IT MODERNISATION RECOVERY INCREMENT 1

WP07 - SYSTEMS INTEGRATION AND CORE CAPABILITIES

INTERFACE DEFINITION DOCUMENT

ITM IDD DLP DISCOVERY

Effective date.....: 27-Jun-23
Version No .....: 1.0
Issued by.....: ITM-RC1 Programme Office
Approved by .....: Martin Diepstraten, POLARIS TDA

Document Control

Title:	Interface Definition Document (IDD)
Version:	1.0
Date:	27-Jun-23
Classification:	NATO UNCLASSIFIED
Filename:	NU-ITMRC1-IDD DLP Discovery

Table of Amendments

Version	Date	Description
1.0	27 Jun 23	Initial release.

Stakeholders Details

Role	Name	Signature
Author	Sander Oudkerk, sander.oudkerk@ncia.nato.int, Chief Technology Office	Sander Oudkerk Digitally signed by Sander Oudkerk Date: 2023.06.27 15:19:54 +02'00'
Reviewer	Kemal Utkuel, Kemal.Utkuel@nr.ncia.nato.int, ITM-RC1 Project Architect	Kemal Utkuel Digitally signed by Kemal Utkuel Date: 2023.06.27 15:30:31 +02'00'
Approver	Martin J. Diepstraten, Martin.Diepstraten@ncia.nato.int, Polaris Technical Design Authority	Martin Diepstraten Digitally signed by Martin Diepstraten Date: 2023.06.29 10:18:31 +02'00'

Contents

List of Figures

List of Tables

1. OUTLINE SERVICE DESCRIPTION

0001 **Service Name:** DLP[1] Discovery.

0002 **Service Hierarchy:** DLP Discovery is composed of a management and technical service.

A. The technical service maps to the following parents in the C3 Taxonomy:
   - Core Services/Platform Services/Policy Enforcement Point Services/Policy Decision Point Services;
   - Core Services/Platform Services/Policy Enforcement Point Services/Policy Enforcement Point Services.

B. The management service maps to Core Services/Platform Services/Policy Enforcement Point Services/Policy Administration Point Services.

C. Within the ON Services hierarchy (see Architecture Documentation Package (ADP) Section 3.2) DLP Discovery is a cyber security service that falls under Client Provisioning (CPS) Cyber Security Services ON.

0003 **Service Architecture Building Block (ABB) reference**: See the overview of 'NATO ON Cyber Security Services' in Figure 3-49 in the ADP.

0004 **Service Solution Building Block (SBB) reference:** Not available (N/A).

0005 **Outline description of the service:** DLP Discovery is composed of three services:

A. Technical service 'Data-at-Rest Discovery Service'. This service offers the following operations:
   - Scan resources on a network to locate data;
   - Classify data according to classification[2] criteria;
   - Index data;
   - Subject data to protection policies;
   - Alert when data is violating a protection policy.

   For a subset of the operations 'Data-at-Rest Discovery Service' will make use of agent embedded on endpoints.

B. Application service 'Data-at-Rest Discovery Management Application Service'. This service offers the operations to:
   - Control 'Data-at-Rest Discovery Service';
   - Configure criteria for data classification;
   - Create protection policies and track policy violations;
   - Query and mine indexed data;
   - Report.

C. Business[3] service 'Data-at-Rest Discovery Management Service'. This service configures and operates the technical service 'Data-at-Rest Discovery'. It makes use of the application service 'Data-at-Rest Discovery Management Application Service'.

0006 DLP Discovery is a cyber security service that contributes to the enforcement of 'Data Loss Prevention' (DLP). Within the NATO Enterprise a number of NCI Agency catalogue services are involved in the enforcement of DLP. NCI Agency catalogue service SEC012 provides support (subject matter expertise; 3rd line support) for the catalogue services that enforce

[1] DLP is the abbreviation of 'Data Loss Prevention', however the service is referred to using the abbreviation DLP.
[2] The term 'classification' is used in the broad sense of the meaning of assigning data to different data categories based on criteria that can be set by the organization. Classification of data into data sensitivity categories, e.g. NU and NR, is an example of the more general 'classification'.
[3] In this document the term 'business service' is used as it is defined in the Archimate language.

DLP. The decomposition of DLP Discovery, and expected service context, is shown in Figure 1.

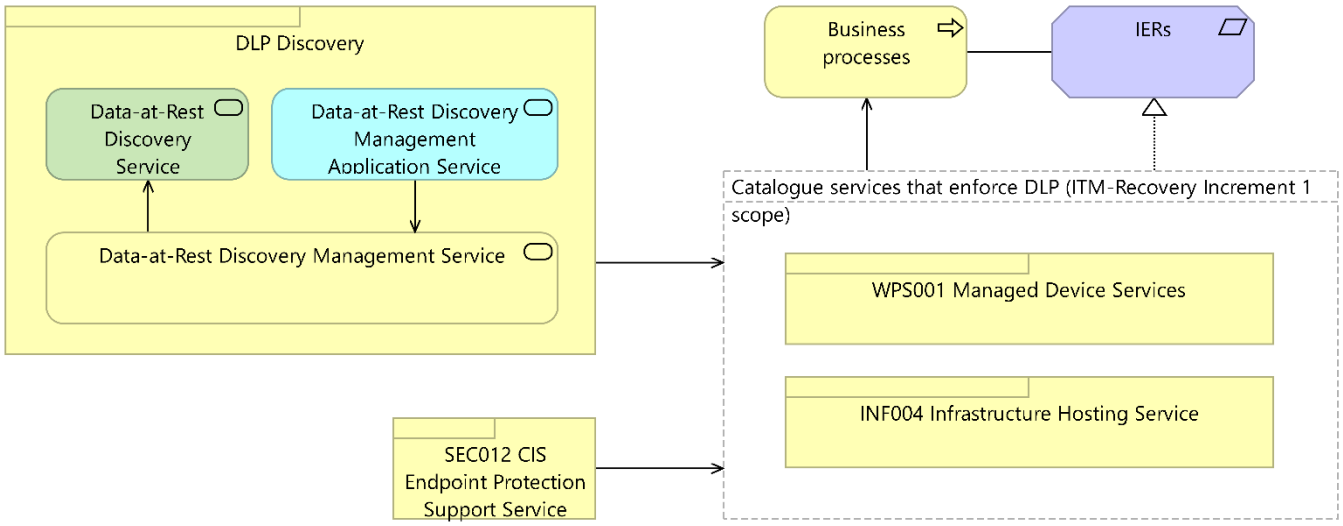

Figure 1 – Decomposition of DLP Discovery

0007 'Data-at-Rest Discovery Service' covers the ITM Operational Network (ON). It can scan for data, locally and over the network, and accesses file shares, databases, and SharePoint portals.

0008 'Data-at-Rest Discovery Service' has the following dependent services in the ITM Operational Network:

0009 C3 Taxonomy Services

A. Domain name services;
B. IPv4 Routed Access Services;
C. IPv6 Routed Access Services;
D. Infrastructure Storage Services;
E. Infrastructure Processing Services;
F. Database Services;
G. Information Platform Services;
H. Web Platform Services;
I. ON Cyber Security Services:
   - Enterprise Logging Service;
   - Privileged Access Management (PAM) Service.

0010 Figure 2 shows the services that 'Data-at-Rest Discovery Service' depends on and the interfaces it requires.

0011 The operations implemented by 'Data-at-Rest Discovery Service' are executed over the network for servers and involve a local agent for scanning of client file systems. The server scans require credentials.

0012 The results of the operations are collected at two provided logical interfaces as shown in Figure 2: one interface is dedicated to data discovery on clients, and one to data discovery on servers[4]. This distinction is made in order to be able to – per client and server - distinguish

[4] According to the ADP, for ITM Recovery Increment 1 the scope of DLP Discovery for the NATO ON is limited to servers.

between the interfaces and services that DLP Discovery depends on. The interface IDs are specified in Section 2.1, as well as a number of additional logical sub-interfaces per type of server.

0013 The service ‘Data-at-Rest Discovery Management Application Service’ is used by ‘Data-at-Rest Discovery Management Service’ and exposes two interfaces ‘Data-at-Rest Discovery Management Application Service – interface’, one for the management of DLP Discovery on servers, and one for clients. The interface IDs are specified in Section 2.1.

0014 ‘Data-at-Rest Discovery Management Application Service’ is used to configure, query, or instruct ‘Data-at-Rest Discovery Service’ to run operations. The communication between ‘Data-at-Rest Discovery Management Application Service’ and ‘Data-at-Rest Discovery Service’ is considered internal communication and is not specified further.

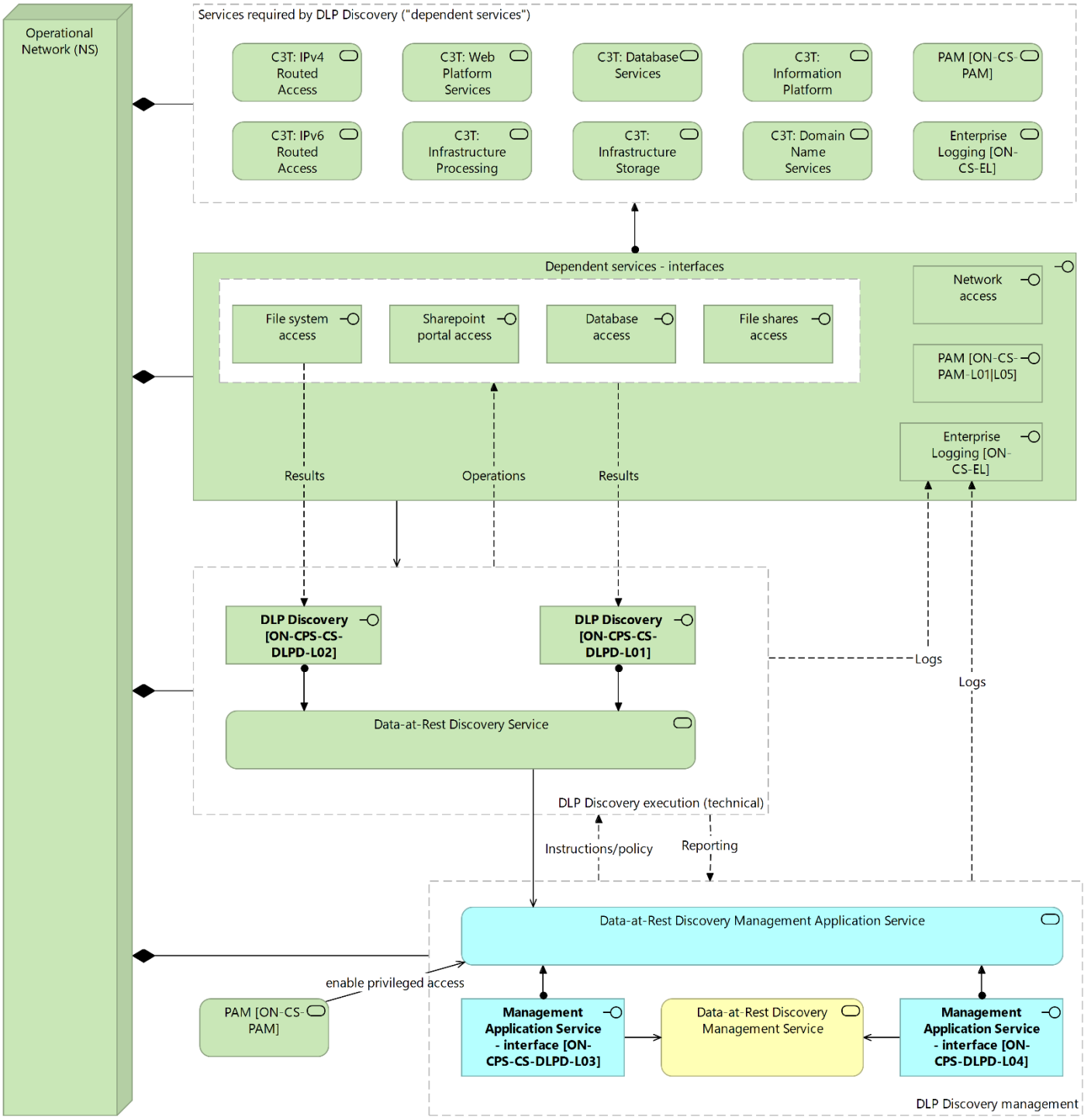

Figure 2 – Provided/dependent interfaces and services of 'Data-at-Rest Discovery Service'

2. PROVIDED INTERFACES

2.1. List of interfaces

0015 This section lists all interfaces that the building block provides.

Interface ID	Full name	Related sub service	References
ON-CPS-CS-DLPD-L01	Data-at-Rest Discovery results collection interface for servers – general interface	Data-at-Rest Discovery Service for servers	Section 2.2
ON-CPS-CS-DLPD-L02	Data-at-Rest Discovery results collection interface for clients	Data-at-Rest Discovery Service for clients – local file system	Section 2.3
ON-CPS-CS-DLPD-L10	Data-at-Rest Discovery results collection interface for servers	Data-at-Rest Discovery Service for servers – local file system	Section 2.2
ON-CPS-CS-DLPD-L11	Data-at-Rest Discovery results collection interface for servers	Data-at-Rest Discovery Service for servers - SMB/CIFS file shares	Section 2.2
ON-CPS-CS-DLPD-L12	Data-at-Rest Discovery results collection interface for servers	Data-at-Rest Discovery Service for database servers	Section 2.2
ON-CPS-CS-DLPD-L13	Data-at-Rest Discovery results collection interface for servers	Data-at-Rest Discovery Service for SharePoint portals	Section 2.2
ON-CPS-CS-DLPD-L03	Data-at-Rest Discovery Management Application Service - interface	Data-at-Rest Discovery Management Application Service for clients	Section 2.3
ON-CPS-CS-DLPD-L04	Data-at-Rest Discovery Management Application Service - interface	Data-at-Rest Discovery Management Application Service for servers	Section 2.5

Table 1 – All provided interfaces

2.2. ON-CPS-CS-DLPD-L01: Collection of results at servers

2.2.1. Operations

0016 ON-CPS-CS-DLPD-L01 provides over the network collection of results from Data-at-Rest Discovery operations at servers. Depending on the server, sub-interfaces are distinguished below:

A. ON-CPS-CS-DLPD-L10: Discovery of data on servers' local file system;
B. ON-CPS-CS-DLPD-L11: Discovery of data on SMB/CIFS file shares;
C. ON-CPS-CS-DLPD-L12: Discovery of data on database servers;
D. ON-CPS-CS-DLPD-L13: Discovery of data on SharePoint portals.

2.3. ON-CPS-CS-DLPD-L02: Collection of results at clients

2.3.1. Operations

0017 ON-CPS-CS-DLPD-L02 provides collection of results from Data-at-Rest Discovery operations at endpoints (clients).

0018 The result collection interface is part of a local agent embedded on the endpoints (clients).

2.4. ON-CPS-CS-DLPD-L03: Service administration for clients

2.4.1. Operations

0019 Description: ON-CPS-CS-DLPD-L03 offers the operations to manage and control DLP Discovery for clients. It offers the following operations:

A. Control 'Data-at-Rest Discovery Service', i.e. instruct 'Data-at-Rest Discovery Service' to:
   A.1. Scan resources on the local file system to locate data;
   A.2. Classify data according to classification criteria;
   A.3. Index data;
   A.4. Subject data to protection policies;
   A.5. Alert when data is violating a protection policy.
B. Configure criteria for data classification;
C. Create protection policies;
D. Track policy violations;
E. Query and mine indexed data;
F. Generate reports.
G. Maps to IERs:

0020 DLP Discovery is part of the enforcement of DLP, see paragraph 0006. DLP Discovery contributes to the overall goal of ensuring that the NCI Agency services can operate at the service level that is required to properly support the business processes and associated IERs.

2.5. ON-CPS-CS-DLPD-L04: Service administration for servers

2.5.1. Operations

0021 Description: ON-CPS-CS-DLPD-L04 offers the operations to manage and control DLP Discovery for servers. It offers the following operations:

A. Control 'Data-at-Rest Discovery Service', i.e. instruct 'Data-at-Rest Discovery Service' to:
   A.1. Scan resources on servers in the network to locate data;
   A.2. Classify data according to classification criteria;
   A.3. Index data;
   A.4. Subject data to protection policies;
   A.5. Alert when data is violating a protection policy.
B. Configure criteria for data classification;
C. Create protection policies;
D. Track policy violations;
   D.1. Query and mine indexed data;
   D.2. Generate reports.
E. Maps to IERs:

0022 DLP Discovery is part of Data Loss Prevention which is used by a number of catalogue services, see Figure 1. DLP Discovery contributes to the overall goal of ensuring that these services can operate at the service level that is required to properly support the business processes and associated IERs.

3. DEPENDENT SERVICE INTERFACES

0023 This section lists all interfaces of services that the building block depends on. The technical detail is provided in the dependent service interface definition.

Interface ID	Description	References
ON-ECS-Web-L01	Required by 'Data-at-Rest Discovery' to run its operations on data located on SharePoint portals.	ECS SDP
ON-ECS-DB-L0*	Required by 'Data-at-Rest Discovery' to run its operations on data located in databases.	ECS SDP
ON-Infra-Proc-L01 and ON-Infra-Stor-L02	Required by 'Data-at-Rest Discovery' to run its operations on data located on file shares.	IDT and IaaS SDP
ON-Infra-Stor-L02	Required by 'Data-at-Rest Discovery' to run its operations on data stored locally on network resources (and not made available via file sharing).	IDT and IaaS SDP
ON-Infra-NETW-L04	Required by 'Data-at-Rest Discovery' to run its operations on data located on resources in the network.	IDT and IaaS SDP
ON-CS-EL	Required by 'Data-at-Rest Discovery' and by 'Data-at-Rest Discovery Management Application' to log cyber security relevant events and alerts.	Enterprise Logging IDD.
ON-CS-PAM-L01	PAM Service interface – Session Proxy	PAM IDD.
ON-CS-PAM-L05	PAM Service interface – Track & Secure Privileged Accounts	PAM IDD.

Table 2 – Dependent service interfaces