Destination Earth Core Service Platform

DESP Operations Concept Document

Reference: DEST-SRCO-TN-2300330
Date: 30/01/2024
Version: 1.3

Role/Title	Name	Signature	Date
Author	DESP Design Team		30/01/2024
Verified	DESP Service Manager		30/01/2024
Approved	DESP Contract Manager		30/01/2024

Change register

Version/Rev.	Date	Change	Reason
0.1	13/07/2023		First DRAFT version
0.2	04/09/2023		Second DRAFT version
0.3	08/09/2023		Third DRAFT version
0.4	19/09/2023		Fourth DRAFT version
0.5	25/09/2023		Fifth DRAFT version
1.0	29/09/2023		First Version of the document
1.1	13/10/2023	Added reference to OMP. Updated Section 2.2.3, 3.1.1, 3.1.2, 3.1.4, 3.1.5, 3.2.1, 3.2.4, 3.3.1, 3.3.2, 3.4.1.14, 3.5.2, 3.5.9, 3.7.2, 3.11.1	Updated version
1.2	18/01/2024	Updated Sections: 2.2.3, 3.1.1, 3.1.2, 3.1.4, 3.1.5, 3.2.1, 3.2.4, 3.3.1, 3.3.2, 3.4.14, 3.7.1, 3.7.1.1, 3.7.1.2, 3.7.2, 3.9.1, 3.9.2, 3.9.3, 3.9.4, 3.9.5. All subsections of Section 3.8 and 3.11. Added Annex 2.	Updated version DCMS and Traceability Service new scenarios
1.3	30/01/2024	Updated AD-8 and its cross-references	Updated Reference Document

Table of Contents

Index of Figures

Index of Tables

1. Introduction

1.1 Scope

This document provides the Operations Concept for the "*Destination Earth – DestinE Core Service Platform Framework – Platform & Data Management Services*".

1.2 Purpose

The purpose of this document is to state the operational concepts applicable to DESP, to provide the associated operational scenarios and the traceability with the SOW requirements. It is intended to constitute the highest-level reference for DESP validation and operations.

The purpose of the operational concept is to provide a full picture of how DESP will be used and operated in a nominal context. These concepts, and the operational scenarios which describe them, are meant to define the optimal operational usage of the system and thus demonstrate how it can be utilized to best accomplish service tasks and satisfy operational target and constraints.

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
AD-6	[DSP-PDM-ICD] DESP System Design Document and Master ICD	DEST-SRCO-DD-2300317, v1.1
AD-7	[DSP-PDM-SDP] DESP Framework – Platform and Data Management - Services & Data Portfolio	DEST-SRCO-TN-2300323, v1.0
AD-8	[DSP-USR-SDP] DESP Services Portfolio	DEST-SRCO-TN-2300324, v1.0
AD-9	DESTINE ACCESS – GOVERNANCE GUIDELINES	ESA-DEST-EOP-GD-TN-02, 0.2, 30/06/2023

1.4 Reference Documents

Ref.	Title	Reference and Version
RD-1.	DESP Service Management Plan	DEST-SRCO-PL-2300318, v1.1

RD-2.	DESP System Verification and Validation Plan	DEST-SRCO-PL-2300328, v1.0
RD-3.	DESP Onboarding Governance and Process	DEST-SRCO-PR-2300339
RD-4.	DESP Integration procedure IAM Service and Service Registry	DEST-SRCO-TN-2300361
RD-5.	DESP Integration Procedure: Runtime Platform	DEST-SRCO-TN-2300355
RD-6.	DESP Communication Plan	DEST-SRCO-PL-2300378, v1.0
RD-7.	Identity and Access Management Service Overview	DEST-SRCO-TN-2300330_Annex 1
RD-8.	Destination Earth visual guidelines	DEUC-TN-23-07
RD-9.	Evolution Plan - Schedule	DEST-SRCO-PL-2300322
RD-10.	OVH Public Cloud APIs	https://api.ovh.com/console/#/
RD-11.	OpenSearch API	https://www.ogc.org/standard/opensearch/
RD-12.	STAC API	https://stacspec.org/en
RD-13.	WMS	https://www.ogc.org/standard/wms/
RD-14.	WCS2	https://www.ogc.org/standard/wcs/
RD-15.	S3 API	https://docs.aws.amazon.com/AmazonS3/latest/API/
RD-16.	Security Governance Management Plan	DEST-SRCO-PL-2300364
RD-17.	DESP Anomaly Management Procedures	DEST-SRCO-PR-2300315
RD-18.	DESP IAM Service, Accounting Service and Service Registry ICD	DEST-SRCO-IF-2300371
RD-19.	Operations Management Plan	DEST-SRCO-PL-2300395
RD-20.	Information Dissemination & Onboarding Support Management Plan	DEST-SRCO-PL-2300397

RD-21.	DESP Data Visualization Service ICD	DEST-SRCO-IF-2300370

1.5 Acronyms and Abbreviations

Acronym	Definition
AD	Applicable Document
c.e.c.	current economic conditions
COG	Cloud Optimised GeoTiff
DCU	DestinE Credit Unit
DEDL	DestinE Data Lake
DESP	DestinE Core Service Platform
DTAC	DestinE Terms and Conditions
DTE	Digital Twin Earth
ECMWF	European Center Medium Weather Forecast
ECSS	European Cooperation for Space Standardization
ESA	European Space Agency
FIP	Federated Identity Providers
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol Secure
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICD	Interface Control Document
LoL	Limit of Liability
OCD	Operations Concept Document
OS	Operational Scenarios
RD	Reference Document
SDD	System Design Document
SOW	Statement of Work
SSO	Single Sign On

2. Operations Concept overview

The Operational Concept Document (OCD) defines:

- the way (how) the system will be used to accomplish the objectives stated in the system requirements and associated documentation
- the system users categories
- any critical, top-level performance requirements or objectives (stated either qualitatively or quantitatively) and system rationale.

Other objectives are:

- To provide traceability between operational needs and the captured source requirements.
- To establish a basis for requirements to support the system over its life, such as personnel requirements, support requirements, etc.
- To establish a basis for end-to-end validation planning, system-level integration requirements, and any requirements for environmental simulators.
- To generate operational analysis models to test the validity of external interfaces between the system and its environment, including interactions with external systems.

2.1 General Concepts

General concepts on which the DestinE Core Service Platform are listed and described in Annex 1 [RD-7]. We report them here below for sake of clarity.

2.1.1 DestinE Platform Configuration Board

Serco operates the DestinE Platform Configuration Board to coordinate with its partners the platform operational configuration. In particular, the board shall report to the DestinE Joint Configuration & Control Board on DestinE services configuration and consumptions and may issue recommendations for the management of DestinE services. The board constituted by industry representatives of the platform with the authority to decide on implementation measures shall ensure development towards a sustainable ecosystem of services and users.

The DestinE Platform Configuration Board is the book captain of the Code of Conduct.

2.1.2 SSO

The IAM Service provides the Single Sign On feature. Users can access all the authorised DESP Services by a single log-in without the need to re-authenticate to access each service (and remain logged-in DESP) until they perform the log-out scenario (see Section 3.4.6) or the user Authentication Token expires.

The IAM solution is based on Keycloak software, which is an identity and access management solution widely adopted, strongly supported by the community and open source.

The Keycloak software is, on top, extended by an Identity For Earth Observation Product developed by Deimos called identity4EO.

2.1.3 Authentication Tokens

The Authentication Token identifies the user after a successful log-in. It is generated by the IAM Service via the Token Issuer endpoint and it contains all relevant information about the user such as Roles, Groups and Attributes.

This information is used by the Registered Services to properly assign specific access capabilities, quotas, roles and allowed behaviours.

The Authentication Token has a validity defined at the service level. After this period an Authentication Token will be considered invalid and not usable through the DESP Services. A valid token near to the expiration date can be refreshed by appropriate interactions with the Token Issuer endpoint provided by the DESP IAM Service.

Each communication within the platform will happen by using secure encrypted calls based on the HTTPS protocol. The IAM Service supports open Authentication protocol standards such as OAuth 2.0, OpenID Connect and SAML 2.0.

2.1.4 Security

Thales Alenia Spaces (TAS) is responsible for the platform security (see [AD-6]) as part of the DESP Consortium. It will drive the security activities based on the global Thales Alenia Space Cybersecurity scheme. This scheme is derived from the ISO27001. OVH infrastructure provides several solutions to recognize malicious activities on the system and block them. Security by design principles are also adopted for the platform to properly mitigate the risks associated with such a large system.

The DestinE Platform Configuration Board has the responsibility of restricting, rejecting or revoking access to DestinE ecosystem to users or organisations in case of:

- an unfair use of the system, potentially impacting the performance of DestinE services, or
- people or organisations being blacklisted by the European Commission or other UN-like organization.

2.1.5 GDPR

All Data related to DESP and managed by Serco are under Serco’s "Data Protection Framework" compliant with GDPR.

2.1.6 DESP Tenant

A DESP Tenant is a logic container of DESP resources/services. This container is managed by a Tenant Admin and its resources/services can be consumed by its Tenant Members.

2.1.7 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.

2.1.8 DESP Registered Service

A DESP Registered Service is listed in the DESP registry of services, and available with free access to authorized DESP registered users.

A new registered service has, as a minimum, the following main interfaces:

- It is integrated in DESP following the approval of the Onboarding Procedure.
- Access to all authorised DESP Registered Services, based on the same digital identity, is granted by DESP IAM Service.
- It is catalogued in the DESP Service Registry.
- [optional] It can be deployed onto the Runtime Platform or outside it.
- [optional] It can be integrated with the Accounting Service, if agreed.
- [optional] It can be integrated with the Service Monitoring Dashboard Services, if agreed.

For what concerns the DESP Registered Service belonging to the Consortium or the new ones which have been successfully onboarded.

- Footer complies with Destination Earth visual guidelines stated by ESA (refer to [RD-8]) in terms of logos; colour follows the hex code #0D1527, moreover it reports legal information as DESP Code of Conduct (DCOC), Terms and Conditions and Privacy Policies.
- Header colour follows the hex code #0D1527, the DESP logo is present and the Login button is in the right part of the header. Other panels relevant to the service are reported.
- Two dedicated buttons redirect to the Support Area and User Guides Area of the DESP Web Portal.

2.1.9 Federated Identity Provider

A Federated Identity Provider (example: a university) fulfils the following requirements:

- Federation does not follow the Onboarding Procedure but a direct agreement with ESA/Serco.
- The users of the Federated Identity Provider can access DESP Platform via their existing Federated Identity Provider identity as Federated Users
- Its IAM Service is linked to DESP IAM Service.
- It is catalogued in the DESP Web Portal in a dedicated section listing DESP Identity Providers.
- It is not deployed onto the Runtime Platform.
- It is not integrated with the Accounting Service.
- It is not integrated with the Service Monitoring Dashboard Services.

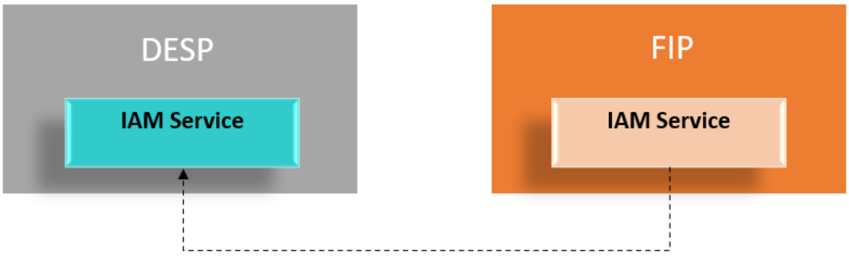


Figure 1: Federated Identity Providers

2.1.10 Federated Service

A Federated Service (example: OVH, see [AD-6]) complies with the following requirements:

- It follows a "Federation Procedure" (TBW)
- The users of the DESP Platform can access the Federated Service via their existing DESP identity
- Its IAM Service is linked to DESP IAM Service.
- It is integrated with the Accounting Service.
- It is catalogued in the DESP Service Registry.
- It is not deployed onto the Runtime Platform.
- It is not integrated with the Service Monitoring Dashboard Services.

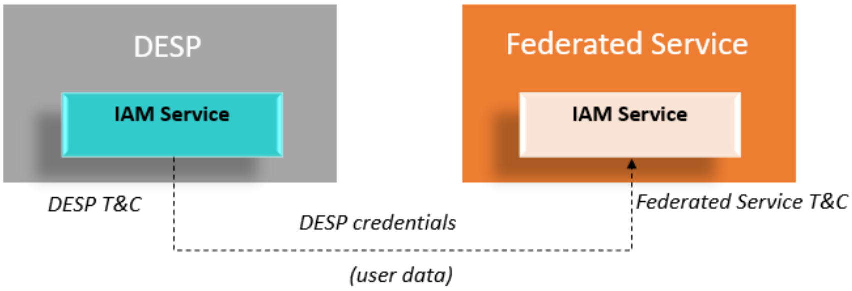


Figure 2: Federated Service

2.1.11 External Federated Service

An external Federated Service (example: CSC Dataspace, see [AD-6]) is defined by the following points:

- It follows a "Federation Procedure" (TBW)
- The users of the External Federated Service can access DESP Platform via their existing EFS identity as Federated Users

- The users of the DESP Platform can access the External Federated Service via their existing DESP identity
- Its IAM Service is linked to DESP IAM Service.
- It is not integrated with the Accounting Service.
- It is catalogued in the DESP Service Registry.
- It is not deployed onto the Runtime Platform.
- It is not integrated with the Service Monitoring Dashboard Services.
- Legal aspect (need for upstream filtering) TBD

2.1.12 DCU

In order to support the end-to-end management of chained services and associated transparent cost management for the users, a DestinE Credit Unit (DCU) is introduced as a common service unit for all DESP Core Services.

Cost of 1 DCU in Euro at current economic conditions (2023) is 1 DCU = 100.00 Euro.

2.2 Actors

In this Section, the Actors identified in the framework of DESP and involved in the Operational Scenarios are described.

The different actors defined to describe the set of services and capabilities of the DestinE Core Service Platform are described in the following subsections. Please note that each identified actor can be matched with the user groups described in the SIMPL platform architecture (Table 1 in this Section). Serco intends to reuse the same definition coherently within its own federated services to offer a unique continuity of services to the users. Particular attention is being paid to the link with the infrastructure provider to enable seamless scalability through a unique continuum of operations.

In the following table the User Access Classes defined by the DestinE access governance are mapped with the platform actor’s categories and with the four actor groups identified within the SIMPL platform architecture.

Table 1: User Access Classes

User Access Class	Access Policy	SIMPL actor group	Identified Actors
General Public Access	Access is granted to any potential user with no need of registration in DESP.	End Users	Unregistered users
Registered General Public Access	Access is granted to any potential users after self-registration and acceptance of DESP CoC.		Standard Users

User Access Class	Access Policy	SIMPL actor group	Identified Actors
Tenant Access	Access is granted to users or entities representing a community, translating into a coherent usage of resources by its individual users. Tenancy-associated users are consuming a common set of resources and need to register at DESP through the Service Desk.	End Users	Tenant Admins & Tenant Members
Registered Public Authorities Access	Tenant type of access, granted to entities self-declared as acting on behalf of a European Public Authority and confirmed by DG-CNECT.	End Users	Tenant Admins
Partnerships Access	Tenant type of access, granted to entities participating in a project identified through a 3Es partnership agreement.	End Users	Tenant Admins
Use Cases Access	Tenant type of access, granted to entities participating in a 3Es selected use case.	End Users	Tenant Admins
Registered Service Access	Access is granted to users or entities operating DestinE registered services. This type of access shall be requested at DESP through the Service Desk.	Data Providers, Infrastructure Providers, Application Providers	Registered Service Providers
Federated Access	Access is granted to users registered and authenticated in external-to-DestinE ecosystems. The Federation needs to be recognized and approved by the high-level governance.	End users	Federated users
Development Access	Tenant type of access, granted to teams taking part of the implementation of DestinE ecosystem. This type of access is only applicable for limited period of time corresponding to the development duration.	Data Providers, Infrastructure Providers, Application Providers	Registered Service Provider

Please note that, actors are not constrained to a single role. When necessary, they have the flexibility to switch roles or even take on multiple roles simultaneously.

2.2.1 Unregistered users

Users who are not registered in the IAM Service and are therefore able to access a limited set of DESP functionalities.

2.2.2 Registered Users

Users registered in the IAM service, and categorized as follows.

2.2.2.1 Standard Users

DESP Standard Users have performed the self-registration and, with the Access Profile of Registered User, they consume resources and services.

2.2.2.2 Registered Service Providers

DESP Registered Services Providers, are the providers of services listed in the DESP Service Registry, and available to Standard Users. This group is composed of:

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

All Registered Services shall offer a free tier to all DestinE users corresponding to a *DestinE Usage Profile* describing the characteristics of the free access. The free tier can be enhanced through the direct procurement of resources directly to the service providers with a public offer documented in the Service Registry and characteristics referenced as *Service Usage Profile* (also referred as *Premium*).

Please note that the Platform Management Services offer only the *DestinE Usage Profile.*

2.2.2.3 Tenant Users

DESP Tenant Users are Standard Users with the assigned role of Tenant Admin or Tenant Member. They are providing and/or consuming resources/services within a DESP Tenant.

Tenant Finance Adminstrators

DESP Tenant Finance Administrators are able to manage the Tenant Payment Method (recharge Tenant Wallet or change to arrear Payment Method).

Tenant Technical Administrators

DESP Tenant Technical Administrators are able to manage a DESP Tenant in terms of purchase/dismiss resources to Tenant and assign/remove them to Tenant Members.

Tenant Members

DESP Tenant Members are Standard Users participating to a group of Users enabled to use Tenant resources/services.

2.2.3 DESP Administrators

A DESP Administrator is an actor in charge of managing the configuration elements of the DESP Core Services with administrative privileges. A DESP Administrator applies the identified operational routines and approved changes to the DESP IAM Service and other DESP components configurations.

The characters belonging to DESP Administrators are:

- The ones described in the Operations Management Plan [RD-19].
- the I&V Manager, responsible of the end-to-end validation of the DESP System.

- The ones traced in [RD-20] for what concerns the "User Community Management" service element.

2.2.4 Federated users

Federated Users are users whose personal data are provided by an external Identity Provider and may be propagated to the IAM Service upon acceptance of the User.

The Federated Users are enabled to access all the DESP features, functions and services freely accessible.

Note that the available User Attributes and personal data (shared by the User) may not be sufficient to allow the exploitation of every paid DESP features and Services. In these cases they shall be integrated with the needed attributes, data and Payment Method.

2.3 User Access Management Scenarios

The User Access Management Scenarios are intended to detail the interaction lifecycle within the DESP Ecosystem for each type of user. They are outlined in Annex 1 [RD-7].

3. Core Service Operational Scenarios

These set of Operational Scenarios are mapped with the functional area relevant to each DESP Services, described in the DESP SDD and Master ICD [AD-6].

3.1 Info Dissemination & Onboarding Support Service operational scenarios

3.1.1 Web Portal access and browsing

This scenario describes the content of DESP website (Web Portal) and how users can browse it.

DESP Web Portal content is organized into functional utility panels, such as:

- "Home" Page, accessible as the first displayed page, containing: a description of DESP, a summary of its latest news, a description of Destination Earth System and a link to its official website, and finally the logos of all the partners of DESP consortium.
- "About" panel, providing general information about DESP and DESP consortium's Partners, with the link to their websites.
- "Updates" panel, reporting categorized news (see Scenario in Section 3.1.5).
- "Onboarding" panel, where users can find a summary relevant the onboarding procedure, and a "Get on board" button redirecting to the entire procedure to become a DESP Service Provider and integrate *(onboard*) a new service in the DESP perimeter.
- "Service Registry" panel, with the link redirecting to the DESP Service Registry, which catalogues all DESP services and price lists.
- "Data Offer" panel, reporting the current and updated DESP data offer.
- The link to other DESP platforms or services, such as:
    - the link to the User community channels (forum, social media, and live messaging),
    - the "Support" form linking to the Service Desk email and the relevant issue tracking system (including support for DTE and DEDL)
- The "Log in/Register now" button, to access user individual profile information for the self-registration or login authorized panel of the Web Portal – besides all the DESP Services. The panel reports also the list of federated IdP.
- A Panel containing a button to access user individual profile information (redirecting to the User Account Management UI, where they can visualize and edit the relevant attributes, see Section 3.5.2) and a description of how and where DESP Standard Users can recharge their wallet and follow their invoices. This panel also contain the cost of 1 DCU in Euro at c.e.c.
- Newsletter registration and newsletter archive
- Footer complies with Destination Earth visual guidelines stated by ESA (refer to [RD-8]) in terms of logos; colour follows the hex code #0D1527, moreover it reports legal information as DESP Code of Conduct (DCOC), Terms and Conditions and Privacy Policies.

- Header colour follows the hex code #0D1527, the DESP logo is present and the Login button is at the right of the header.
- The DESP knowledge base, including user guides, technical guides, webinars, training or video tutorials, glossary, FAQs.
- The DESP Information Model description and visual representation.

Unregistered users can only:

- Follow DESP on social media
- Visualize "Home" page, "About" panel, "Updates" panel, "Onboarding" panel, "Service Registry" panel, "Data Offer" panel. In these cases, elements of the GUI are partially visible to unregistered users, to encourage users to register. After a configurable amount of time, a pop-up is showed reporting that to continue, registration is needed and it is free.

All the other functionalities require registration.

The subscription to the DESP newsletter is upon request for any user.

3.1.2 Web Portal content management

The process of managing web portal contents is to distribute information to the User Community so that to make it widely known and accessible. It involves the transmission, sharing, and delivery of information across the DESP Community Platforms to reach the intended recipients. The overall process ensures that relevant and accurate information reaches the user in a timely manner. It plays a crucial role in communication, education, awareness campaigns, public relations, and knowledge sharing within the community. Being informed indeed, users can register to events, webinars, and services, increasing the DESP audience share.

This scenario is played by the DESP Administrators (Information Team) under the supervision of:

- The Communication Manager, for any content update
- The Web portal Service champion, for managing contents on the DESP Web Portal
- The User community manager to approve all Knowledge base updates prior to release to the public.

The final objective of this scenario is to update the DESP Web Portal contents periodically according to the Communication Plan [RD-6] and Evolution Plan [RD-9] or after any request of update from ESA. In particular:

- The DESP Web Portal is updated in its interactive image gallery, promoting material such as articles, news, new partnerships and events. The update frequency of this information is defined in the Communication Plan [RD-6].
- Success user stories (onboardings), announcements of achievements, future evolutions according to Evolution Plan [RD-9].
- Training material, guides, webinars and other information in the Knowledge Base. The update frequency of this information is defined in the Service Management Plan.
- DESP information model, ensuring that its contents are updated and maintained all along the duration of the Contract.

Please note that Service documentation provided by Service Providers will be updated at each service upgrade: the relevant wiki - which includes user guides equipped with examples – will be updated by Information Team.

3.1.3 Community channels usage

Any user can access the DESP community channels and go through different types of interactions.

Updates

Users finds the “Updates” panel among the ones reported in the Header of the DESP Web Portal. It reports news of several categories, such as:

- DESP Services technical information (new features available to users, etc)
- DESP Services maintenance and operations information
- A new registered service in DESP Ecosystem and relevant update of service offer

- Events organized by DESP
- External events to which DESP participated.

Social media

The available social media channels (Facebook, X, LinkedIn), referenced in the Web Portal in the Footer and Header, disseminate:

- all the news showed in the "Updates" panel, and moreover:
- Post with educational purposes (e.g., a short tutorial about some DESP feature)
- Awareness building posts
- Posts encouraging User community engagement
- A new registered service in DESP Ecosystem and relevant update of service offer

Newsletter

Users find the "Newsletter" subscription button at the bottom of both "Home" and "Updates" panel. They are enabled to subscribe to the DESP newsletter, and thus receive emails periodically.

Community Forum

DESP registered users can read or create contents on the DESP Community Forum, i.e., post open questions in the Forum to which the Service Desk can respond in a way that is visible to all users. Furthermore, the forum allows users to reply to openly posted questions or to provide other kind of content useful for the user community.

3.1.4 Community channels management

DESP community channels are managed by User Community Manager and the Communication manager and kept updated by the Information Team.

Updates

The Communication Manager may receive hints and elements to prepare News from different actors (Service Manager, User community manager, Integration Manager, Business Manager). He/she is responsible for providing content to the Information Team, who will publish it.

Social Media

The publication of a post on the social media channels can be triggered by:

- The Communication manager, in the Communication plan defines posts messages and frequency of information to be shared with all community members related to news and major achievements, adding links to imagery, videos or external resources. Posted contents are defined by the DESP Communication Manager, approved by the User community manager and published by the information team.
- An autonomous initiative of users: they can cite DESP official account (hashtag or mention) according to the type of interaction demanded to the specific social media channel used. Each quote concerning

DESP is checked by the Communication Manager and Information Team to analyse if a reply is needed in case of unproper content of the post.

Newsletter

The DESP Information Team regularly distributes updates to the subscribers via email. Posted contents are provided by the DESP Communication Manager.

Community Forum

The forum moderator ensures that the forum operates smoothly, adheres to community guidelines, and maintains a respectful and constructive environment for users. The forum moderator is the User Community Manager. The Service Desk monitors the questions raised by Forum participants and forward them to the relevant Service Champion -in charge of responding to the community on specific service channels.

3.1.5 Onboarding procedure acquaint

The “Onboarding” panel of the DESP Web Portal aims to acquaint the reader with existing regulations of the onboarding procedure, i.e., the steps a Standard User should perform to request that his/her Service becomes part of the DESP Ecosystem.

Under the “Get on board” button redirecting to the Onboarding Procedure, it is specified that to continue the registration is needed.

The guide also describes the duties and benefits of a Service integration into DESP, the security and technical requirements to be accomplished, and a high-level description of which information should be provided (see Scenario in Section 3.3.2).

3.2 Service Desk operational scenarios

3.2.1 Support Request opening

This scenario describes how DESP users can raise a support request - depending on their roles.

Any DESP registered and logged user can open a support request onto the DESP issue tracking system. The DESP issue tracking system is reachable via a ‘Contact Us’ form present on the Web Portal. The request automatically opens a ticket into the Issue Tracking System (JIRA).

In the form, the user provides information and relevant metadata to:

- Specify the type of request (incident, anomaly, User Request etc.)
- Add textual description addressing the request
- Specify the DESP service impacted
- Any relevant attachment (in specific formats)
- the relevance of the issue as perceived by the user
- User email

This information is synched in the raised ticket.

At ticket opening, the user is notified (via email). Service Desk response is put on Jira and results in automatic emails to the User. The user could be asked to provide further information if required. Ticket closure is notified to the user via email, with the option to provide feedback on the level of support received (see Section 4.2.2.3).

Unregistered users can open support requests only for registration related issues or for further information.

A Service Provider can open a support request as well but following a different procedure. He/she accesses to the Service Provider Jira Project and clicks to open a ticket, and assigns the issue to the User Community Manager, that is notified at any update of the issue within the project. Please refer to the *DESP Anomaly Management Procedures document* [RD-17] for more details.

3.2.2 Support provisioning

The process of support provisioning involves DESP Administrators and any relevant stakeholder through 3 levels of support, as described in OMP [RD-19] and [RD-17].

3.2.3 Service Rating

A DESP Standard User that has consumed any DESP Registered Service (Platform Management Services, Data Management Services or an onboarded Service) is enabled to give a feedback about the quality and satisfaction of the consumed Service, with a 1 to 5 score. A pop-up appears at the end of one of the transactions consumed in one user session. The pop-up contains a link that redirects him/her to the Service Registry. Here, the user can vote by assigning the score.

Service Rating can be also performed directly via the Service Registry (see Scenario in Section 3.3.1).

3.2.4 User Support Rating

Any user who opened a support request (see Section 3.2.1) can rate the level of support received by raising a specific request. At support request closure, users are asked to rate the level of support received, in terms of effectiveness, efficiency and quality. Feedback is provided in terms of a score from 1 to 5 for different voices of evaluation (like a survey), onto the issue tracking system (JIRA) where the support request is followed.

3.2.5 Events Rating

Any DESP registered user participating to DESP events provides feedback on the event in terms of interest, quality and level of support, etc.

Participants who attended Events are invited by the Information Team to provide this feedback through a survey, sent to them via email at event closure.

3.2.6 User feedback presentation

This scenario describes the process of data collection, preparation, analysis and presentation to relevant stakeholders (ESA and Consortium partners). It is performed by DESP Administrators (User Satisfaction Analyst) on the following items.

- Service rating. This data provides a quantitative information on the overall user experience on DESP. Data on service rating is collected by a dedicated component and available at the Monitoring system.

- User support rating, that include key performance metrics to evaluate the effectiveness, the efficiency and the quality of support. Example of metrics are response time, resolution time, incident/request volume and other derived quantities. This data cope in identifying areas for improvement, and track service level adherence. Data on user support rating is stored within the issue tracking system.
- Events rating, such as the number of participants to events, webinars, or training sessions. This data provides insights on user engagement during dedicated events. Data is collected via email surveys.

User feedback analytics (i.e. User support rating) is presented on a private page of the Executive Dashboard to ESA and EC. The other rating mentioned above are publicly visible within the Executive Dashboard, which allows the exposure of metrics results relevant to Platform Management Services, Data Management Services and new onboarded services which chose to integrate DESP Monitoring.

Moreover, Service usage statistics, giving quantitative information on user's uptake on single DESP services (e.g., data access, downloads, number of active users, etc) are provided by any DESP Service and stored at the Service Operations Monitoring Dashboard Service.

3.3 Service Registry operational scenarios

3.3.1 Service Discovery

Unregistered and registered users can visualize and read the catalogue of DESP Registered Services exposed by the Service Registry. The DESP Registered Services are:

- Platform Management Services
- Data Management Services
- New registered Services, included in the DESP Framework after the onboarding process.

It is visible with direct access to the Service Registry endpoint, and also clicking in a dedicated button on the Web Portal redirecting to it.

The Service Registry supports the possibility of searching for services according to defined keywords/ filtering criteria exploiting existing service metadata (this includes the service usage profile). Moreover, the Service Registry supports a specific area where the user, after selecting a service, can provide a satisfaction score i.e. Service rating (see Section 3.2.3).

Please note that unregistered users can visualize the list of Services, but to access them they need to be registered and logged.

Each DESP registered Service listed in the Service Registry exposes its public offer, listing all available functionalities and price. These functionalities are the available transactions provided by a Service (see Section 3.5.1). Each available transaction must expose all necessary information to the user to understand the price and the exact function offered, including limitations (e.g. quotas). The set of available transactions is the Service Price List.

Service Providers are able to expose their list and related prices within the Service Registry.

Note: The definition of the available transactions is responsibility of the Service Provider, who must be able to support the transaction and its specifics.

The Service Registry also exposes the cost of 1 DCU in Euro at c.e.c.

3.3.2 Onboarding support request

A DESP Standard User willing to become a Service Provider can request to onboard a new service in DESP via the dedicated onboarding panel of the Service Registry.

The Standard User, after the login to the Service Registry, finds the onboarding page with dedicated panels and forms to be fulfil with the information stated in [RD-3].

In particular, main steps are:

- Acceptance of the DTaC (DestinE Terms and Conditions [RD-3], and acknowledge applicable DESP Framework Technical Requirements ([RD-4] and [RD-5]) and DESP Security Requirements [RD-16], by clicking on relevant checkmarks.
- Fulfilling of online form with the following service information (please refer to [RD-3] for details):
  a) Service Name
  b) Service Description
  c) Access Policy
  d) Registration Method
  e) Interface Type
  f) Service Consumption Type
  g) DestinE Usage Profile
  h) Service Usage Profile(s) – if provided by the Service
  i) Content Source Management
- Documentation sharing related to the new Service
- Acknowledge of DESP Services price
- Promotion package delivery (see in [RD-3])
- Administrative and technical Contact points sharing

At the end of this steps:

- sent information are stored and handled via a JIRA Ticketing System.
- the Service Desk is notified (JIRA new ticket) of a new Service Onboarding request and find all the material associated to the onboarding request.via a JIRA Ticketing System.
- The Standard User which submitted the request receives an email confirming the Service Onboarding Request submission.

From this moment on, Standard Users follows the status of their request notified via email(pending/successful/rejected).

3.3.3 Service publication and registration

After the successful Service Evaluation and Service Integration phases [RD-3], the DESP Administrator for the Service Registry receives a notification from the Integration Manager concerning the successful approval of the onboarding of a new Service into the DESP Framework.

The DESP Administrator register the new Service in the Service Registry.

As output:

- The Standard User receives a confirmation email of the successful service registration. Moreover he/she is informed of his/her new role within the IAM Service as 'service provider'.
- the new Service is visible to all unregistered and registered users. Each registered service is characterised by a set of metadata reporting pricing, links, service provider identity information etc.

If needed, only after a specific notification of the Integration Manager, a DESP Administrator can delete a Service from the catalogue.

3.3.4 Digital goods purchase

Every Data Management Service and new onboarded Service of the DESP Platform, has the possibility to offer additional and premium Usage Profiles beyond the free DestinE Usage Profile. Moreover, the Registered Services can offer periodic Subscription to premium resources/functionalities or premium Support packs.

These are identified as Digital Goods, which enable the buyer to premium Service features for a defined period (the Digital Good has an expiration date in terms of months defined by the user at the purchase moment).

The Digital Goods are exposed by the Service Registry page of the Service, the DESP User can navigate through all different types of transactions provided by the Service and, with the availability of a Payment Method, he/she can purchase the available Digital Goods.

The Digital Good purchase follows the Accounting and Billing Scenario in the Section 3.5.

After a Digital Good Purchase, the acquired item is visible in the User Profile Management section of the DESP IAM Service. In this section it is possible to see all the purchased Digital Goods of a user, the active and the expired ones.

3.4 IAM Service operational scenarios

3.4.1 DESP Self-Registration

This scenario describes how unregistered users become DESP Standard Users registering by themselves with self-declaration and self-defined username and password.

An unregistered user reaches the Web Portal of the ID&OS Service. A "Log in/Register now" button dedicated to the registration is present.

In the registration form, in addition to the required User Attribute Fields, the user is invited to review and accept the "DESP Code of Conduct" and the services "Terms and Conditions".

Moreover, there is a CATPCHA check box to avoid bot driven account registrations.

User clicks on the three check boxes and the "sign up" is enabled. By clicking on it, the user is redirected to the SSO page (to the IAM Service) to perform the registration of a new account.

The new account is activated clicking on a link received by DESP via email, to validate the registration.

At the end of the user registration scenario:

- On first access, the user is asked to log-in. Login form is visible and easily accessible from all visitor users not logged;
- DESP Standard Users have full access to the knowledge base at the Web Portal (webinars, documentation, user guides, training material);
- The user is able to open and update tickets thanks to the Service Desk interface;
- DESP Standard Users can access the users forum and write contents/posts;
- DESP Standard Users can access their own cloud project, where they can exploit virtual resources;
- A Wallet (empty) is created, associated to the user account;
- DESP Standard Users can access all DESP Services and relevant resources according to their defined Service Usage Profiles and consume pay-per-use resources according to credits available in the wallet;
- The user is able to log-in into DESP system after entering the correct username/email and password, otherwise an error message is displayed;
- After the log-in, registered users are able to update their profile: clicking on a dedicated button in the DESP Web Portal, they are redirected to the account page on IAM Service, able to update a set of profile attributes (but their username);
- The user's login activity is logged (in compliance to the GDPR) for auditing and security purposes.

3.4.2 DESP Registered Services registration

The scenario describing the procedure to become a DESP Registered Service Provider is covered by scenarios in Sections 3.1.5, 3.3.2 and 3.3.3.

3.4.3 DESP Federated Services registration

This scenario describes how an external service can become a Federated Service and how to enable its own users to access the DESP as Federated Users.

The applicant sends the Federated Service registration request to the Service Desk, following the "Federation Procedure" (TBD).

After the completion, all DESP users are able to login and consume Federated Services using their credentials.

3.4.4 Authorization scenario

IAM Service Administrator can assign one or more User Roles to each DESP registered user, managing the user account directly in the IAM Service dedicated panel.

Once logged-in into the IAM Service with the proper role, the IAM Service Administrator can select a user and enable/disable his/her User Roles.

DESP Administrators can:

- Register services (i.e. client, applications) that can be used for authentication by users

DESP Administrator and Service Providers can:

- Register service resources
- Manage the user authorization over the administrated service resources according to applicable policies over custom attributes and permissions schemes.
- Registered Service Providers are able to manage their own Service Authorization via a dedicated section of the User Account Management UI. In this section, the Service Provider is able to assign specific Client-roles to DESP Users and to manage Service Resources protected by the DESP IAM Service.

3.4.5 Authentication scenario

This scenario describes the log-in of DESP registered users, using IAM Service.

After a successful registration, a DESP Standard User can log-in into the Web Portal of the ID&OS Service, thanks to the dedicated "login button".

After a successful Credential Validation phase, in case of a User participating in at least one Tenant, is required and requested to user to specify the "Context" of the current session. The "Context" determines the correct payment and billing management by the Accounting component. For example, a Standard User participating in a Tenant as Member, after the login can choose to behave like a Standard User or as Tenant Member of the Tenant to which he/she belongs. Please note that a User can participate to more than one Tenant.

Once logged-in, he/she can access all the authorised DESP Services without performing the log-in again (and remain logged-in DESP) until he/she performs the log-out scenario (see Section 3.4.6) or until the user authentication token does not expire.

If a DESP Standard User access directly one of the DESP Service, without having performed the log-in via Web Portal, the user is redirect to IAM Service page to insert credentials.

Moreover, federated users can login into DESP using their credentials, selecting one of the federated IdP listed in the "Log in" Button of the Web Portal.

3.4.6 Log-out

This scenario describes how a DESP Registered User can perform the log-out from DESP.

When a user wants to log out of DESP Services that have a graphical user interface (GUI), they can simply click on the log-out button found on the main page of the corresponding GUI. By doing so, the user is redirected to the IAM Service to complete the log-out process. The user token shall be invalidated, and the account disconnected. A message of log-out successful is shown to the user.

If the service does not have a GUI, the logout is performed via Web Portal or directly via IAM Service exposed API.

3.4.7 Forgot password

This scenario describes how a DESP Standard User can reset his/her password to access DESP and its Services.

The user accesses the Web Portal and clicking on the "forgot password" button is redirected to Keycloak and performs the forgot password procedure, according to the password rules set in Keycloak itself.

The password rules are: the password shall contain minimum 8 characters and shall accept alphanumeric characters plus the following: "!", "@", "#", "$", "%", "^", "&", "*", ")", "(", "+", "=", ".", "_", "-"

3.4.8 User deletion

This scenario describes how a DESP account can be deleted.

The deletion can be performed by triggering an automated procedure via form/button/links provided in the User Profile management section or by a direct request to the Service-Desk.

As result of the completed procedure, the account and all User related data are deleted except for the ones related to financial transactions and reporting purposes. Such data will be kept after appropriate anonymization procedure.

In case of Tenant Member, all the Tenant-context-related User Data will be deleted.

- Delete Account and related User Data
- Implement compliance with GDPR's right to erasure.

3.4.9 Tenant Finance Administrator access

This scenario describes the functionalities provided to a Tenant Finance Administrator by a dedicated Tenant management section of User Account Management UI:

- Manage the active Tenant Payment Method (recharge Tenant Wallet if applicable)

3.4.10 Tenant Technical Administrator access

This scenario describes the functionalities provided to a Tenant Technical Administrator by a dedicated Tenant management section of the User Account Management UI:

- Manage a set of DESP resources assigned to Tenant (purchase/dismiss/assign Digital Goods to Tenant members)

- Manage Tenant group membership (add/remove Standard Users to/from Tenant group)
- Send Tenant membership Invitation to Standard Users

3.4.11 Tenant invitation

In this scenario is described how a Tenant Admin can send to a target DESP Standard User a Membership invitation.

The Tenant Admin access the Tenant management section and send to a target existing user, the request to join for a specific Tenant.

When a DESP Standard User receives such an invitation, he/she has the option to redeem the code or follow the link to finally become a Tenant Member.

Note that a DESP Standard User has the flexibility to participate in multiple tenants, not limited to just one.

3.4.12 Tenant Member access

This scenario describes the functionalities provided to a Tenant Member after DESP login:

- Consume the Tenant resources
- Resign to Tenant Membership in the User Profile section of the User Account Management UI

To login as Tenant Member a user needs to select the "context" for the session, which determines the Tenant Resources accessible to the User. The context selection also allows the option to function as a regular DESP Standard User. The context selection also defines the credit management mechanism:

- If the user acts as a Tenant Member, the Tenant Resources are sustained by the Tenant Payment Method.
- If the user acts as a DESP Standard User (with no membership), the resource consumptions is sustained by its own Payment Method

3.4.13 Federated user access

This scenario describes the functionalities provided to a Federated User and the login phase:

- access to all DESP Standard User functions (except for the Payment Method management which needs a User Personal data integration procedure)
- dedicated quotas/privileges to certain services.

The DESP login page shows the user the ability to execute a login with one of the federated external IAMs.

As a federated user, the user chooses and is redirected to the specific external IAM to perform the login.

The Login phase is managed by the Federated external IAM, after a successful login the user is redirected to DESP platform.

The user can review and authorize the sharing of external User Profile attributes within the DESP IAM Service. These data are used in the relevant monitoring and reporting functionalities in compliance to the GDPR.

Please note that the DESP IAM Service may stores the agreed-by-user Federated User Information except for the User Credentials.

3.4.14 Registered User access

This scenario describes the functionalities provided to a Registered User and the login phase. The functionalities comprehends:

- full access to the DESP Web Portal (webinars, documentation, user guides, training material), and to information on the access modalities and useful contacts;
- access the online discussion platform (Forum) with his/her nickname and write contents/posts, share information and provide feedbacks/suggestions to the registered services;
- contact the Service Desk for any information and request, open and update tickets;
- access the user profile section to modify personal information in the dedicated IAM Service form;
- request the removal of its own account (GDPR "right to erasure");
- access to all the public free services and according to the Service Usage Profile for additional capacity, functions or performances;
- access the Executive Dashboard restricted area;
- manage the User Payment Method and recharge the Wallet;
- the possibility to upgrade their Usage Profile on a chosen Service (by purchasing credits).

The access to DESP Platform happens via Web GUI provided by the DESP Web Portal, thanks to the dedicated "login button". This button redirects the user to the log-in form of the IAM Service where credentials are required to successfully authenticate the user in the DESP (obtain a valid Authentication Token). With this flow, the User is completely unaware of the Authentication Token management. In case of missing Authentication Token, the User is redirected to the IAM Service log-in page.

Please note that the login button/link can be displayed also by DESP Services.

Another access option is via Command Line interface by directly interacting with the Token issuing endpoint provided by the IAM Service (dedicated to technical expert users and scripting purposes). The issued Authentication Token can be attached to the Service Requests that the User performs.

3.4.15 Registered Service Provider access

This scenario describes the functionalities provided to a Registered Service Provider and the login phase:

- perform all DESP Standard User functions
- Service Deployment to designated Infrastructure (Runtime Platform, DESP-Purchased OVH Infrastructure, External Infrastructure)

- DESP IAM Service Integration
- Register the Service in the Service Registry
- register and manage Service Resources (as URIs) through the IAM Service
- manage the Service Payment Method

And optionally:

- Utilise the ecosystem orchestration, high-availability and autoscaling features (available with the Runtime Platform deployment)
- Utilise the ecosystem monitoring and reporting service (available with the Runtime Platform deployment or proper component integration)

Service Providers login in the same way of Standard Users.

3.5 Accounting and Billing operational scenarios

3.5.1 Transactions definition

This scenario describes how a Service Provider defines the available transactions and the relevant Service Price List of his/her Service, to be exposed via Service Registry (see Section 3.3.1).

The transactions that constitute a Service Price List can be of different types:

- Direct transactions: the transaction has an end date, within which it has been completed. E.g., download of a dataset. The cost of the transaction is univocally determined within the price list.
- Digital Goods: the transaction enables to its buyer/tenant member specific behaviours defined and maintained at Service Level. E.g., monthly subscription, Usage Profiles, Support Packs. The specific behaviours are granted until the expiration date, defined at the purchase moment by the User (it can be possible for the User to choose the validity period in terms of number of months).
- Standing Orders: the transaction has no end date; it is performed by the Service Provider as long as the user cancels it or the Service Provider terminates it. E.g., purchase of a cloud resource (VM). The cost of the transaction is time based within the price list.

These types of transactions are treated differently for what regards the consumption (see dedicated Scenarios in the following Sections).

All available transactions within a Service are grouped in Service Usage Profiles. Definition of the kind and the number of Service Usage Profiles is exclusive responsibility of the Service Provider, which has the only requirement to define a 'free' usage profile, called DestinE Usage Profile, while the Service Usage Profiles are payable.

The sponsorship of DestinE is as follows:

- Below a certain number of users (defined in the Cost Model) the service is free

- Above that same number, the service is still free, but the Service Provider can introduce limitations (e.g., reduced performances or execution queues).

As a reference, see in particular [DSP-SOW-056], [DSP-SOW-057], [DSP-TSR-006].

The only difference in the available transactions pertaining to the DestinE Usage Profile is that they are paid by DestinE, but they are nonetheless accounted and billed for as explained in Section 3.5.2.

3.5.2 Payment methods management

The DESP Standard user shall be able to pay to consume services (Data Management Services).

There are two types of payment schema which can be foreseen:

- advanced payment: user purchases in advance DCUs
- arrear payment: user pays the services utilised in the previous TBD period (e.g. monthly).

In the advanced payment case, for a user to be able to use a service (consume the available transactions of a Service), his/her wallet must contain DCUs which are the currency of DESP.

DESP Standard users who wants to recharge their wallet (whether it is empty or not), must insert the Fiscal Info into the user profile via profile editing (in the User Account Management UI). If users attempt to recharge the wallet without tax info, they are redirected to the tax data compilation form.

Then, the user goes to the pop-up form (present in the payment method management section) which shows the number of DCUs that he/she can purchase - there is a drop-down menu with the DCUs to reload.

When the user presses the top-up button, he/she is sent to the payment method choice pop-up (Payment System, payment gateway) where he/she can see how much that transaction will cost them (in any currency).

If the payment is successful in DESP, the user finds the number of DCU credits selected at the beginning, available to be spent.

Once payment has been made, the Billing System sends the invoice of the amount spent using the user's tax data.

Also, please note that the invoices generated by the Billing System are reported in the user's currency.

Please note that DESP does not store any credit card information since it relies on external services for payment purposes.

In the arrear payment case, the user does not use the wallet. Instead, there is an agreement in place between the user and the DESP (Serco). In particular for what regards services consumption, the agreement shall state that the user will pay for all utilised resources on a monthly basis, according to a consumption report to be provided by the platform. Under dedicated agreement, the payment can be quarterly, with discounts based on the volumes etc. Billing is done at month’s end by DESP (Serco).

Registered Standard Users are enabled to find their wallet in the User Account Management UI, recharge it (for the arrear payment) and follow their consumptions, relevant invoices (TBD) and active/expired Digital Goods.

3.5.3 Service Consumption by a DESP registered Standard User

This scenario details the Service consumption by a DESP Registered User.

Whenever a user performs a transaction the Service Provider requests for the accounting approval processed by the Clearing House, by applying the necessary checks and allows or disallows the transaction. The checks are as follows:

- *Advanced payment case*: If the price of the selected transaction is lower than the available DCUs, the transaction is allowed, else it is rejected ("not enough credits").
- *Arrear payment case*: if the price of the services is already utilised within the month ,this allows the transaction if below the Limit of Liability (LoL) of the Service. Example, the agreement between DESP and a user might state that there is a cap of 1,000 DCU per month, so if the already utilised resources amount to 990 DCU and the requested transaction amounts to 20 DCU, it shall not be allowed. The counter resets at each payment period.

If the transaction is allowed, the Service Provider executes it for the user.

At any time, if user has not enough DCUs in its wallet (Adv. Payment case) or has exceeded the cap established in the agreement with the Service Provider (Arrear Payment case), the transaction is disallowed.

In case of Digital Good purchase, the Accounting triggers the assignment to the User of a corresponding IAM Label (and force token refresh) in order to consent the Service Provider to recognize the User and to enable specific behaviours granted by the type of purchased Digital Good.

Moreover, the User receives a confirmation email about the purchased Digital Good and the new purchase is visible (and active) in the User Profile Management Section of the IAM where all the other active/expired Digital Goods are visible.

3.5.4 Billing for Service Consumption by a DESP registered Standard User

The billing scenario for a Service consumption performed by a DESP Registered User is:

- *Advanced payment case*: when a user charges his/her wallet, DESP Billing System issues an invoice with all relevant details.
- *Arrear payment case*: User is billed by DESP Billing System for the consumed resources in the reporting period.

3.5.5 Payment Scenario for Service Consumption by a DESP registered Standard User

The payment scenario for a Service consumption performed by a DESP Registered User is the following.

DESP acts as an intermediary between consumer and provider, so when a user uses a Service, in financial terms:

- The user pays DESP for utilising the Service (and is billed by DESP).
- The Service gets paid by DESP for its consumed resources (Service bills the DESP).

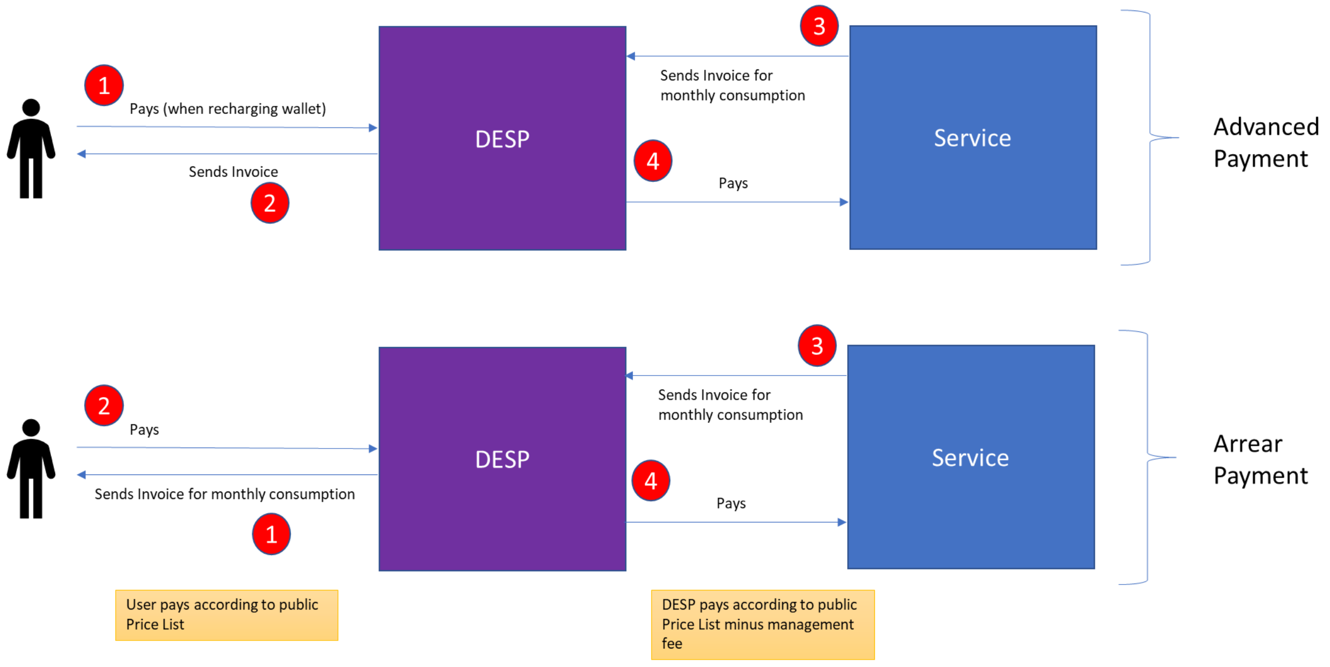

1
Pays (when recharging wallet)
Sends Invoice
2
DESP
3
Sends Invoice for monthly consumption
4
Pays
Service
Advanced Payment
2
Pays
Sends Invoice for monthly consumption
1
DESP
3
Sends Invoice for monthly consumption
4
Pays
Service
Arrear Payment
User pays according to public Price List
DESP pays according to public Price List minus management fee

Figure 3: Payment scenario for Service Consumption by a registered user

User pays either when charging its wallet or on a monthly basis when receiving invoice from the DESP for the monthly consumed services. The Service Provider gets paid by DESP for the consumed resources on a monthly basis (step 4 in the diagram). The payment is based on the public price list minus a platform management fee to be deducted. For example, if for a given transaction the price is 10 DCU, the user shall be billed for 10 DCU but DESP will pay the Service for 8.5 DCU. The difference 1.5 DCU is the revenue of the platform which covers the overall costs of managing it.

Note: the management of this 'platform management fee' is TBD. It is currently already present in the cost models of the Data Management Services, whose price list has actually two prices, one is the public final price for the users, the other is the hidden internal price.

3.5.6 Service Consumption by a Tenant Member

This scenario is the same of the Service Consumption by a DESP registered Standard User with the exception of the charge of the DCU payment to the Tenant Payment Method instead of the User Payment Method.

This flow is allowed within DESP since the Service Provider is aware of the User login context and provides it to the Clearing House which, in this way, can charge the DCU payment to the context-specified Tenant payment Method.

3.5.7 Billing for Service Consumption by a Tenant Member

The billing scenario for a Service consumption performed by a Tenant Member is:

- *Advanced payment case*: when a Tenant Finance Administrator recharges his/her wallet, DESP Billing System issues an invoice with all relevant details to the Tenant Finance Administrator as representative of the Tenant owner entity.

- *Arrear payment case*: Tenant Finance Administrator as representative of the Tenant owner entity is billed by DESP Billing System for the consumed resources in the reporting period.

3.5.8 Payment Scenario for Service Consumption by a Tenant Member

This scenario is the same of the Payment Scenario for Service Consumption by a DESP registered Standard User with the exception of the consumptions are performed by Tenant Members (instead of User) and the charged payment method is the one owned by Tenant and managed by the Tenant Finance Administrator.

3.5.9 Service consumption by another Service

This scenario details the Service consumption by another Service.

Whenever a Service A performs a transaction on the Service Provider B, the latter performs necessary checks and allows or disallows the transaction. The checks are as follows:

- Advanced payment case: arrear.
- Arrear payment case: the Service Provider B queries Clearing House and checks the price of the services already utilised within the month by Service A, and allows the transaction if below the Limit of Liability (LoL) established in the agreement.

If the transaction is allowed, the Service Provider B executes it for Service A.

At any time, if Service A has exceeded the cap established in the agreement with the Service B, the transaction is disallowed.

3.5.10 Billing for Service Consumption by another Service

The billing scenario for a Service consumption performed by another Service is:

- *Advanced payment case*: not foreseen
- *Arrear payment case*: Service A is billed by DESP Billing System for the consumed resources in the reporting period.

3.5.11 Payment scenario for Service Consumption by another Service

The payment scenario for a Service consumption performed by another Service is the following.

Foreword: DESP acts as an intermediary between consumer and provider, so when a Service A uses another Service B, in financial terms:

- The Service A pays DESP for utilising the Service B (and is billed by DESP).
- The Service B gets paid by DESP for its consumed resources (Service B bills the DESP).

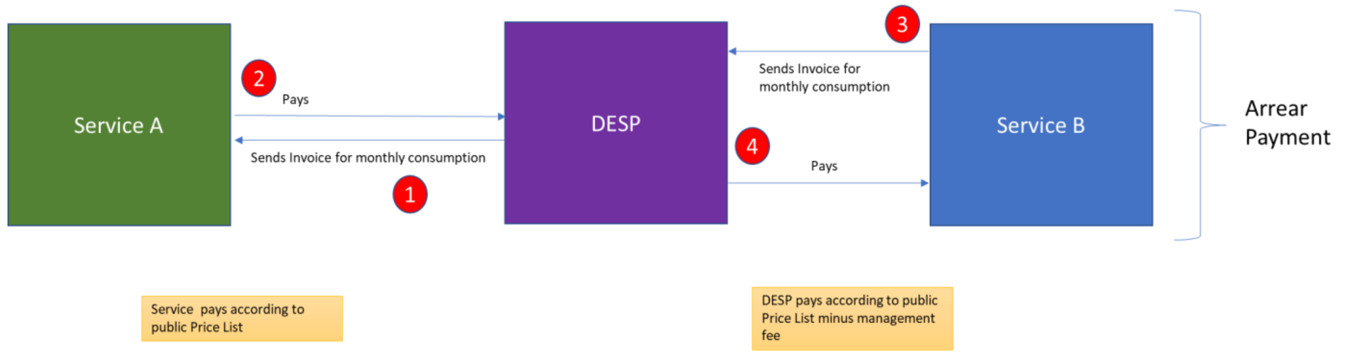

Service A
2
Pays
Sends Invoice for monthly consumption
1
DESP
3
Sends Invoice for monthly consumption
4
Pays
Service B
Arrear Payment
Service pays according to public Price List
DESP pays according to public Price List minus management fee

Figure 4: Payment scenario for Service Consumption performed by another Service

Service A pays on a monthly basis when receiving invoice from the DESP for the monthly consumed services of Service B. The Service Provider B gets paid by DESP for the consumed resources on a monthly basis (step 4 in the diagram). The payment is based on the public price list minus a platform management fee to be deducted. For example, if for a given transaction the price is 10 DCU, the user shall be billed for 10 DCU but DESP will pay the Service for 8.5 DCU. The difference 1.5 DCU is the revenue of the platform which covers the overall costs of managing it.

Note: the management of this 'platform management fee' is TBD. It is currently already present in the cost models of the Data Management Services, whose price list has actually two prices, one is the public final price for the users, the other is the hidden internal price.

3.5.12 Service transaction logging

Within the DESP, the element in charge of managing all the occurring transactions is the Clearing House. Management is in terms of:

- Storing transactions
- Querying the stored transactions according to selection criteria
- Export reports on stored transactions
- Allow/deny transactions requested by Service Providers.

The Clearing House is managed by its Service Operations Manager who has full access to its contents. DESP Standard Users do not access directly the Clearing House. Service Providers may access it only limited to the queries on their services.

Whenever a Service executes a transaction, it shall record an entry within the Clearing House which will contain as a minimum, the transaction ID, the timestamp, the ID of the originator (be it a user or another service) the parameters of the transaction if any and the price of the transaction in DCUs.

Clearing House reports are extracted by Service Providers or DESP System Administrator to provide the detailed list of transactions a user (service) has performed in a given time frame.

3.5.13 Integration of a new Service with Accounting Service and Billing System

In the context of onboarding (Service Integration) a Service onto DESP, one of the elements that can be optionally integrated is the Accounting Service/Clearing House and Billing System.

The DESP Accounting allows a Service Provider to perfectly record all the available transactions it performs to satisfy requests (by Users and other Services). Only transactions stored in the Accounting (Clearing House) will be accounted for the Service Provider to request the related payments.

Assumption: It is assumed that:

- the Service has been already registered into the DESP Service Registry, and that it has (as part of the registration) defined all its available transactions and related Price List, categorised per Service Usage Profiles (see Scenarios in Section 3.5.1).
- The Service has been integrated already with the DESP IAM Service.
- The consumption of resources needed to perform the transaction (e.g, VMs, other Services) are responsibility of the Service Provider as well as the monitoring and payment of the incurred costs.

Integration of a Service Provider within DESP requires it to get write privileges to the Clearing House, to be able primarily to store transactions. The access is granted by DESP Administrator who configures the Clearing House.

The Clearing House - responsible for storing, querying and reporting on the Service available transactions - exposes the following functions for the Service Provider (Transaction Storing, Transactions Querying, Transaction Reporting and Transaction Allow/Deny). Please refer to the relevant ICD [RD-18] for the needed steps.

Moreover, all transactions are invoiced by Serco to User/Other Service via the Billing System which generates the invoices as necessary. The Service Provider in turn invoices Serco for its provided service.

Therefore, integration of a Service Provider with the Billing System requires that the Service Provider gives its relevant financial details to the Serco Billing System.

Part of this integration is the definition of Accounting and Billing Service costs. Preliminarily, it may depend on the maximum number of transactions storable in time (e.g., monthly) and the number of queries and reports doable in time.

3.6 Dashboard Services operational scenarios

3.6.1 DESP Services monitoring

To check the DESP Services performance, ensure the target level of quality and achieving goals prefixed for each DESP service, automatic and independent tools are used as much as possible, for routinely monitor different applications of DESP by means of specific parameters.

The service monitoring stakeholders are the Monitoring Manager, Operations Manager and Service Manager, interested in monitoring the various services status, capacity and expense.

The information and parameters of interest are:

- collected from several sources time-tagged and suitably formatted for further processing by other functions;

- recorded in real-time and long-term databases: the real time database is designed as rolling archive providing access with minimal delay to the parameters of interest and the long-term database, a.k.a. data lake, is designed to provide a persistent and virtually infinite store of records;
- visualized using graphic application requesting time series or cumulative parameters from the DBs (e.g. Grafana).

3.6.2 DESP Services Reporting

The data mining, targeting mainly to the data warehouse, allows extracting both basic information (e.g. values of records in a given time range) and processed information (e.g. value of function of several records, its integral over time, etc.) in order to routinely, according a configurable schedule, report them onto Service Operations Monitoring Dashboard reports.

3.6.3 DESP Services Alerting

DESP includes the possibility to set of rule engine able to check if any monitored parameter crosses some threshold. The evaluation processes are also helped by an alerting tool which sends messages (sms or emails) in case significant event of DESP services take place.

There are two types of alerting: internal and external.

1. Internal alert (handled by the monitoring service, i.e., Service Operations Monitoring Dashboard): the Operations manager are notified about any service component whose failure may compromise the service level quality (KPIs).
2. External alert (handled by the Wallet Management, see Scenario in Section 3.5.2): self-service users are notified in case they are about to be out of resources (wallet amount going down to 0 DCU credits): there is a scheduled task that computes the residual number of days before a wallet expires based on the cost of actually running resources/services.

A notification is sent to the user a configurable number of days before the computed expiration date (the number of days is part of the configuration management provided to the Operation Manager).

During the last notification, the operation team receives the request to handle resources deletion, including a clear indication of the resources to be deleted and the user is also notified 24 h before the planned deletion.

3.7 Data Workflow Services operational scenarios

3.7.1 Data retrieval and ingestion

This scenario describes how DESP Administrators can configure the data collections / datasets in the “Data Access & Retrieval Service” to enable DESP Standard Users to search and download data (see Section 1.3.2). The data collections / datasets compliance with [DSP-USR-SDP] which describes the supporting services to each dataset available for DESP Core Services is described in Section 3.7.4.

The DESP Administrator accesses the Data Access & Retrieval Service dashboard user interface, which enables the configuration of Data Sources and Datasets, as well as access authorization.

He/she handles the Data Access & Retrieval Service resources (i.e. adapters):

- To configure the Data Source, including Name, Description and capabilities / services
- To retrieve Data Collection / Dataset from the data source,
- To configure the access policy / terms and conditions / users and groups,
- To configure the cache policy / retention policy.

The data collections retrieval from Data Sources starts. Then, products are submitted to data integrity check (see dedicated scenario), and if successfully passed, they are stored.

In case there is a failure during the retrieval of a product, the Data Access & Retrieval Service forwards to the DESP Administrator the error code / error description.

3.7.1.1 Data Availability

This scenario describes how retrieved data (see Scenario in Section <3.7.1>) are stored, and how they are made available to DESP Standard Users.

The Data Catalogue & Discovery Service exposes both HDA API and the OGC API to exploit data specified in [DSP-USR-SDP].

Data retrieved from Data Sources are stored in two dedicated cache volumes: a systematic cache and a smart cache.

- The Systematic Cache is used to cache the data collected routinely as defined in [DSP-PDM-SDP], that will be immediately available to DESP Registered Users (as they are physically present in the storage).
- The Smart Cache is used to cache all the other data specified in [DSP-USR-SDP]. In particular, it contains data that users do not have found immediately available since they were not physically stored in the Systematic Cache, so they had to submit an order. Once re-ordered, they are stored (physically present) in the Smart Cache and available.

So, summarizing, the following two scenarios can coexist in the Data Catalogue & Discovery Service:

- Case 1: Data are not physically present in the storage (Smart Cache or Systematic Cache). Data can be ordered by interested Users according to the dedicated scenario (Section 3.7.2) and then present in the Smart Cache.
- Case 2: Data are physically present in the storage (Smart Cache or Systematic Cache). Users can benefit from the cache policy applied to the data collection, but physical data are subjected to retention policies as described in the dedicated scenario (Section 3.7.3).

As output, Data Catalogue and Discovery Service allows DESP Standard Users to find retrieved data (see Section <3.7.1.3>), belonging to the specified in [DSP-USR-SDP], thanks to dedicated APIs.

3.7.1.2 Data Storage

Products stored in the Systematic Cache and/or in the Smart Cache follows this Archiving Structure:

`<root directory>/`, this is the object storage

    `<data source>/`, it refers to the data source

`<data collection ID>/`, it refers to the data Collection

`<dataset ID>/`, it refers to the dataset

`[<YYYY>/<MM>/<DD>/]`, this is an optional

`<product ID>`, it refers to the physical file

3.7.2 Data search and download

This scenario describes how DESP Standard users can search and download data specified in [DSP-USR-SDP] thanks to Data Catalogue & Discovery Service - at least any DEDL dataset (see [AD-DDL-DP]) and all datasets available in the Copernicus Data Access.

The Data Catalogue & Discovery Service provides both REST API and web graphic user interface to support the data search, access and download. A ReDoc or Swagger page is released as documentation to describe the HDA API. The Finder is made available to DESP Standard users to discover and access data belonging to the Portfolio in a user-friendly web application.

Unregistered users can discover the list of available datasets specified in [DSP-USR-SDP]. To have full access to the Catalogue, the user needs to be registered and logged.

After a successful login, Standard Users and DESP Administrators have a two steps search for data available in the Data Catalogue & Discovery Service through Harmonised Data Access (HDA) APIs and / or through the HDA Finder web interface exposed by Data Catalogue & Discovery Service.

Dataset discovery (1st step search)

Users are required to select, as a first choice, the Dataset – (e.g. Sentinel-1, Envisat, Meteosat Third Generation, …).

Then, within the selected Dataset, they are allowed to select geographical and temporal filtering criteria, concatenating them with the "&" symbol as they are built upon the AND logical operator.

Possible filter criteria are:

- Temporal criteria (e.g. start date, end date)
- Geographical area (e.g. spatial extend in lat/lon)
- Data Source (e.g. Copernicus Data Space Ecosystem, Copernicus Marine, Data Lake, …)
- Additional queryables defined at data collection level (e.g. cloud cover, quality flag, …) are directly retrieved and managed through the HDA API.

If available among the Data Sources functions, access to geographical subsets is supported as well: in this case, the action is not executed starting from a product already available in the Cache but it is retrieved from the Data Source.

Data search (2nd step search)

Once selected the dataset of interest, the DESP Standard Users can search for data by applying spatial and temporal filters, as well as any other queryable defined at data collection level such as product type, orbit direction, cloud cover, quality flag.

As output, a paginated list of products and metadata corresponding to filtered criteria are returned to users. Each item has a series of metadata and associated services.

All available metadata at products level - including product ID, start date, end date, quicklook / thumbnail (when available), download URI, as well as all other attributes and access services available on the Data Source are directly retrieved from them (see Data Workflow Service ICD).

The download URI is used to perform the data download: the access granularity, namely the access to full product or partial product (manifest, band, etc...), as well as the data format (e.g. nc, TIFF, COG) and packaging (e.g. SAFE, ZIP) are defined at the data sources.

Data provided by the Data Workflow Service can be searched by all users, even unregistered. For data access instead, the registration is needed. Nevertheless, the access to products belonging to specific Datasets are governed by user roles and groups. In case of future needs, an access policy based on groups can be configured.

As defined in [DSP-PDM-SDP], a subset of data belonging to the systematic cache is subject to data processing pipelines (e.g. conversion from native data format to cloud-native data format).

All the metadata at products level are retrieved by the Data Access and Retrieval Service from the original External Data Sources. The following services and interfaces are offered in addition to the HDA API:

- OGC services and API (OGC OpenSearch with Geo and Time Extensions, OGC Web Map Service, OGC Web Coverage Service) [RD-11, RD-13, RD-14]
- STAC API [RD-12]
- S3 API [RD-15]

Please note that for the OGC Web Map Service and OGC Web Coverage Service offers layer visualization without mosaicking capabilities. The layer can be global or a single AOI depending on the geographic coverage.

3.7.3 Data cache management

This scenario describes how DESP Standard Users can benefit from the Smart Cache and Systematic Cache of MEEO's Data Workflow Service, which supports optimised data access for fresh products available from DEDL as well as federated access services.

Within the Systematic Cache, a subset of the DESP datasets is converted into cloud-native data formats. The generic cloud-native data conversion workflow consists of a series of steps as presented in Figure 5.

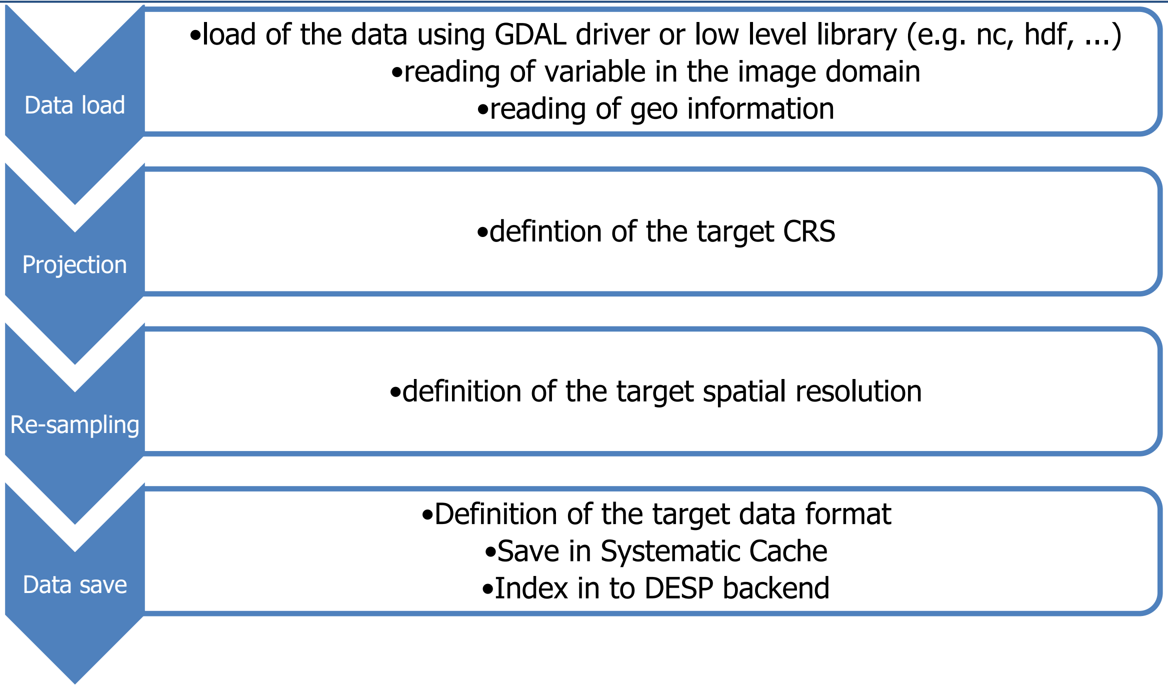

Data load
•load of the data using GDAL driver or low level library (e.g. nc, hdf, ...)
•reading of variable in the image domain
•reading of geo information
Projection
•defintion of the target CRS
Re-sampling
•definition of the target spatial resolution
Data save
•Definition of the target data format
•Save in Systematic Cache
•Index in to DESP backend

Figure 5: Data conversion workflow

Please note that the Cache is applicable only to the data specified in [DSP-USR-SDP], while direct upload of user own data in the Data Cache Management Service is not supported as a DESP Core Service. *Users generated data (as output of User Workflow Services of DESP) are stored in the storage of the user (Cloud Resources).*

On the data listed in specified in [DSP-USR-SDP] routinely data collection and data transformation are applied. For the remaining data, a default cache strategy with a retention policy of one week is applied.

The DESP Administrator can dynamically configure the cache strategy and retention policy (see as described in Section 3.7.1) at data collection level.

3.7.4 Data Offer Completeness

The check of completeness in the data offer is scheduled on a regular temporal basis (configurable) and it consists in a comparison of the list of all data collection / datasets published on the MEEO's Data Workflow Service and DESP data sources (as DEDL and federated access services). In case the comparison shows the presence of missing data collection and dataset on the Data Workflow Services interfaces, they are recovered with highest priority.

The Data Offer Completeness tool

- connects with Data Source (i.e. DEDL and federated access services) to retrieve the data collections and datasets list
- compares the list retrieved from the item above with the "Data Catalogue and Discovery Services" data offer
- updates relevant metadata (e.g. temporal extent, description, …)
- notifies the DESP Administrator about changes applied and/or anomalies in data availability.

3.7.5 Data Integrity

This scenario describes how Data Workflow Services check whether the products are integer or not, before storing them in the Cache.

After the products retrieval and before their storing/their referencing, the Service performs the following steps for each product:

- Identification of available information (such as product size, checksum) by the data producer (Data Source).
- According to the previous point, when that information is available at Data Source level – the Data Workflow Service computes them at the end of data retrieval and before the storing in the Cache.
- Comparison between the information above.

The output of this activity is that the Data Workflow Services only ingest products for which the integrity check is passed and data are preserved in respect to the Data Source.

3.7.6 Data eviction and deletion

Retention policies as defined in the external data sources (i.e. DEDL, federated data access) are inherited in the Data Workflow Services.

Eviction refers to the automatic process to remove items from the Data Workflow Services.

Deletion refers to the on-demand / human-driven process to remove a series of products from the Data Workflow Services.

Eviction of products from the DESP Cache is performed according to the retention policies defined in [DSP-PDM-SDP].

Eviction policies are:

- the data order time has exceeded the eviction time
- the volume of the data reaches the 90% of the storage resources allocated to the Cache.

The Deletion process is performed by DESP Administrators using an ad-hoc API which accepts as input the array of the products' IDs to be deleted.

3.8 Data Cache Management Service operational scenarios

3.8.1 Data retrieval and ingestion

This scenario describes how data from external Data Sources can be retrieved and ingested in DESP DCMS.

Primarily, DESP Administrators can properly configure DCMS to retrieve data specified in [DSP-USR-SDP], defining:

- Data to be retrieve,

- the Data Sources from which they should be gathered,
- the relevant stated retention policy,
- the format in which products can be ingested, and then stored (different or not w.r.t. the one in the native Data Source),
- User-based quota relevant to access.

DCMS routinely retrieves data and stores them in a 'local archive'.

As output, Registered Users are enabled to search, access, and download data in the 'local archive'.

Note that this action can be proposed as part of the DCMS DestinE Usage Profile (free).

Further, DESP Registered Users or DESP Data Management Services interested in having a specific Data Collection easily available in DESP, can contact the Service Desk via the dedicated Web Portal form.

The retrievable datasets can be visualized from the "Data Offer" panel in the DESP Web Portal, which reports the data specified in [DSP-USR-SDP]. Moreover, also datasets not belonging to DestinE data sources can be proposed.

The request to the Service Desk should contain:

- the data source including name, description and capabilities.
- the Data Collection / Dataset to be retrieved from that data source.
- metadata to be ingested (in case of Data Sources not belonging to DestinE perimeter. Otherwise, the extracted metadata will follow a default Data Model showed in the Service Registry/ Information Model)
- the cache retention policy, i.e., how long datasets must be kept in the DCMS.
- The access policy / terms and conditions / users and groups / quota, i.e. who can access the retrieved dataset.

The request is evaluated and, when accepted, the DESP Registered Users is notified via email.

At this stage, DESP Administrator configures the Data Cache Management Service via the dedicated API. As output, chosen data are stored in a dedicated 'service cache' accessible according to the agreed data policy.

In both cases, products are submitted to data integrity check, and if successfully passed, they are stored. In parallel, a trace is created for each published product (see dedicated scenario).

In case there is a failure during the retrieval of a product, the DCMS DESP Administrator is notified with an error code / error description.

Please note that neither DESP Administrators, nor Registered Users can autonomously upload his/her products directly into the Cache Management Service.

3.8.2 Search and download

After a successful authentication and authorization, DESP Registered Users can access to the Data Cache Management Service.

According to the chosen access policy set by DESP Administrators, a specific Data Collection /Dataset can be searched and filtered in DCMS.

For what concerns data chosen by DESP Registered Users, this data can be found only by the requester (and his/her relevant Service, if Service Provider) and by the set of other Service Providers declared as allowed by him/her or by ESA.

Moreover, if this data are ingested in another Service, they can be searched and filtered by means of this Service with a *Service specific* data access policy – not the one of DCMS.

Search and filtering are allowed by a standard API (S3 and STAC).

Following again the defined access policy, users can also download products in DCMS with the agreed user-quota. The supported download is partial, i.e., only chunks of data can be requested.

3.8.3 Cache retention policy

Retention policies are chosen by the Service providers for each chosen dataset/ data collection.

Eviction policies are:

- the volume of the data reaches the configurable percentage (e.g., 90%) of the storage resources allocated to the Cache for the relative Service Provider.

- Data offer is not compliant with the one specified in [DSP-USR-SDP].

If needed, DESP Registered Users also contact DESP Administrators (via the Service Desk) if a set of products should be deleted. They should provide a description of the cause of this request. If accepted, the Deletion process is performed by DESP Administrators using an ad-hoc API which accepts as input the array of the products' IDs to be deleted.

For each eviction/deletion activity performed on a product, the relevant trace in the Traceability Service changes tracking the operation.

3.9 User Workflow Services operational scenarios

3.9.1 Code editor usage

3.9.1.1 User environment instancing and configuration

Any DESP registered user can access the User Workflow service and use the configured virtual resources (RAM, CPU/GPU) to exploit, depending on their usage profile.

At the User Workflow service, the user identity is verified (by the IAM) and a new Jupyter Notebook server is instanced, running asynchronously on the DESP runtime platform with the requested resources.

Onto the Jupyter Server, the user environment shows the following characteristics:

- All the DESP Common Software Services are installed and properly configured for usage. This includes also the *conda* and *pip* utilities to install additional packages.

- A certain amount of disk space is provided within the user environment to store small-sized user generated data. The disk space depends on the usage profile. To increase storage, the user can update own profile or access own buckets purchased on OVH services (Python libraries).

- Server usage is monitored on time scale of usage. For efficiency, unused servers are claimed back and removed from the pool. The storage is persisted and later attached to a Server instantiated later from the same user.

- Monitoring data are collected by the Monitoring Service.

Within their own environment, users can develop code, run algorithms, or invoke any allowed transformation on data.

When accessing the User Workflow services, user is also provided with templates aiming at speeding up integration activities.

In particular, when accessing the *Development Environment (JupyterHub)* the following set of templates with integrated libraries is provided e.g. to support data transformation services:

- EO Expert (GDAL, RASTERIO, proj)

- AI/ML EO Expert (GDAL, RASTERIO, PyTorch, TensorFlow, scikit learn)

When accessing the *Processing Environment*, via API or UI, user is provided with

- Basic template (Dockerfile and scripts) for simple processing integration (e.g. snap graph)

- Basic template (Dockerfile and scripts) for AI processor integration (e.g. Sentinel-2 image segmentation)

The user can also adapt (and save) the templates, consult available tutorials and request for support.

3.9.1.2 Data Fetching

Within their own Jupyter environment, any DESP registered user can fetch data from the Data Workflow service. The Data Workflow API can be invoked via Jupyter Notebook and will allow users to exploit data in their own coding architectures. The data can be accessed remotely (or even data portions, e.g. range header, single variables, etc.) with no need of local/temporary download in the user environment. If needed, data can also be locally downloaded. Notebook templates will show some examples of data access, by means of e.g. Python functions.

3.9.1.3 Data transformation and preparation

Any DESP registered user can transform data at scale by means of on-demand processing workflows within the Jupyter environment. This is achieved across the following steps.

- Data is accessed at scale at the Data Workflow service and loaded into the coding environment. Thanks to the Data Workflow APIs (see also [RD-11], [RD-12], [RD-13], [RD-14] and [RD-15]) users can access data variable or single bands throughout their custom workflows with no need of accessing the entire dataset.

- Users can exploit the DESP Common Software Services to transform this data on the fly. The output data can be redirected onto user's own workspace or also into user's own OVH storage buckets.
- Users can instance dedicated on-demand processing workflows to prepare data into ARD, specifying the destination output location (user's own workspace or also into user's own OVH storage buckets). Please note that data preparation routines are assumed to be provided by the users as being part of their own workflows. Some examples will be made available by the User Workflow Service as templates.
    - The User Workflow Service offers further engineering support to optimize user's algorithms to efficiently parallelize tasks.
- Data stored in local storage or user's own buckets can be re-used throughout further user workflows. Own buckets (reachable via the internet and given access credentials) can be attached to the user environment and the content accessed via API (e.g. S3).
- *(Way forward)* Prepared datasets can be accessed by other data management services throughout the DESP perimeter upon request. The system exposes a dedicated API to publish prepared datasets. An example is the Visualization service, accessing the User Workflow to visualize datasets after transformation or preparation workflows.

Users can monitor the status of running data transformation/preparation workflows, having full access control to stop or re-initiate them via an API.

Some examples of processing workflows are available within the User Workflow service; users can load these templates in their own environment and edit the code architectures if needed to create new workflows. Any template is reusable by users within their own environment.

3.9.1.4 AI Workflows

Any DESP registered user can run AI/ML workflows within the development and processing environment. These are already configured with all the required AI packages and manages computations on the GPU(s) specified by the user, depending on the profile.

Some AI template architectures are available within the User Workflow; users can load templates in their own environment and edit the code architectures if needed to create new workflows. Any template is reusable by users within their own environment.

Users can monitor the status of running AI workflows, having full access control to stop or re-initiate them via CLI/UI dashboard.

A minimal set of AI packages is part of the environment template instanced at user's first access. However, users can customize this set by adding more packages, or upgrade/downgrade versions depending on their needs via *pip* or *conda* utilities.

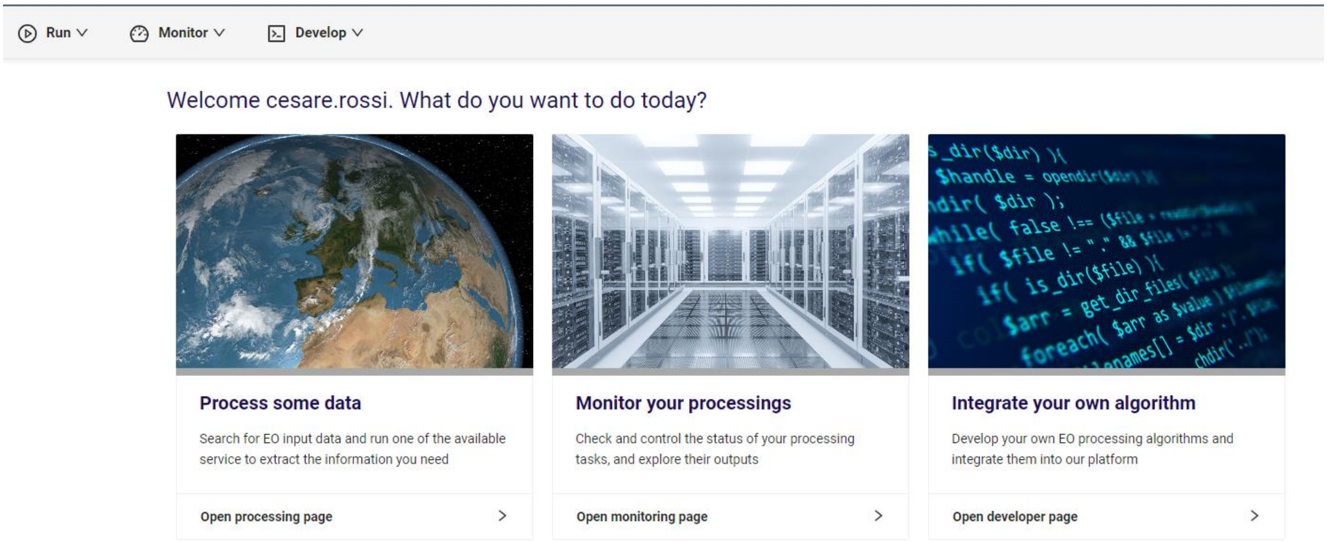
GPUs are instanced with the AI template, depending on the usage profile, and computations are automatically redirected to GPUs processing, with no need of further configuration by users.

3.9.2 Processing Environment Usage

Any DESP registered user can access the User Workflow service at scale, using the Processing Environment.

At the User Workflow service, the user identity is verified (at the IAM) and a Web Interface is available to:

- Process some data (e.g. prepare ARD)
- Monitor the processing pipeline;
- Integrate new algorithms, for a processing workflow at scale



Welcome cesare.rossi. What do you want to do today?

Process some data

Search for EO input data and run one of the available service to extract the information you need

Monitor your processings

Check and control the status of your processing tasks, and explore their outputs

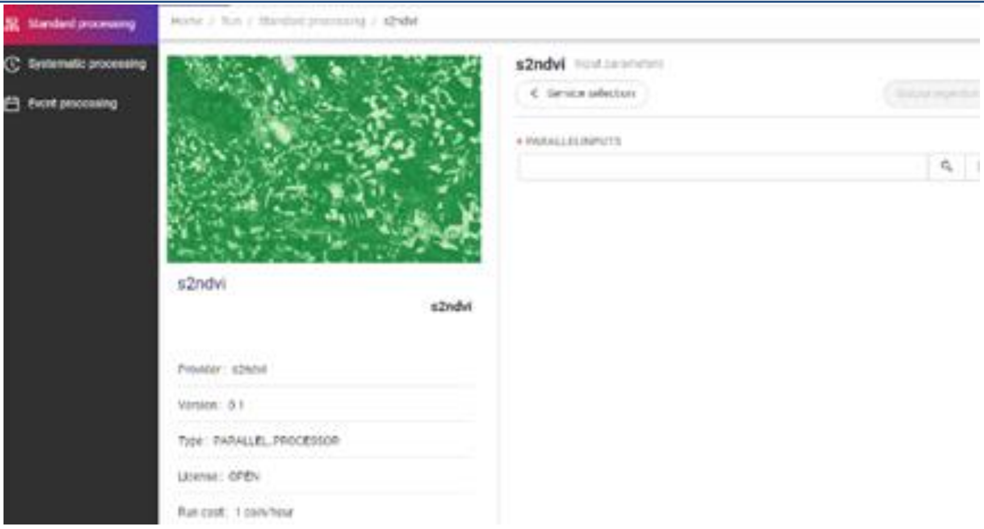
Integrate your own algorithm

Develop your own EO processing algorithms and integrate them into our platform

Figure 6: Processing environment UI presentation.

The processing workflow consists in the following steps:

- Create the structure of the service implementing the algorithm via templating (e.g., AI/ML services, EO Processing)
- Add code and configuration to the structure:
  - The definition of the Dockerfile (i.e., libraries and tools)
  - The definition of input and output
  - The parallelisation, that is a parallel processor spawning one job per input file
- Build code and configuration via UI
- As a result, the service appears in the UI with all the information provided by the user at the previous steps (see Figure below, example NDVI processing on Sentinel-2 data)



s2ndvi

Provider : s2ndvi

Version : 0.1

Type : PARALLEL_PROCESSOR

License : OPEN

Run cost : 1 coin/hour

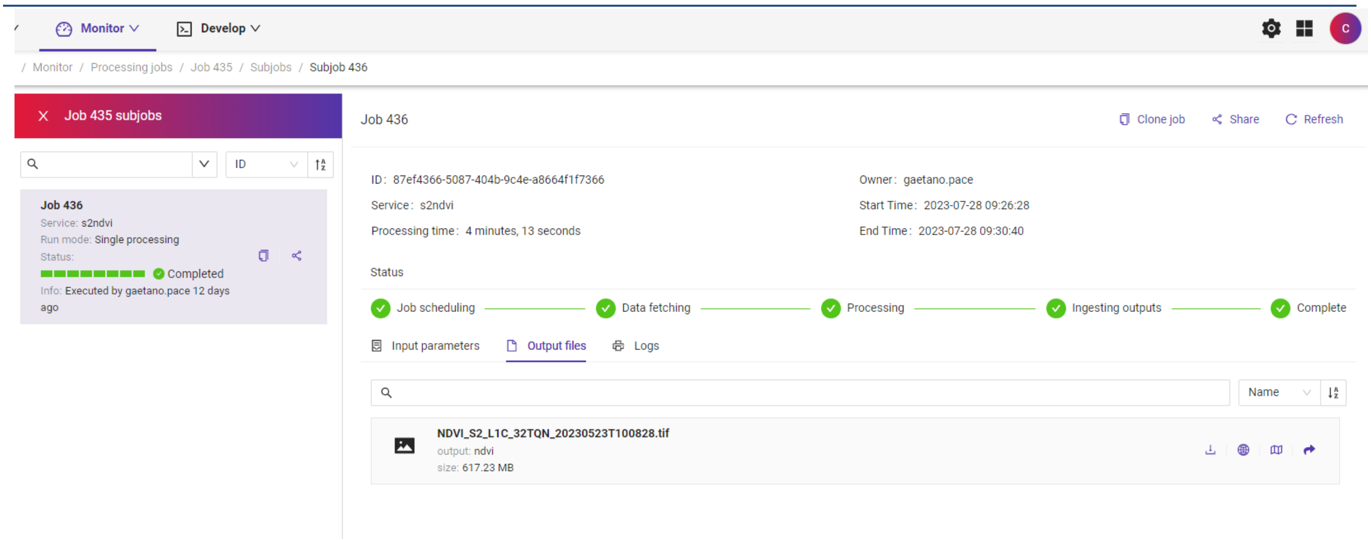
Figure 7: Example of NDVI processing service on Sentinel-2 data deployed in the User Workflow processing environment.

- Run the service, being able to select the input files, using the embedded catalogue search (searching on all DestinE input data) and choosing the list of input files to be used for the processing.
- Monitor the execution, and access the results generated. Results can be inspected directly within the Processing Environment UI, analysed from other environments like JupyterHub or the User's local environment, by accessing them using OGC Protocols (e.g., WMS WCS).

  An example of execution may consist in:

  - Job scheduling (configuration of datetime of workflow execution)
  - Data fetching (access the data used for processing)
  - Processing (run the user's algorithm)
  - Outputs ingestion

  The UI guides the user through the steps above like represented in the Figure below.



Job 436
Service: s2ndvi
Run mode: Single processing
Status: Completed
Info: Executed by gaetano.pace 12 days ago

Job 436

ID: 87ef4366-5087-404b-9c4e-a8664f1f7366
Service: s2ndvi
Processing time: 4 minutes, 13 seconds
Owner: gaetano.pace
Start Time: 2023-07-28 09:26:28
End Time: 2023-07-28 09:30:40

NDVI_S2_L1C_32TQN_20230523T100828.tif
output: ndvi
size: 617.23 MB

Figure 8: Example of processing pipeline displayed in the processing environment UI.

The Processing Environment functions are entirely accessible via a REST API, and therefore the access can be achieved via Python (e.g., using Python libraries) or Shell (e.g., using *curl* or *wget* utilities).

The Processing Environment can be used for data preparation workflows, upon request or on scheduled baseline as well. Prepared ARD is made available via a dedicated API of data access by the User Workflow.

3.9.3 User Workflow Community

3.9.3.1 Sharing

(Way forward) Any DESP registered user can share their own notebooks (containing code, plots, etc.) with other users and collaborate on the same contents. The system synchronizes with a remote open-source repository, so that the user generates a link HTTP that redirects shared selected contents via web interface, with customizable permissions. *This scenario will be foreseen at later stage*.

3.9.3.2 Publication

Any DESP Registered user can publish:

- User generated software or applications images
- *(Way forward)* User generated datasets or data archive*.*

Publication is upon request via a REST API. Published elements will be uploaded in a public data store and made available to other users for consumption (access permissions could be customized).

As concerning software images, the user can load public images via API and re-use them within own workflows.

As concerning data sets, user's generated data are published by adopting a naming convention. Such reference is assigned within the DESP perimeter (not at the Data Lake). *This scenario will be foreseen at later stage*.

3.9.3.3 Contributing

Any DESP Standard User accessing the User Workflow service can remotely synchronize their own code via the DESP Common Software services (i.e. *git* utility) installed within the development environment.

Access is granted to user's own repository, external to the DESP perimeter.

3.10 Visualization Services operational scenarios

3.10.1 Create Visualization scenarios via UI

Any DESP Standard User can access the Data Visualization service to visualize data and information on a dynamic map.

The user starts the data visualization service upon action, via UI on web or mobile, loading the data available for visualization, in real time. In doing this, the user is creating a visualization scenario, also called "show", regarding a phenomenon or a user's case study of interest.

Creating a show means to:

- Select a region of interest (ROI).
- Select a time of interest (TOI).
- Select a canvas1 on the graphical user interface.
- Access the Data Workflow and select a dataset among the "visualization-ready" data options.
- Select a layer where to add the dataset.
- Get a preview, given the above selections.
- Save the show.

The creation of the show and its customizations rely on the expertise of the user and on the case study.

The above options are available in the Data Visualization Service UI.

3.10.1.1 Visualization-ready data

"Visualization-ready" datasets are part of the DESP data specified in [DSP-USR-SDP] and exposed by the Data Visualization Service as part of its service offering (please refer to [RD-21]). This data is already prepared and optimized in advance for the visualization service. This includes geospatial datasets like static maps, layers or interactive timeseries on 2D/3D/4D, given standard data formats (GeoTiff, WMS, WMTS, WCS or GeoJSON). This also includes a 3D-rendering, procedural modelling, and procedural animation capabilities to create highly immersive and engaging experiences.

Geometric (pixel) resolution is optimized to reduce the time required for loading data, by displaying portions of the whole dataset available on 2000x4000 pixel grid. The user can then zoom on higher scales, increasing interactively the resolution on the data portion visualized.

[1] graphical workspace where data is displayed and visualized. It can be the whole Earth (spherical or planar projection), or a portion as selected by the user.

On the other hand, the geographic resolution depends on the dataset visualized (e.g. 10km, 10m, …) thus is not interactively adjustable by users. Projection used is WGS84 (EPSG 4326).

3.10.1.2 "Near" visualization-ready data

(Way forward) The possibility of creating custom shows using user's generated datasets requires an interface with the User Workflow service. User's generated datasets are available upon request via a dedicated API exposed by the User Workflow. This scenario is not covered by the present OCD yet (see also 3.9.1.3 and 3.9.2). *This scenario will be foreseen at later stage*.

3.10.2 Update Visualization scenarios

Any DESP Standard User accessing the Data Visualization service can update the visualization scenario by loading different datasets, according to the available "visualization-ready" dataset options.

Update the show means to retrieve a show (previously saved) or load a local file and:

- Modify or delete layers as needed
- Change the reference dataset, given access to the Data Workflow
- Change the TOI or ROI
- Graphical adjustments like zoom-in or zoom-out the show (automatically managed by the system) on user selected area of interests
- Imagery adjustments as colour scale adjustment, resolution, sub setting, projection, etc.
- Layout adjustments, as visualization type, style, colour scheme, fonts, etc.
- Save the new show or override

3.10.3 Share visualization scenarios

Any DESP Standard User accessing the Data Visualization service and creating a scenario, can share it with other DESP Standard Users in real time. The Visualization system generates a web link upon user request, pointing to the metadata of a user's generated show previously saved. The link provides only read permissions to other users, via the web interface.

3.10.4 Export visualization outputs

Any DESP Standard User accessing the Data Visualization service and creating a scenario, can export the scenario via the web interface and save on local file system.

In doing this, the system automatically generates and downloads on his own device all the information related to the visualized scenario, in a specific file (e.g. PNG, CSV, …) or metadata file (JSON object).

3.10.5 Create Visualization scenarios via API

(Way forward) As an evolution, the Data Visualization Service will expose a REST interface that can be used programmatically to create a show via API from a JSON object.

Selections and customizations on the show are the same of Section 3.10.1, following the specifications given in [RD-21].

Users first export a show as JSON, then they can modify it to build a new show or update an existing one.

3.11 Traceability Services operational scenarios

[design to be consolidated]

3.11.1 Traceability acknowledge

A DESP Registered User can acknowledge the capabilities and conditions to generate, record and validate unique traces in DESP, reading this information via:

- the User Guide of the Traceability Service, exposed by the Web Portal,
- the Traceability Service panel, reported by Service Registry,
- from the Traceability Service Graphical User Interface.

Among the provided information, the following are highlighted:

- Any DESP Registered User can generate unique traces by a dedicated Traceability Client Tool (see dedicated scenario).
- DESP Registered Users need to be authorised to send generated traces to the Traceability Service via a preliminary request to Service Desk, via ticket (selecting 'Traceability' category). Specification concerning the traced item should be provided.
- DESP Registered and Federated Users are enabled to search and check traces using the functions offered by the Traceability Service. The complete list of API endpoints to the Traceability Service is exposed to the user via Swagger mode.

In case of Traceability Service unavailability, it is responsibility of the user to re-send a generated trace file towards the Traceability Service.

3.11.2 Traceability Client Tool management

DESP Registered Users become aware that trace generation can be implemented by a dedicated Traceability Client Tool– released as Open-Source software in a dedicated Open-Source GitHub repository available to them. Each client tool release is accompanied by proper documentation (User Manual, Installation and Configuration Manual, Release Note).

Registered Users can find the link to the GitHub repository in the same interfaces listed in *scenario above*.

After authentication and authorization to the repository, they can download the most recent Traceability Client Tool release directly from the dedicated GitHub repository.

Once the tool is downloaded, they can deploy it on their environment, otherwise they should include it in a new release package of their Service, to be newly deployed into the Runtime Platform following the steps expected for Data Management Service.

3.11.3 Trace generation for DESP data

Any DESP Registered User (and / or Data Management Service) can generate unique traces using the Traceability Client Tool – a deliverable of the Traceability Service.

- In case the data is managed in Data Workflow Services, each Data Workflow Service integrates the Traceability Client Tool in their system to be able to generate/register/sending traces.
- In case the data is generated by the User, the Traceability Client Tool needs to be run at User side to be able to generate traces.
- The complete list of properties and attributes to be included in the trace is reported in the DESP Information Model [RD]. The generated trace should comprehend the following properties and attributes, to be configured by DESP Registered User (see *Table here below)*.

Table 2: Trace Attributes description

Attribute Name	Type	M	Description
serviceContext	string	Y	The context provided by the Traceability Service `Ex: DestinE /Desp`
serviceType	string	Y	The service type as defined by the interface delivery naming (whereby establishing a schema for the relative attributes to be provided along with the trace record) `Ex: Data Workflow Service (see services definitions in DESP SDD & Master ICD), Use Cases, Advanced Services`
serviceProvider	string	Y	The service provides unique identifier `EX: meeo / DESP Consortium/ serco`
eventType	string	Y	`CREATE`: For each new data in DESP, either retrieved from a Data Source or generated by a user, the trace record is created with full set of attributes describing that item . `COPY`: In case of a copy of a data item in a service different from the one that published it, the trace record may be created only as reference to the original item. `DELETE`: In case of a deletion of a data item from the service that published it in the DESP framework, the trace record may be created only as a reference to the original item.
deletionCause	string	N	Mandatory in case of "DELETE" Example: `"Data quality reduced due to incorrect AUX"`
name	string	Y	Product name according to standard naming convention, including file type extension. Ex: `S2B_OPER_MSI_L0__GR_SGS__201`

			`91014T075559_S20191014T05080`
			`6_D09_N02.08.tar`

dataset id	string	Y	Identifier of the Dataset
productType	string	N	Product type of the product Mandatory only for georeferenced data.
size	integer	Y	Product size in bytes (B) EX: `66384556`
origin	string	N	Data Source from which the data has been retrieved. Not present for user generated data.
beginningDateTime	string	N	Sensing date of the product. Mandatory only for georeferenced data.
hash	string	Y	The primary hash of the data being traced, according to the **hash_algorithm** (e.g. as calculated by the Traceability Tool). It corresponds to the entire product package. EX: `1bb4eb2c9570dc6ba723f9e427e9fa07`

hashList	string	N	The hash list array for components of the product (e.g. as calculated by the Traceability Tool). It corresponds to key components within the product package (e.g., image bands).
			Example:
			`[`
			`"/path/file1:61d2eed6b1363af 3de405a9496e4c27d",`
			`"/path/file2:61d2eed6ff363af`
			`3de40999412e4c254"`
			`]`

hashAlgo	string	Y	Hash algorithm. Default hashing algorithm is the SHA-256 algorithm.
Area Of Interest (AOI)		N	Area of interest. Mandatory only for georeferenced data.
Digital Object Identifier (DOI)		N	Unique identifier for a digital object

processorName		N	Name of the software component.
processorVersion		N	Version or release identifier of the software component.

At trace generation, the tool returns a message reporting the outcome in JSON format with the full list of trace metadata including the hash associated to the trace.

Trace generation for Software and Algorithms be foreseen at later stage.

A dedicated API exposed by the Traceability Service allows DESP Registered Users to interface with Traceability Service and push trace records. The User configures this endpoint into the Traceability Client Tool, so that the generated trace (in JSON format) is pushed towards the Traceability Service.

Please note that trace creation and pushing does not affect any publication process in charge of Data Workflow Services, and products whose trace creation failed can be exposed via catalogue.

3.11.4 Trace ingestion and publication

The trace pushed by DESP Registered User is syntactically verified by the Traceability Service, including verification of the service type, provider, all mandatory parameters, and full set of properties schema.

The trace is indexed (i.e, a unique identifier is assigned by the Traceability Service) and stored in the Traceability Service DB. Please note that no rolling of trace records is foreseen in DESP for traces relevant to Data Cache Management Service and MEEO'S Data Workflow Service.

DESP Registered users, Services not belonging to the Consortium Storing traces in the Traceability Service belongs to the Service Usage Profile, so it is not free.

As output of this scenario, traces are exposed via DESP Traceability Service on both Service API and GUI.

3.11.5 Trace search and verification

DESP Registered Users, Data Management Services and Federated Users can access the Traceability Service (via API and UI) to search for all available traces. Traces can be searched using the following properties:

- Product name
- Hash
- Publication Date

The Traceability Client Tool is able to calculate the hash of an item, either generated by users themselves or exposed by a DESP Services integrated with the Traceability Service.

The verification can be performed comparing the hash computed by the Tool with the hash of the traced item in the Traceability Service catalogue. This can be done for items for which the trace generation and recording was successful.

3.12 Infrastructure operational scenarios

3.12.1 Cloud Resources purchasing

This scenario describes how different category of users interacting with DESP can purchase Cloud Services.

DESP Standard Users

DESP registered Standard Users can select the OVHcloud Service among the services catalogued on the DESP Service Registry. OVHcloud is a federated service of DESP, thus DESP Registered users access the OVHcloud Service with his/her DESP credentials.

Via Service Registry, users can click on a button that automatically open a ticket in the Ticketing System, for the creation of an OVHcloud Public Cloud Project. The Service Desk is notified and verifies if the user's wallet has sufficient credit for the requested action. If so, the Service Desk creates the Project.

Once the operation is successfully finished, the ticket is closed and this automatically trigger an email sending with a standard text, informing the user of the successful project creation.

Using DCUs, DESP Standard users can buy Cloud Services, listed in [AD-8], ensured by the OVHcloud Cloud Infrastructure layer:

- Computing Instances
- Storage
- Network
- Database
- Containers
- Data and AI

Cloud Services management is a service available via OVH Public Cloud APIs [RD-10] or on the GUI of the OVHcloud Public Cloud Project associated with the user and provides the list of available services with their prices.

The price of OVHcloud Services used by a DESP registered user is billed by the DESP *Billing System*.

A user shall have available credits in his/her wallet before purchasing an OVHcloud service. *[The joint accounting functioning is under discussion].*

DESP tenant technical administrator

DESP tenant admin functionalities cover the ones of the DESP Standard users, and moreover he/she can:

- he/she can create more than one OVHcloud Public Cloud Project,
- he/she can invite and assign tenant members to specific OVHcloud Public Cloud Projects among the ones he/she created.

DESP tenant member

DESP tenant member is a Standard User allowed to access:

- His/her personal OVHcloud Public Cloud Project – if any;
- The OVHcloud Public Cloud Projects he/she is assigned to.

Please note that the accessibility of the Cloud Project is determined by the User current “context” (Section 3.4.5).

DESP service providers

DESP Service Providers can consume OVH resources in two ways (not mutually exclusive):

- They can access DESP computing resources in form of containers orchestrated on a Kubernetes-based platform (the Runtime Platform), when this is agreed with DESP (Serco) under a contract. In this case, the contract defines their interface to use the resources, the DESP runtime platform and the cost of the infrastructure. The consumption of the resources is monitored and billed by the DESP platform itself (invoiced as ‘Runtime Platform consumption’).
- As a DESP registered users, the Service Providers can own a personal OVHcloud Public Cloud Project. Here he/she can purchase OVH Cloud Services. The consumption of the resources is monitored and billed by the DESP platform itself (invoiced as ‘OVH Cloud Services consumption’).

Please note that a Service Provider whose services are hosted on the Runtime Platform can use smoothly OVH Cloud Services hosted on his/her Project – being the Projects in the same OVH Cloud account (Serco/ESA Account).

Annex 1. Identity and Access Management Overview

See “DEST-SRCO-TN-2300330_Annex1 - IAM Service Overview” [RD-7].

Annex 2. Definition for Dashboard Services

See "DEST-SRCO-TN-2300330_Annex2 – Definitions for Dashboard Services"