Destination Earth Core Service Platform

DESP Integration procedure IAM and Service registry

Destination Earth Funded by the European Union Implemented by ECMWF esa EUMETSAT

Reference: DEST-SRCO-TN-2300361
Date: 15/09/2023
Version:1.0

Role/Title	Name	Signature	Date
Author	DESP Team		15/09/2023
Verified	DESP Service Manager		15/09/2023
Approved	DESP Contract Manager		15/09/2023

Change register

Version/Rev.	Date	Change	Reason
1.0	15/09/2023		First release of the document

Table of Contents

Index of Figures

1. Introduction

1.1 Scope

This document describes the procedure to integrate a Service with the DESP IAM Service and Service Registry for the "*Destination Earth – DestinE Core Service Platform Framework – Platform & Data Management Services*".

1.2 Purpose

The purpose of this document is to provide a clear and comprehensive step-by-step procedure for

- The integration of an external Service with the DESP IAM Service and
- The publication of an external Service in the Service Registry.

1.3 Applicable Documents

Ref.	Title	Reference and Version
AD-1	[DP-SOW] Statement of Work - Destination Earth – Destine Core Service Platform Framework – Platform & Data Management Services	ESA-EOPG-EOPGD-SOW-10, v 1.0
AD-2	[AD-DSP-TSR] DESP Framework – Platform & Data Management Services – Technical and Service Requirements	ESA-EOPG-EOPGD-RS-10, v1.0
AD-3	[AD-DDL-DP] DestinE – System Framework – Data Portfolio	EUM/TSS/DOC/22/1279455, v1G, 09/09/2022
AD-4	[AD-DSP-SR] DESP Framework – Platform & Data Management Services – Security Requirements	ESA-ESO-SSRS-2022-0111, v1.0
AD-5	Space engineering – Software	ECSS-E-ST-40C, 06/03/2009

1.4 Reference Documents

Ref.	Title	Reference and Version
RD-1.	DEST-SRCO-TN-2300330 - IAM Service Overview	0.6
RD-2.	DEST-SRCO-TN-2300330 - DESP Operations Concept	0.3
RD-3.	DESP Onboarding Governance and Process	1.3
RD-4.	Keycloak	https://www.keycloak.org/

RD-5.	Configuration of client_id and client_secret in a Service.	https://www.keycloak.org/docs/22.0.3/securing_apps/
RD-6.	Keycloak Client Role management	https://www.keycloak.org/docs/latest/server_admin/#con-client-roles_server_administration_guide

1.5 Acronyms and Abbreviations

Acronym	Definition
AD	Applicable Document
API	Application Programming Interface
ECSS	European Cooperation for Space Standardization
ESA	European Space Agency
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
RD	Reference Document
SOW	Statement of Work

2. Actors

In this section will follow a list and a brief description of the involved actors. For more information, please refer to [RD-1].

2.1 Service Provider

A Service Provider is a third-party entity that wants to expose its service through the DESP Platform to DESP Users.

As per [RD-2], the group of Service Providers is composed of:

- DESP Core Service Providers providing the DESP Registered Services.
- DESP Framework Service Providers providing DESP Registered Services to offer applications and algorithms.

2.2 Service Desk

The Service Desk acts as the primary contact point for service requests, User requests and issues reporting. It offers various communication channels and serves as the initiator for all established and standard procedures, evaluating additionally the custom ones. Specially, it leads the user feedback and satisfaction analysis process.

It is supported by a ticketing System, and it may trigger internal procedures.

2.3 IAM Admin

It is an Administrator in charge of operating the DESP components included the Identity and Access Management ones.

2.4 Decision Board

It is an entity in charge to evaluate decisions about particular User and Service requests. It is involved when the existing procedures need its intervention or in case of issues.

3. Components

3.1 IAM

The core component of the Identity and Access Management service is Keycloak [RD-4].

3.2 Service Registry

A system dedicated to store and managing all the existing Services exploitable within DESP Platform. It can be used to discover existing Services and to follow the procedure to become a Registered Service Provider.

4. Integration Procedure

The overall integration procedure for a service provider willing to be onboarded in DESP is described in [RD-3]. The following sections depict the detailed procedure for the integration with the DESP IAM and Service Registry.

4.1 Pre-requirements

The Service Provider has passed Phase 1 "Service Onboard Request" and Phase 2 "Service Evaluation" and he is starting Phase 3 "Service Integration" as per [RD-3].

As result of the Phase 1 and 2 mentioned above, the Service Provider should have:

- A correctly configured (by the IAM Admin) IAM Account.
- An "onboarding" record in the Service Registry, representing the Service with the "onboarding" status set on "ongoing".
- A Price List table in the Service Registry related to Service available purchasable resources.

4.2 Step-by-step process

The Integration Procedure described below is part of the Onboarding Procedure Phase 3 ("Service Integration" as per [RD-3]).

After this event, the Service can be discovered and consumed by the DESP Users.

Here in below a table with detailed steps:

Step number	Step	Actor	Component	Description
1.	Create Client and configuration.	IAM Admin	Keycloak	The IAM Admin enable permissions for the Service Provider to configure a Client for his/her service in the IAM.
2.	Send *client_id* and *client_secret* to Service Provider.	IAM Admin	email with encrypted content (TBD)	The IAM Admin Send *client_id* and *client_secret* to Service Provider.
3.	Configure *client_id* and *client_secret* in its own Service.	Service Provider	Registered Service software component	Please see Keycloak documentation [RD-5] for a full description of the configuration steps.
4.	Create Specific Service Provider Role.	IAM Admin	Keycloak	The Role shall consent the Service Provider to autonomously manage its assigned Client (Policy, Permissions, Realm-Management Client Roles).
5.	Assign Specific Service Provider Role to the requester DESP User.	IAM Admin	Keycloak	The IAM Admin assigns the role of Service Provider to the DESP

				User who is following this process.
6.	Communicate to the Service Provider the availability of the Client-Role Management function.	IAM Admin	email	The IAM Admin informs the Service Provider of his/her new role.
7.	Client-Role Management – assignment to Users.	Service Provider	Keycloak	See section 4.2.1
8.	*The process continues with further Integration Steps as Service Testing and Service Operational Deployment i.e. from step 3.2.3 to 3.3.3 of [RD-3].*			
9.	Service Publication	DESP Administrator	Service Registry	At the end of the Phase 3, the “onboarding” record of the Service Provider in the Service Registry is set to “onboarding complete” status by the DESP Administrator and the Service is visible into the Service registry.

4.2.1 Client-Role Management

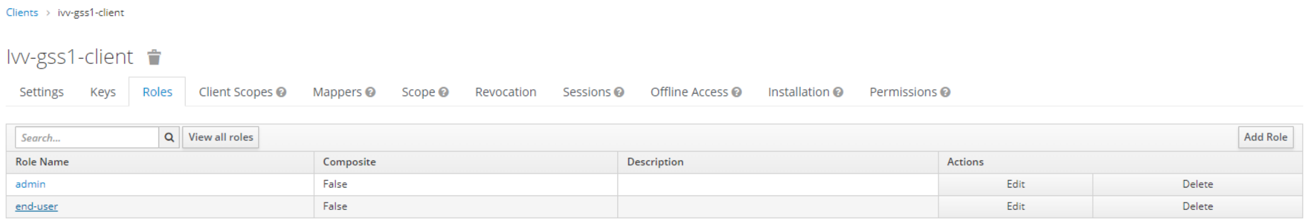
The implementation of the authorization function within a Service is managed through the definition of user roles. The Service Provider shall implement service roles by creating them on the IAM as Client-Roles. Please note that the full documentation on the steps to be performed is available online [RD-6], however the following subsections depict report a summary to facilitate the job of the Service provider.

4.2.1.1 Procedure

Client-Role creation

1) Access the 'Clients' section and select the Client ID received by the IAM Admin.
2) Access the 'Roles' tab and click on 'Add Role'.
3) Insert a name and description. At the end of the insertion, click on 'Save'.

   Please note that the 'Description' field is optional.

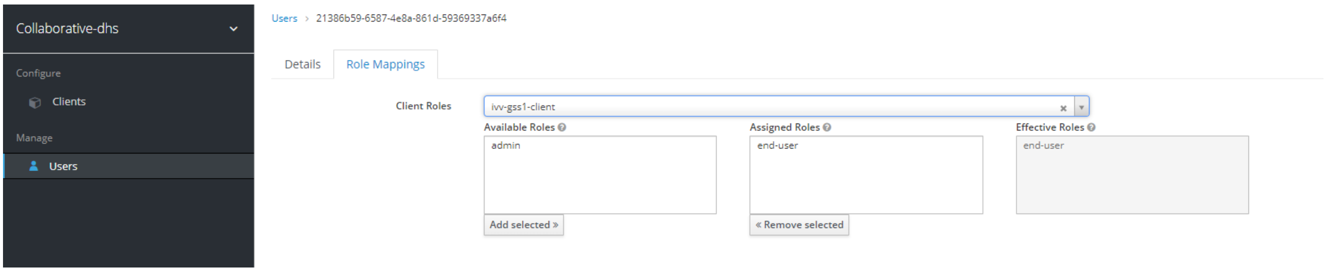


Role Name	Composite	Description	Actions	
admin	False		Edit	Delete
end-user	False		Edit	Delete

Figure 1: Client-Roles creation

Assign Roles to User

1) Access the 'Users' section and search for the user on which assign the selected roles.
2) Click on the resulting User ID.
3) Access the 'Role Mappings' tab and select the Client ID received by the IAM Admin in the 'Client Roles' dropdown menu.
4) Click on the Roles available in the 'Available Roles' list and assign them to the user clicking the 'Add Selected' button.



Client Roles: ivv-gss1-client

Available Roles: admin

Assigned Roles: end-user

Effective Roles: end-user

Figure 2: Client-Roles assignment

4.2.1.2 Best Practice

It is recommended to establish a predefined usage limit (default quotas) for existing Service users. Please avoid requiring the functional activation of client-role assignments, as it may entail a substantial operational effort.

<End of the document>