest, Romania).