Service Delivery Team Onboarding and Service Delivery Guide

dsf.dmrid.gov.cy/2024/10/17/service-delivery-team-onboarding-and-service-delivery-guide/

> *Version 1.5*

Version control table

Version	Date	Comments
0.1	20/10/2022	Initial Draft
1.0	22/11/2022	Published Document
1.1	12/09/2023	**Amendments** – Updated Introduction – Updated Onboarding Stage – Updated Development Process – Updated Going Live – **Added** Service fixes and iterations – **Added** README file link – **Added** CHANGELOG file link
1.2	09/02/2024	**Amendments** – Updated Development Process – Updated Data Access and Storage Requirements – Updated Appendix A – Service Delivery Quick Check List
1.3	23/05/2024	**Amendments** – Updated Testing Process – Updated Assurance Process
1.4	20/09/2024	**Amendments** – **Added** Security and Risk Management – **Added** Repository Access
1.5	17/10/2024	**Amendments** – Updated Authentication Requirements – Updated Notification (SMS & Email) Requirements – Updated Payment Requirements – Updated Data Access and Storage Requirements – Updated DSF Architecture

Table of contents

Introduction

The purpose of this guide is to explain all the necessary actions that need to be taken and prerequisites that have to be met by a **service delivery team** to collaborate, develop and deploy a new service or a 'bucket' of services on the **DSF infrastructure** (currently an Azure AKS Cluster) using the **DSF Service Standard** and **DSF Design System** along with the actions to be taken concerning service fixes and iterations. A **Service Delivery Team** could be either an internal team (within the Government of Cyprus) or an external vendor (A private company collaborating with a Government Ministry/Department bound by a **Framework Agreement for the Digital Transformation of Government Services** or by any other type of a government contract. The process of onboarding a service delivery team to successfully deliver a service or a 'bucket' of services is described in detail in the sections that follow.

The process of delivering a Service, in this document, is read as the "project".

Project Initiation Process

Onboarding Stage

Before the implementation of the service, the Project Manager of the Contracting Authority shall fill in a **Service Delivery Initiation Form (Version 1.2)** for each service/iteration to be delivered. This form contains service basic technical information

along with the targeted outcome (outcome-based approach).

All communication between the DSF Tech Team and the Service Team shall be initiated exclusively by a Governmental Technical Officer (Solution Integration Officer) and the technical DSF team. In the event of the absence of a Technical Officer, the role shall be assumed by the Project Manager. The email account dsf-tech@dits.dmrid.gov.cy will serve as the designated point of contact for the Tech Support Model.

The onboarding stage shall be initiated by a meeting of all stakeholders. If needed, other meetings can follow to communicate the goals of the project and identify the service's boundaries by all parties involved.

Initiation Stage

Following the onboarding stage described above, the **Service Architecture Document** shall be submitted by the Project Manager of the Contracting Authority to be reviewed by the Digital Services Factory (DSF) Team. A formal response by DSF shall be communicated back to all involved parties with an initial draft of a **Service Delivery Roadmap**.

A **kick-off meeting** between the DSF Team and the Service Delivery Team shall be arranged by the Project Manager of the Contracting Authority, to officially initiate the project. Any issues, problems and clarifications will be discussed to align all involved parties with the goals. An agile project management approach shall be used with sprint goals defined. Members from both teams, the DSF Team and Service Delivery Team shall participate as needed in agreed meetings to resolve possible issues.

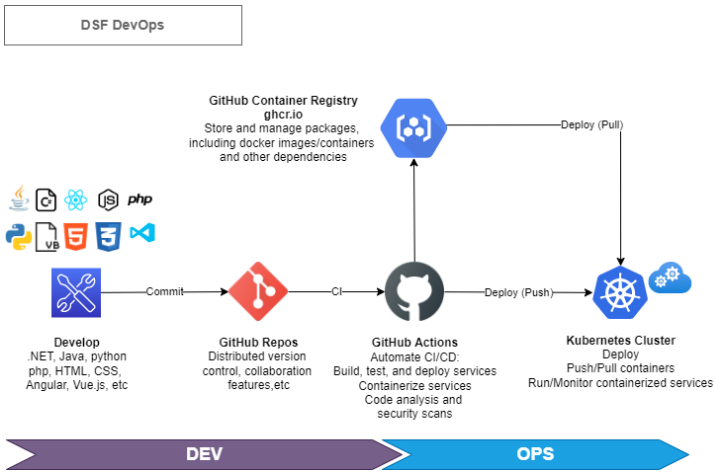
Service Workflow Process

The service shall undergo the following workflow process as per the **Service Standard**; Service Design, User Research, Content Design etc.

Using the DSF Infrastructure

Development Process

All development and deployment processes shall be done using the DSF Infrastructure.



Development Process using the DSF Infrastructure

Diagram 1.1

The source code of the service must be uploaded along with the relevant documentation (**README file**) and will be maintained on a per-project pre-specified **DSF Github Source Repository**. Access shall be granted to the Service Delivery Team's member(s) upon request.

CI/CD Pipeline

A per-service DSF **CI/CD pipeline** shall be configured and run to test, build and store the service container image in the DSF's **Github Container Registry** (**ghcr.io,** *see Diagram 1.1).* It is the responsibility of the Service Delivery Team to have a successful build of the project as a container image using a Docker file in the root folder of the repository.

The service shall be deployed on the DSF's **Azure Kubernetes Service (AKS) cluster**, initially on the DSF's Infrastructure Staging Environment, using a configuration script (number of pods, # of vCpu, RAM etc., performance and CPU intensity info shall be needed to be provided from the service team's part to size the pods appropriately).

Later, during the ***testing process*** ***(see. the Testing Process section in this document)***, a performance and analytics tool shall be used to better assist with the final sizing of the service pods (A "Pod" is a service instance that runs on the AKS cluster; A service can have more than one pod running for high availability and performance).

Authentication Requirements

If Citizen/User authentication is required by the service, authentication requirements shall **ONLY** be fulfilled through **CY Login** authentication service using the CY Login access token to access the required data.

Notification (SMS & Email) Requirements

If citizen notification (either by email or by sms) is required by the service, Notification requirements shall **ONLY** be fulfilled through **CY Notification**. To use the Notification Service, a "Notification Client Account" (provided by the CY Login Team) is required for each deployment environment (Production and Development).

Payment Requirements

Citizen payment requirements shall **ONLY** be fulfilled through **CY Payment**. To use the Payment Engine, a "Payment Client Account" (provided by the CY Login Team) is required for each deployment environment (Production and Development).

Data Access and Storage Requirements

Any data access or data storage requirement shall be handled by the service delivery team's end, using or developing a backend API (shall be developed by the Service Delivery Team or by the Backend's Support Team based on the requirements scoped for the service) and shall be exposed to CY Connect for the service to have access to. The DSF API Standard must be followed when developing the service api.

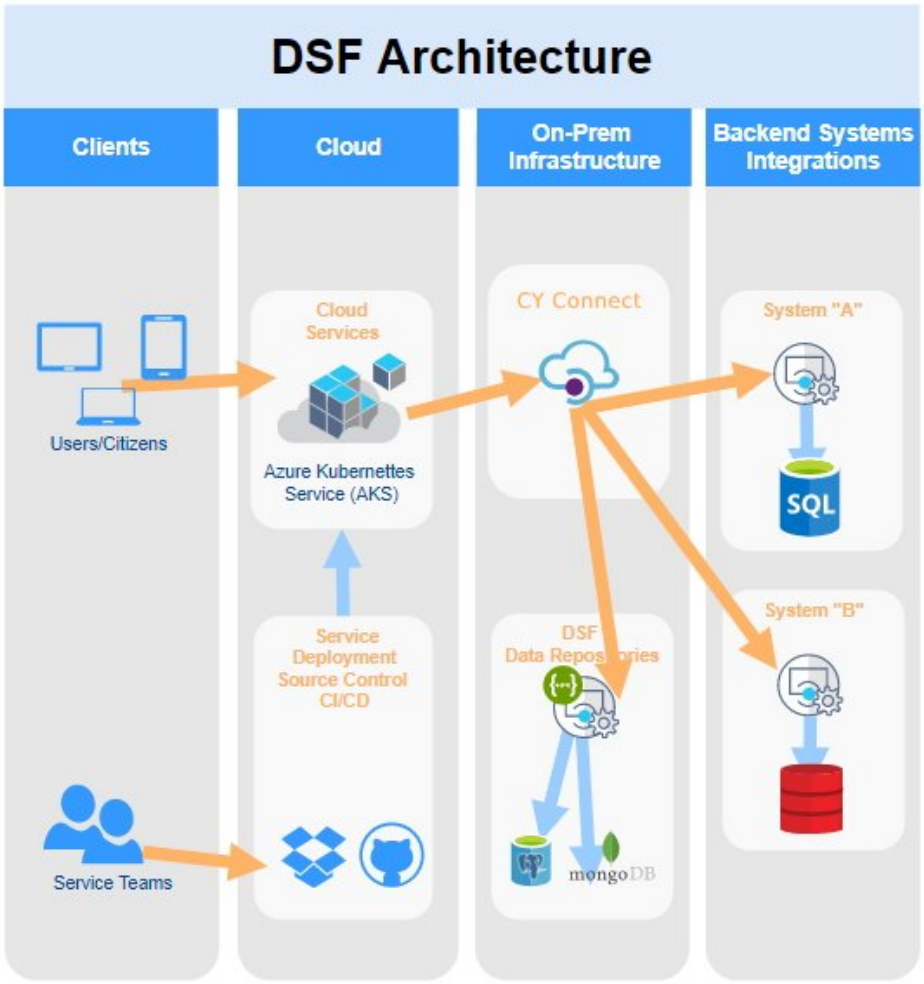


Diagram 1.2

Domain Name Registration Process

A **service name** shall be provided to the DSF tech team to register the Domain Name of the service. All DSF-hosted services shall have qualified names under these two domains:

1. **<service_name>.service.gov.cy** for the production, ie.***do-a-thing.service.gov.cy*** and

2. **<service_name>.staging.service.gov.cy** for the staging environment, ie. ***do-a-thing.staging.service.gov.cy***

For naming the service and the service's end-point URLs please refer to the "Service name and URLs" section of the 'Content Design Standards for Services.

Testing Process

Testing shall be conducted by the Service Delivery Team as needed on the DSF's Staging Environment (**DSF-SE**). It is the service team's responsibility to conduct all necessary tests including **UAT** (User Acceptance Test), unit tests, performance and load/stress testing. A **WASA** (Web Application Security Assessment) should also be conducted before the service is sent to DSF for Quality Assurance assessment. The WASA must be performed by an independently certified penetration (PEN) tester, preferably with relevant experience. The PEN Testing results report shall be disclosed along with the **Data Protection Impact Assessment** (**DPIA**) report to the Personal Data Protection Commissioner.

When all the necessary tests are performed successfully, the service shall be available for the quality assurance assessment.

Assurance Process

The service shall undergo the DSF assurance process to proceed with the deployment process.

Deployment Process

The deployment of the service to the DSF Production environment is done by the DSF Tech Team. The DSF Tech team shall be informed, by the service delivery team within a reasonable period of time prior to deployment of the service, on the date and time the service should be published.

Going Live

It is recommended when the service goes into production, a 'controlled release', usually a week's duration, is introduced. The 'controlled release' precedes the full 'going live' phase and it is a non-advertised production use of the service by a pre-selected group of users/citizens that are eligible to use it to test the whole end-to-end process in the actual production environment. All citizen's applications/requests during this phase shall be officially processed and all the outcomes shall be considered valid. After an assessment of all outcomes of the "controlled release" by the service team, the service shall be advertised and published on the "gov.cy" portal for full public access.

Security and Risk Management

Managing vulnerabilities is crucial for the security of DSF infrastructure. The service owner is responsible for identifying and resolving vulnerabilities in the GitHub repository. Dependabot is a GitHub tool that automatically monitors and updates libraries and dependencies in your project to ensure they remain current and secure.

Critical vulnerabilities must be addressed within the timeframe indicated in the table below. The issue will be escalated if the service owner fails to address these vulnerabilities within the specified timeframes. The escalation will involve immediate notification to the DMRID security team to ensure swift action is taken. This escalation process ensures that security issues are addressed promptly.

Timeframe table for vulnerability resolution:

Vulnerability Severity	Timeframe for resolving
Critical/High	Within 30 days of initial detection
Medium	Within 60 days of initial detection
Low	Within 90 days of initial detection
Informational	No specific deadline unless defined

Project Closure

Project closure is reached when all project requirements are met including receiving the final “Service Standard Verified” seal.

Service fixes and iterations

Any service fixes/iterations performed by the service team shall be communicated to the DSF Team by the Project Manager of the Contracting Authority.

The Project Manager of the Contracting Authority shall request a redeployment of the updated service by providing adequate documentation with reference to the **Assessment Report Number** of the service and describing all new service fixes/iterations performed on the service (an updated service **CHANGELOG** file shall also be included in the request). Upon reviewing the request, the DSF Assurance team shall respond with a direct order for re-deployment or with a request for a new service assessment. In the case of the latter, the order for re-deployment shall be given based on the assurance result.

After acceptance from the Contracting Authority of any service fixes/iterations issued by the service team, they shall be communicated to the DSF Team (dsf-qa@dits.dmrid.gov.cy) via the Project Manager of the Contracting Authority.

The Project Manager of the Contracting Authority must send the files, including a ***CHANGELOG*** file for documentation on the bugs/fixes/the iterations, to the DSF Assurance Team. The DSF Team will handle each request accordingly and decide whether a new assessment is required before deploying the fixes/iterations of the service. The deployment procedure is as described in the Deployment Process above.

Repository Access

Additionally, the service owner must notify DSF (dsf-tech@dits.dmrid.gov.cy) to release the associated GitHub licenses, in case there is a change regarding the repository access of suppliers and/or other stakeholders to ensure continuous compliance and protection.

Appendix A

Service Delivery Quick Check List

1. **Obtain CY Login / Notification/ Payment Engine accounts from the CDS Team (DITS) (if applicable)**
   The Project Manager (Contracting Authority) shall contact the CDS team at DITS via email to: *cds-support@dits.dmrid.gov.cy*.

2. **Obtain Access to the Service GitHub Repository**
   A GitHub repository for the service shall be created by the DSF Tech team. A corporate email address shall be provided by the service team (internal or external supplier).

3. **Upload initial code to the GitHub repository**
   The service team shall upload the initial source code as the first version to the service GitHub repository.

4. **Provide a Service Domain Name**
   A service name must be provided by the service team and communicated to the DSF tech team via email for the registration of the Domain Name of the service. For more details on how to name a service, please refer to the Service Delivery Team Onboarding and Service Delivery Guide under the Domain Name Registration Process.

5. **Service Secrets**
   The service delivery team shall provide the DSF tech team with a text file containing secrets eg. "*appsettings*","*.properties*", *CY Login settings* and *connection endpoints*, or any other sensitive information. (explain how it is used)

6. **Service Access to Backend and/or Other API (s)**
   The DSF tech team in collaboration with the service delivery team and Government Unified Network (GUN) team at DITS (via email noc@dits.dmrid.gov.cy) will set up network access from DSF Infrastructure to backend Service API(s). Additionally, the DSF technical team, in collaboration with the service team, will configure the API Gateway. This gateway will function as a reverse proxy, enabling access through it, to the backend API services.

7. **Use of Gov On-Prem Web Analytics Platform**
   The DSF technical team, in collaboration with the supplier, will integrate Matomo web analytics by embedding the JavaScript Tracking Code, including a unique '*idsite*', into the service. This integration aims to collect data for Key Performance Indicator (KPIs) purposes. In addition, the team will provide access to the Service Owner via email to monitor Matomo web analytics data.

8. **Dockerize your service for the Initial DSF Staging Environment Deployment**
   It is the responsibility of the service delivery team to have a successful build of the project as a container image using a *Dockerfile* in the root folder of the repository. In addition, the DSF tech team in collaboration with the service delivery team will create workflow actions in the above repository to deploy the service to the Staging environment. After this step, each commit on the GitHub repository will automatically push the image to Staging.

9. **End-to-end Integration Connectivity Testing**
   End-to-end integration Connectivity Testing ensures the seamless interoperability of various system components by evaluating connectivity and communication. This essential testing phase verifies that the integrated elements collaborate effectively, guaranteeing a robust and cohesive end-to-end system.

10. **README file**
    It is the responsibility of the supplier to create a README file in the root folder of the repository. For more details check on *About the README file*.

11. **CHANGELOG file**
    It is the responsibility of the supplier to create a README file in the root folder of the repository. For more details check on *About the CHANGELOG file*.

12. **Test the Service**
    Testing shall be conducted by the service delivery team as needed on the DSF's Staging Environment. It is the service delivery team's responsibility to conduct all necessary tests UAT/Pen Test/Functional/Non-Functional etc.).

13. **Pass DSF Assurance**
    The service shall undergo the DSF assurance process to proceed with the deployment process.

14. **Deploy to Production**
    The deployment of the service to the DSF Production environment is done by the DSF Tech Team. The DSF Tech team shall be informed by the Project Manager (Contracting Authority) within a reasonable period before deployment of the service, on the date and time the service should be published.