IT MODERNISATION RECOVERY INCREMENT 1

WP07 - SYSTEMS INTEGRATION AND CORE CAPABILITIES

INTERFACE DEFINITION DOCUMENT

ITM IDD DATA DIODE AS A SERVICE

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 Data Diode as a Service

Table of Amendments

Version	Date	Description
1.0	27 June 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 15:17:14 +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 15:29:34 +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 10:08:40 +02'00'

Contents

1. OUTLINE SERVICE DESCRIPTION 4
2. PROVIDED INTERFACES 11
2.1. Low Domain Proxy interface operations 12
2.1.1. Outline description 12
2.1.2. Transfer of files via file sharing (L31) 13
2.1.3. Transfer of data over UDP (L32) 13
2.1.4. Transfer of data over TCP (L33) 14
2.1.5. Transfer of data over HTPP(S) and REST (L34) 14
2.1.6. Transfer of e-mail (L35) 14
2.2. High Domain Proxy interface (ON-CS-DD-L03) operations 15
2.2.1. Outline description 15
2.2.2. Transfer of files via file sharing (L31) 15
2.2.3. Transfer of data over UDP (L32) 15
2.2.4. Transfer of data over TCP (L33) 16
2.2.5. Transfer of data over HTPP(S) and REST (L34) 16
2.2.6. Transfer of e-mail (L35) 16
2.3. Interface ON-CS-DD-L04 operations 17
2.3.1. Management and configuration 17
3. DEPENDENT SERVICE INTERFACES 18

List of Figures

Figure 1 – Decomposition of DDaaS into three main services 5
Figure 2 – Interconnection diagram 'Data Diode Service' 6
Figure 3 – Data Flow DDaaS 7
Figure 4 – Management and log collection of 'Data Diode Service' 8
Figure 5 – Breakdown of 'Data Diode Service' 9
Figure 6 – Interface IDs for the Operational Network (ON) 10
Figure 7 – Interface IDs for the low domain CISs 10

List of Tables

Table 1 – All provided interfaces 12
Table 2 – Dependent service interfaces 18

1. OUTLINE SERVICE DESCRIPTION

0001 **Service Name:** Data Diode as a Service (DDaaS).

0002 **Service Hierarchy:** Within the ON services hierarchy DDaaS falls under 'Cyber Security Services ON', see Section 3.2 in the Architecture Documentation Package (ADP). DDaaS is composed of management and technical services. The technical services (i.e. data diode and firewall service) map to two parents in the C3 Taxonomy:

A. Core Services/Infrastructure Services/Infrastructure CIS Security Services/Infrastructure Guard Services; and

B. Communications Services/Communications Access CIS Security Services/Network Firewall Services.

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:** DDaaS will be offered as a service flavour of catalogue service SEC011 (Gateway Security Service). DDaaS is composed of three main services:

A. Technical service 'DDaaS – Low-to-High One-way Data Transfer', **in short 'Data Diode Service'**: this service provides one-way data transfer between the low domain (i.e. a domain of lower trust or classification) to a high domain (i.e. a domain of higher trust or classification with respect to the low domain). The one-way data transfer is enforced by a hardware diode component. Services are mediated between the low and high domain by proxy servers and firewalls, both realizing the 'Data Diode Service'

B. Business[1] service 'DDaaS - System management': centralized management of the IT systems that realize the technical service 'Data Diode Service'. The service 'DDaaS - System management' is supported by the 'Firewall management service' (part of SEC011);

C. Business service 'DDaaS – Service management': ensures 'Data Diode Service' can be offered at the right service level. This includes capacity management, procurement and deployment of the systems and software that realize DDaaS, but also tracking O&M costs of DDaaS.

0006 DDaaS supports a number of business (or operational) processes that have information exchange requirements (IERs) based on one-way data transfer from a low to a high domain.

0007 The decomposition of DDaaS is shown in Figure 1.

[1] In this document the term 'business service' is used as it is defined in the Archimate language.

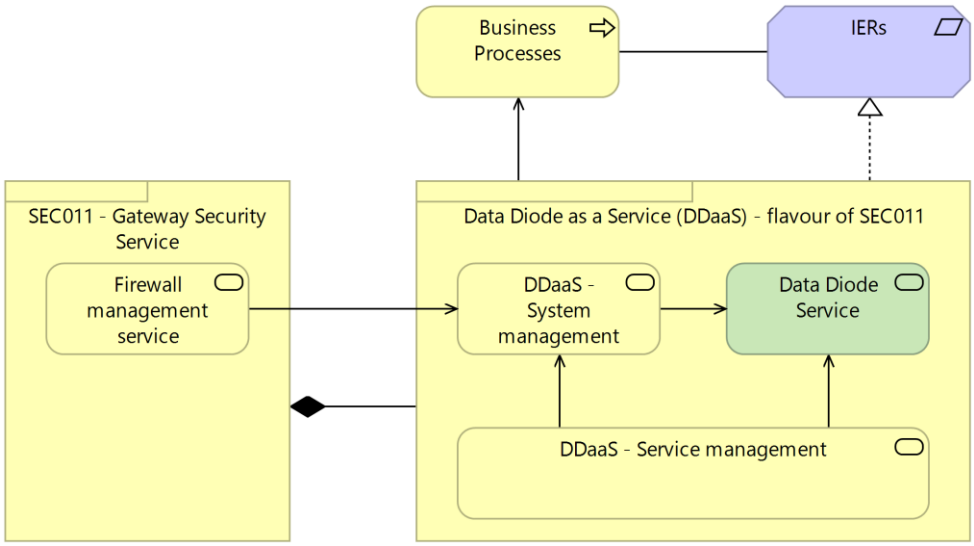

Figure 1 – Decomposition of DDaaS into three main services

0008 DDaaS is a flavour of SEC011 and (internally) supported by the SEC011 'Firewall management service'

0009 Applications or services in the low domains for which the requirement exists to send data to applications or services in the high domain – and the cyber security requirements for the interconnection between the low and the high domain are such that data shall flow in only one direction from low to high – will make use of the 'Data Diode Service'.

0010 DDaaS offers the (logical) technical interface 'Data Diode Service interface' to services in both the low and high domain. This interface breaks down into the logical interfaces:

A. Data Diode Service – Low domain interface, which is considered to be part of the low domain; and
B. Data Diode Service – High domain interface, considered to be part of the high domain.

0011 In both low and high domain the technical service 'Data Diode Service' has the following dependent services:

A. Domain name services;
B. IPv4 Routed Access Services;
C. IPv6 Routed Access Services;
D. Enterprise Logging Service;
E. Privileged Access Management (PAM) Service.

0012 Figure 2 provides an interconnection diagram that shows the technical service 'Data Diode Service', the services by which it is consumed, and those on which it depends. The figure also shows the domains (or 'CIS Segments') between which data will flow:

A. Low domain CIS segments:
   A.1. Internet;
   A.2. PAN (NU);
   A.3. NSF (NU);
   A.4. IREEN (NU);
   A.5. REACH (NR).
B. High domain CIS Segment: ON (NS).

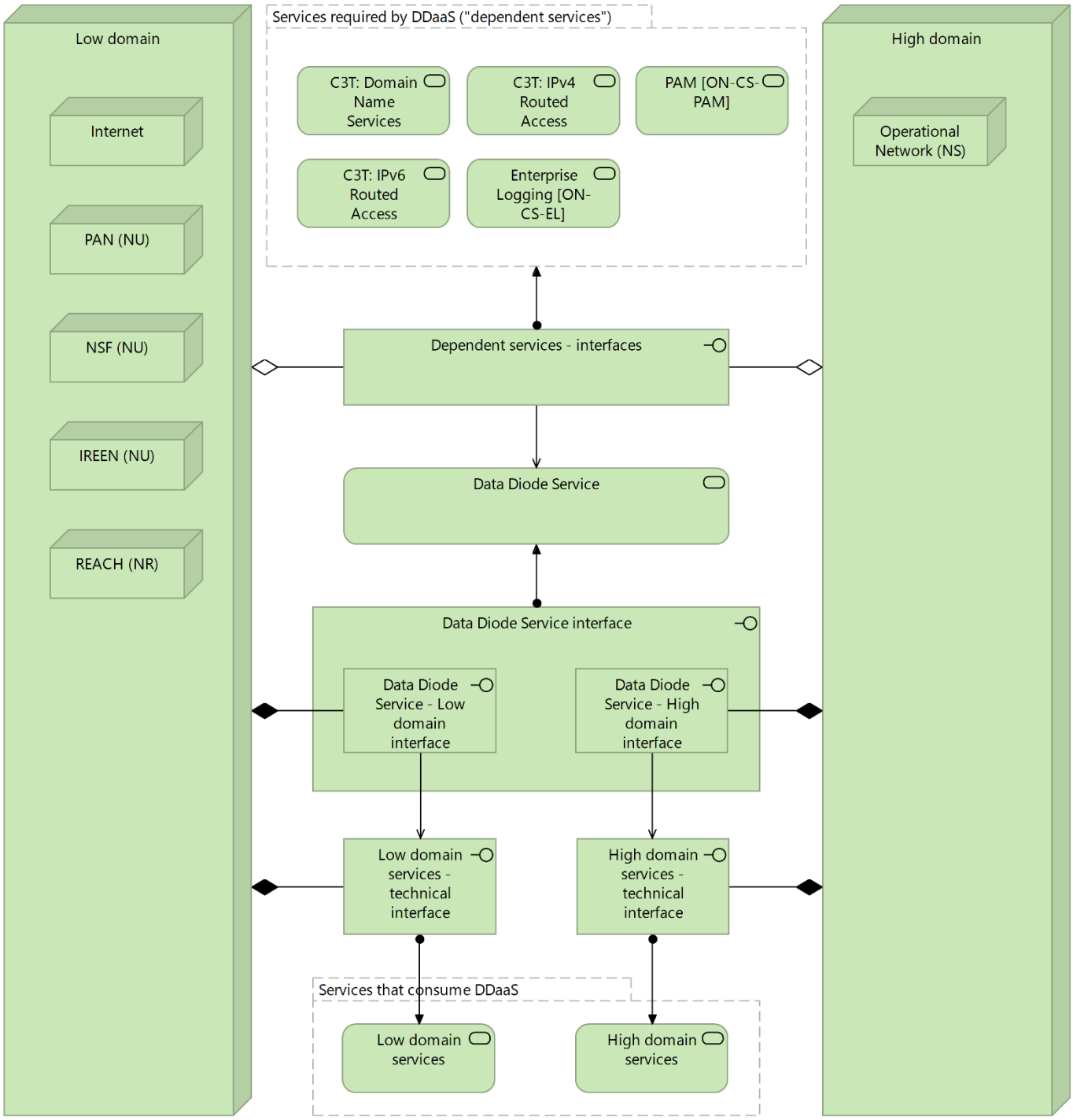

Figure 2 – Interconnection diagram 'Data Diode Service'

0013 The technical service 'Data Diode Service' offers one way data flow from services in the low domain to services in the high domain, and depends on services that must be available in both low and high domain

0014 The information flow that supports the IERs will flow from low domain services to high domain services in one direction. Information flow can be initiated by users or by the services (applications) itself.

0015 The 'Data Diode Service' ensures one-way data transfer from its low domain interface to its high domain interface. Here, 'data' includes both the information that flows from the low domain services to the high domain services as well as the transport protocol data.

0016 Between the ‘Data Diode Service’ low and high domain sub-interfaces and the interface of the low and high domain services respectively, there can be bi-directional data flow, both in terms of transport protocol data as well as information whereby the information flow stays within the domain.

0017 Figure 3 shows the one way information flow between low domain services and high domain services (in red font) and that it supports the IERs associated to the business processes performed by the user communities (or directly by the services).

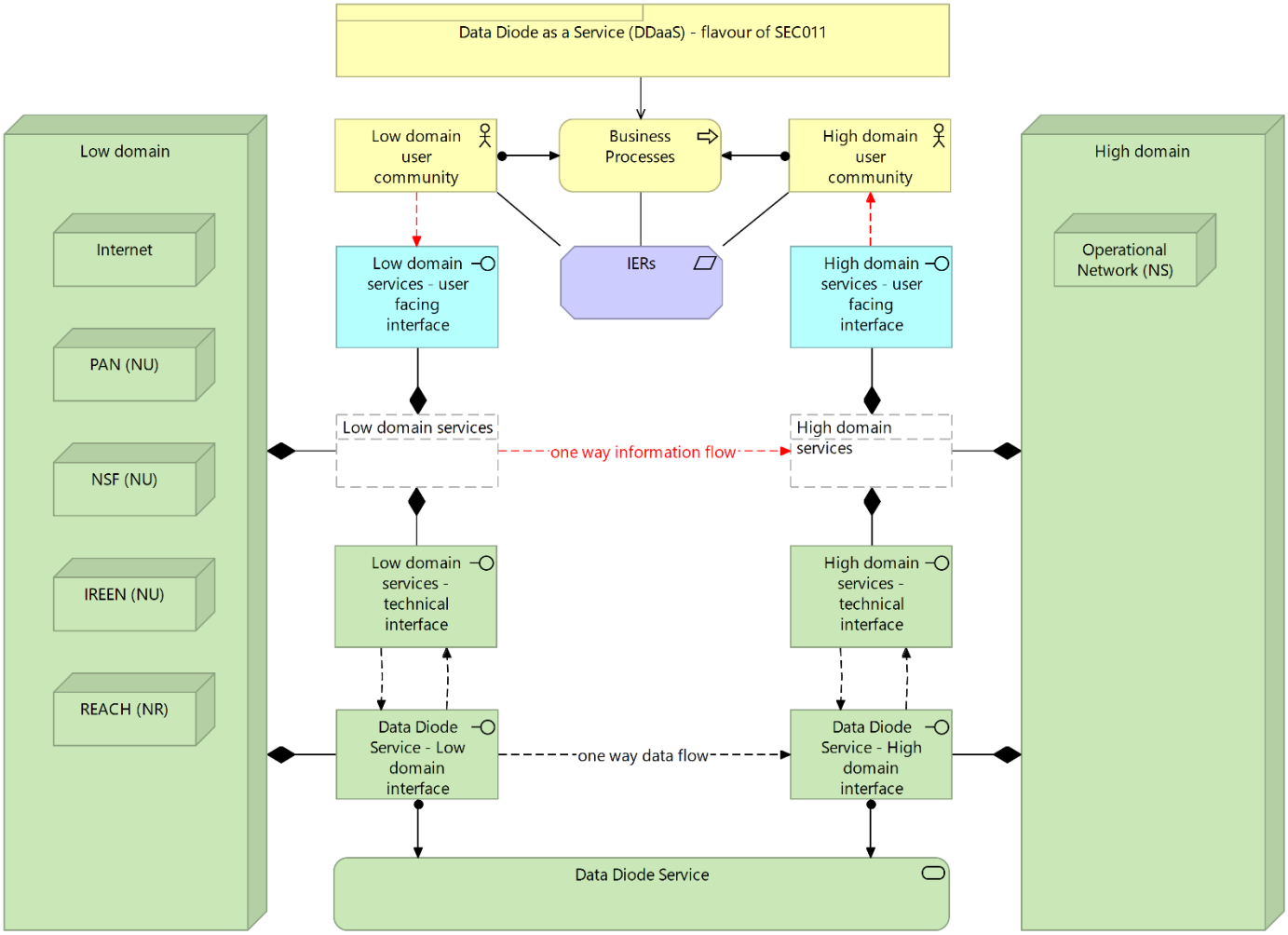

Figure 3 – Data Flow DDaaS

0018 The technical service ‘Data Diode Service’ ensures data flows in one direction from the low domain to the high domain, thereby enabling one way information flow between the low and high domain services

0019 The business service ‘DDaaS – System management’ manages and configures the technical service ‘Data Diode Service’ through a system management application service ‘DDaaS – System management Application Service’ which is accessed at interface ON-CS-DD-L04. Privileged access to this service is provided by PAM. The ‘DDaaS – System management Application Service’ also collects logs/events, which are then forwarded to the Enterprise Logging Service. The technical service ‘Data Diode Service’ may directly forward logs/events to the Enterprise Logging Service. This is depicted in Figure 4.

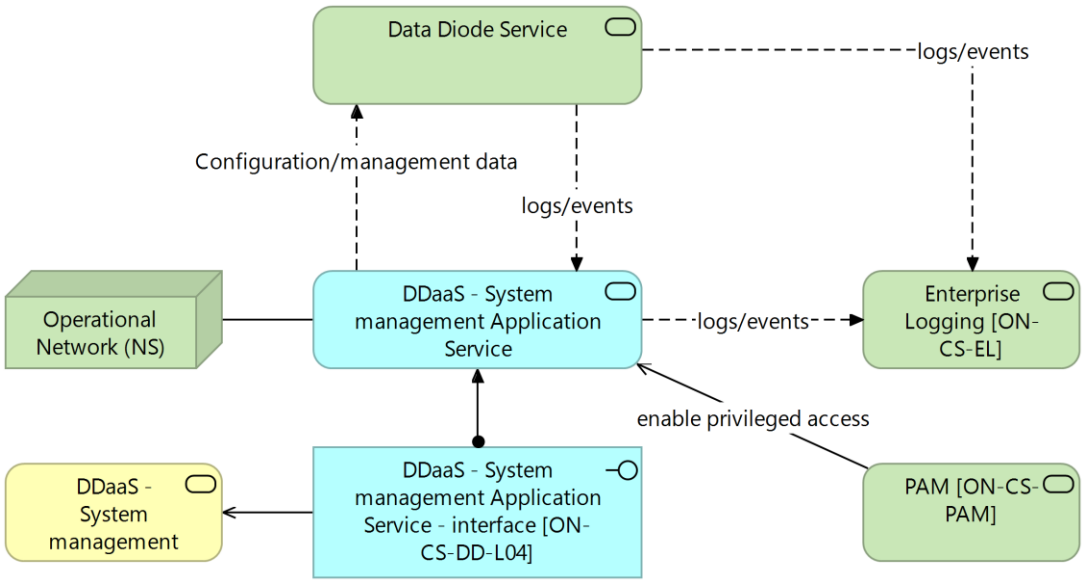

Figure 4 – Management and log collection of 'Data Diode Service'

0020 The 'Data Diode Service' is composed of:

A. a firewall service, realized by two nodes: a low and a high domain firewall;
B. a proxy service, realized by two nodes: a low and high domain proxy;
C. a hardware diode.

0021 Information that is sent from the low domain to the high domain is mediated by the firewall service and the proxy service. The proxy service makes use of a hardware diode to transfer the data, in one direction, from the low to the high domain.

0022 The external (logical) interfaces 'Data Diode Service – Low domain interface' and 'Data Diode Service – high domain interface' are composed of the low domain firewall/proxy interfaces, and the high domain firewall/proxy interfaces respectively. The interfaces of the hardware diode are considered internal interfaces.

0023 Figure 5 shows the breakdown of 'Data Diode Service'. Internal interfaces are labelled [internal] and shown in red. In order to transfer information from the low domain to the high domain, the low domain services will connect to the low domain proxy interface via the low domain firewall interface. The firewall interface will be transparent to the low domain services. The high domain proxy may push data directly to high domain services, or the high domain services connect to the high domain proxy interface via the high domain firewall interface to fetch data. The firewall interface will be transparent to the high domain services.

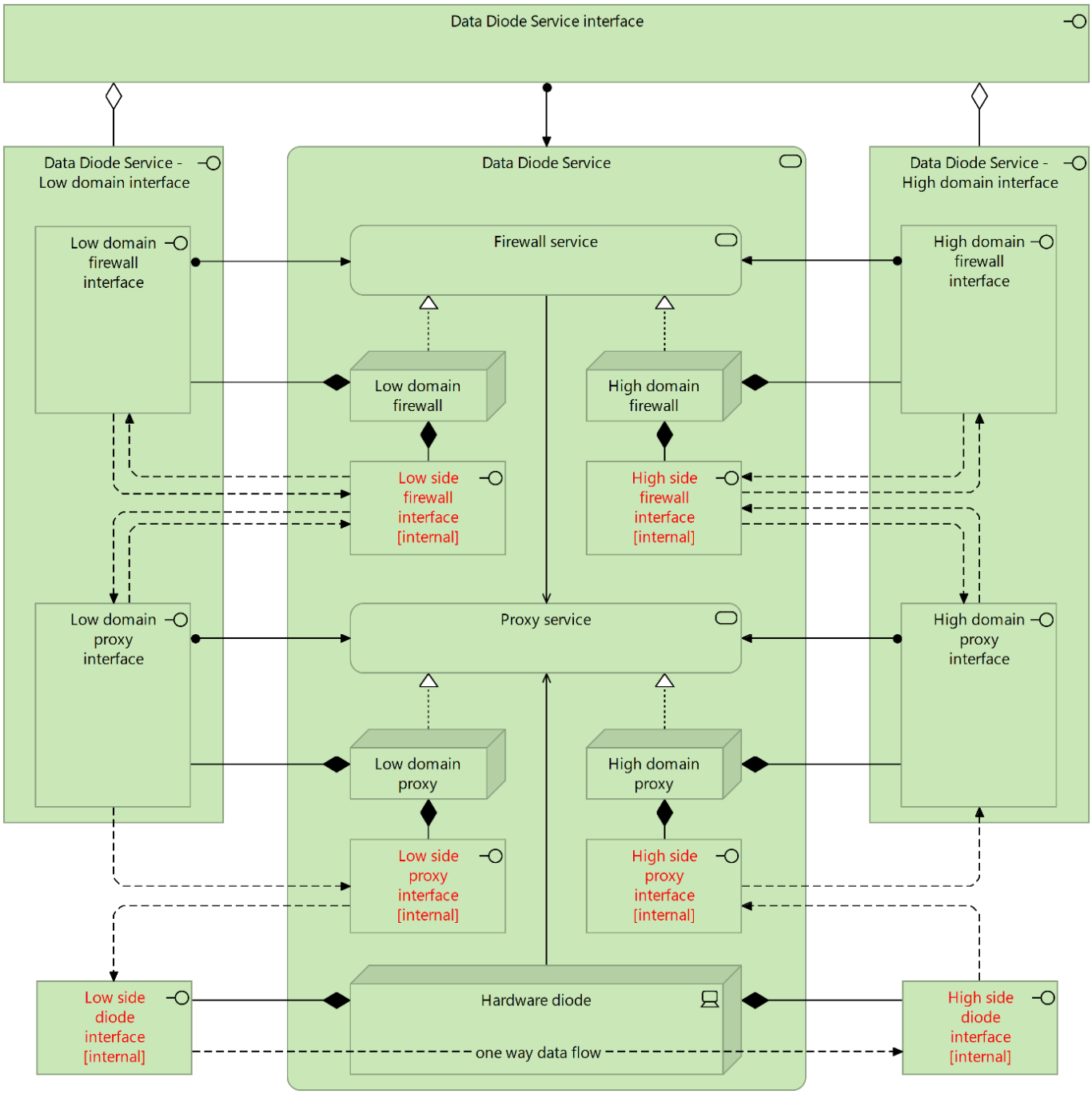

Figure 5 – Breakdown of 'Data Diode Service'

0024 The interfaces in Figure 5 have specific interface IDs depending on the CIS Segments that represent either low or high domain. The interface IDs are shown for the Operational Network in Figure 6, and for the low domain CIS in Figure 7.

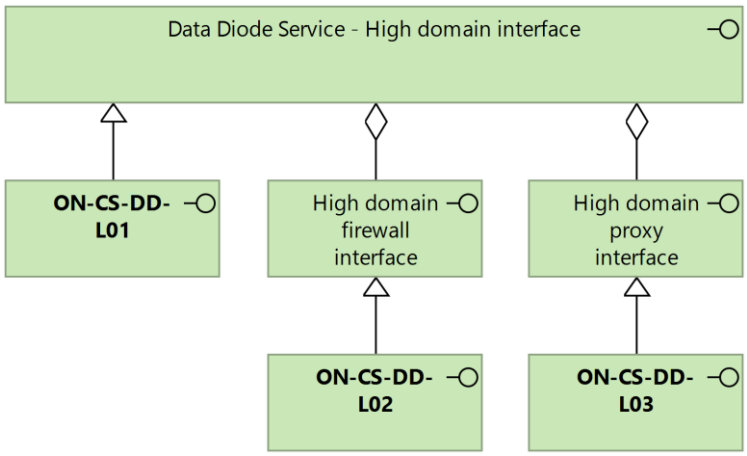

Figure 6 – Interface IDs for the Operational Network (ON)

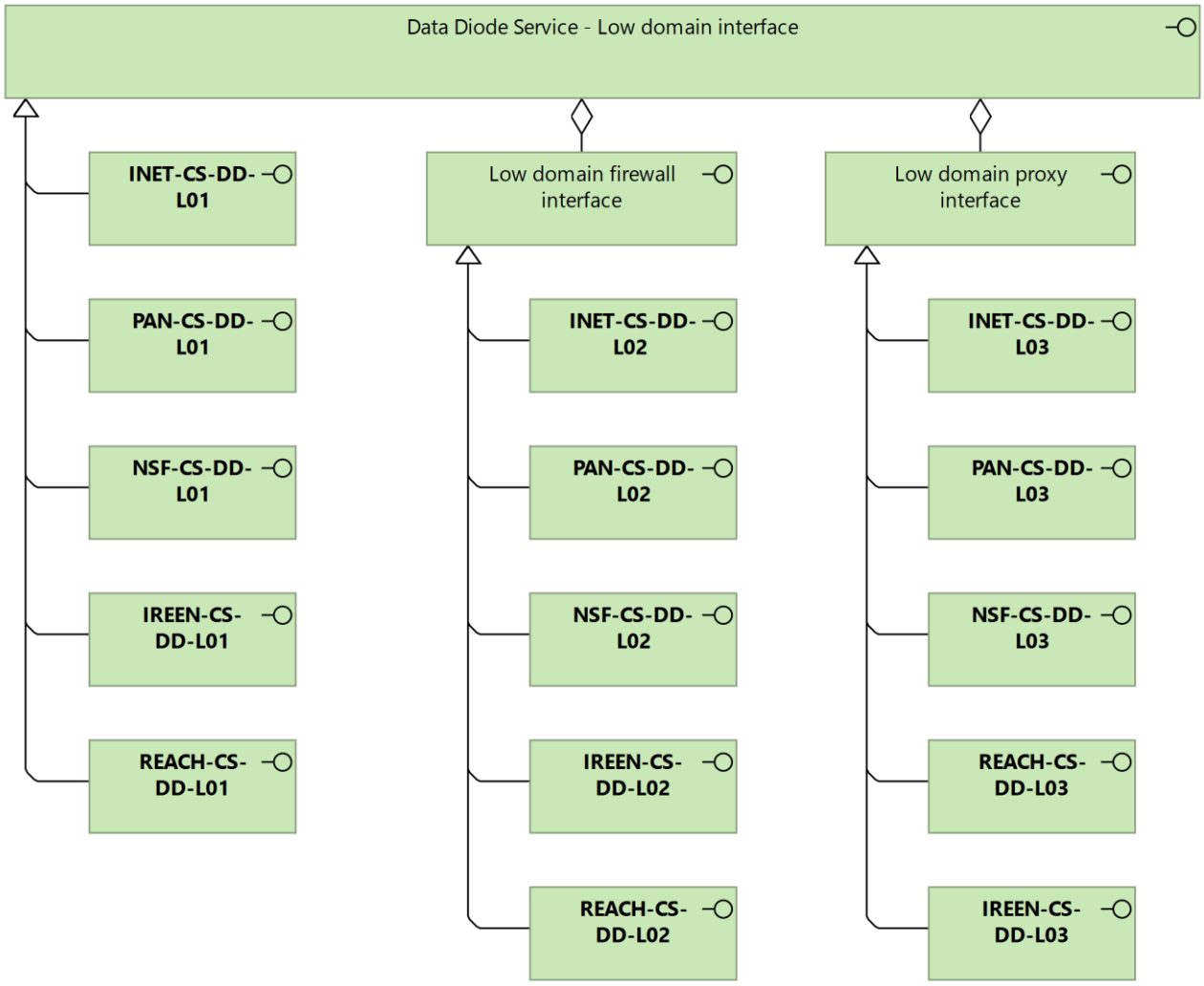

Figure 7 – Interface IDs for the low domain CISs

0025 The low and high domain proxy interfaces break up into a number of sub-interfaces per operation it offers. These sub-interfaces are described in Sections 2.1 and 2.2 respectively.

2. PROVIDED INTERFACES

0026 This section lists all interfaces that the building block provides.

Interface ID	Full name	Related sub service	References
INET-CS-DD-L01	General Data Diode Service Internet facing interface	Data Diode Service	-
PAN-CS-DD-L01	General Data Diode Service interface on PAN	Data Diode Service	-
NSF-CS-DD-L01	General Data Diode Service interface on NSF	Data Diode Service	-
IREEN-CS-DD-L01	General Data Diode Service interface on IREEN (NU)	Data Diode Service	-
REACH-CS-DD-L01	General Data Diode Service interface on REACH	Data Diode Service	-
INET-CS-DD-L02	Firewall interface on Internet	Firewall service	-
PAN-CS-DD-L02	Firewall interface on PAN	Firewall service	-
NSF-CS-DD-L02	Firewall interface on NSF	Firewall service	-
IREEN-CS-DD-L02	Firewall interface on IREEN (NU)	Firewall service	-
REACH-CS-DD-L02	Firewall interface on REACH	Firewall service	-
INET-CS-DD-L03	Internet facing proxy interface	Proxy service	Section 2.1
PAN-CS-DD-L03	Proxy interface on PAN	Proxy service	Section 2.1
NSF-CS-DD-L03	Proxy interface on NSF	Proxy service	Section 2.1
IREEN-CS-DD-L03	Proxy interface on IREEN (NU)	Proxy Service	Section 2.1
REACH-CS-DD-L03	Proxy interface on REACH	Proxy service	Section 2.1

[INET/PAN/NSF/IREEN/REACH]-CS-DD-L31	Transfer of files via file sharing	Proxy service	Section 2.1.2
[INET/PAN/NSF/IREEN/REACH]-CS-DD-L32	Transfer of data over UDP	Proxy service	Section 2.1.3
[INET/PAN/NSF/IREEN/REACH]-CS-DD-L33	Transfer of data over TCP	Proxy service	Section 2.1.4
[INET/PAN/NSF/IREEN/REACH]-CS-DD-L34	Transfer of data over HTPP(S) and REST	Proxy service	Section 2.1.5
[INET/PAN/NSF/IREEN/REACH]-CS-DD-L35	Transfer of e-mail	Proxy service	Section 2.1.6
ON-CS-DD-L01	General Data Diode Service interface on ON	Data Diode Service	-
ON-CS-DD-L02	Firewall interface on ON	Firewall service	-
ON-CS-DD-L03	Proxy interface on ON	Proxy service	Section 2.1.5
ON-CS-DD-L31	Transfer of files via file sharing	Proxy service	Section 2.2.2
ON-CS-DD-L32	Transfer of data over UDP	Proxy service	Section 2.2.3
ON-CS-DD-L33	Transfer of data over TCP	Proxy service	Section 2.2.4
ON-CS-DD-L34	Transfer of data over HTPP(S) and REST	Proxy service	Section 2.2.5
ON-CS-DD-L35	Transfer of e-mail	Proxy service	Section 2.2.6
ON-CS-DD-L04	DDaaS – System management Application Service - interface	DDaaS – System management Application Service	-

Table 1 – All provided interfaces

2.1. Low Domain Proxy interface operations

2.1.1. Outline description

0027 The operations of the Low Domain Proxy interface pertain to the following interfaces, each an instance of the Low Domain Proxy interface:

A. INET-CS-DD-L03 – Internet facing proxy interface;
B. PAN-CS-DD-L03 – Proxy interface on PAN;
C. NSF-CS-DD-L03 – Proxy interface on NSF;
D. IREEN-CS-DD-L03 – Proxy interface on IREEN (NU);

E. REACH-CS-DD-L03 – Proxy interface on REACH.

0028 Each operation offered by the Low Domain Proxy interface is assigned an interface ID per low domain CIS, based on the following naming convention:

0029 [Identifier of low domain CIS]-CS-DD-**L3X**, with X a number in the range 1-9.

0030 The following subsections describe the operations and will identify the interface ID in the header.

2.1.2. Transfer of files via file sharing (L31)

A. Description:
- Interface-LDP offers file server operations.

B. Maps to IERs:
- Low domain services share files with high domain services.

C. Protocols:
- SMB;
- NFS;
- CIFS.

D. RFCs:
- RFC1001 - Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods;
- RFC1002 - Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications;
- RFC1321 - The MD5 Message-Digest Algorithm;
- RFC2104 - HMAC: Keyed-Hashing for Message Authentication;
- RFC2119 - Key words for use in RFCs to Indicate Requirement Levels;
- RFC2307 - An Approach for Using LDAP as a Network Information Service;
- RFC2743 - Generic Security Service Application Program Interface Version 2, Update 1;
- RFC4178 - The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism;
- RFC5716 - Requirements for Federated File Systems;
- RFC7533 - Administration Protocol for Federated File Systems.

2.1.3. Transfer of data over UDP (L32)

A. Description
- Interface-LDP offers UDP (streaming) server connectivity operations.

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over UDP.
- Examples:
  - Syslog;
  - SNMP.

C. Protocols:
- UDP.

D. Standards:
- RFC768 - User Datagram Protocol;
- RFC8085 - UDP Usage Guidelines.

2.1.4. Transfer of data over TCP (L33)

A. Description
- Interface-LDP offers TCP (streaming) server connectivity operations;
- Interface-LDP offers TCP client connectivity operations. The proxy service initiates a TCP connection to a low domain service after which low domain service starts streaming data destined for a high domain service. The proxy service then forwards data to Interface ON-CS-DD-L02. At Interface ON-CS-DD-L02 the proxy service will listen for incoming TCP connections from the high domain service. After a connection has been established the data will be sent to the high domain service.

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over unidirectional[2] TCP streams.
- Examples:
  - Functional area services;
  - Database replication.

C. Protocols:
- TCP.

D. Standards:
- RFC793 - Transmission Control Protocol;
- RFC7414 - A Roadmap for Transmission Control Protocol (TCP).

2.1.5. Transfer of data over HTPP(S) and REST (L34)

A. Description
- Interface-LDP offers HTTP(S) and REST server operations.

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over HTTP(S) or REST.

C. Protocols:
- HTTP(S);
- REST.

D. Standards:
- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1;
- RFC7231 - Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content;
- RFC2818 - HTTP Over TLS.

2.1.6. Transfer of e-mail (L35)

A. Description:
- Interface-LDP offers SMTP server operations.

B. Maps to IERs:
- Low domain user sends e-mail to high domain user;
- Low domain mail server transfers e-mail to high domain mail server.

C. Protocols:
- SMTP.

[2] The term ‘unidirectional TCP’ means that Interface-LDP will not provide a response (at the application layer) to the low domain application that is streaming over TCP.

D. Standards:

- RFC 1869 - Defines the capability for SMTP service extensions, creating Extended SMTP, or ESMTP;
- RFC 1891 - Delivery Status Notification (DSN) extension to SMTP;
- RFC 5321 - The Simple Mail Transfer Protocol; it consolidates, updates, and clarifies several previous documents;
- RFC 2822 - Internet (i.e. e-mail) Message Format, which obsoletes RFC 822;
- RFC 4409 - Message Submission for Mail.

2.2. High Domain Proxy interface (ON-CS-DD-L03) operations

2.2.1. Outline description

0031 The operations of the High Domain Proxy interface pertain to proxy interface on the ON with interface ID ON-CS-DD-L03.

0032 Each operation offered by the High Domain Proxy interface is assigned an interface ID, based on the following naming convention:

0033 *ON-CS-DD-**L3X***, with *X* a number in the range 1-9.

0034 The following subsections describe the operations and will identify the interface ID in the header.

2.2.2. Transfer of files via file sharing (L31)

A. Description:

- Interface ON-CS-DD-L02 offers file server operations.

B. Maps to IERs:

- Low domain services share files with high domain services.

C. Protocols:

- SMB;
- NFS;
- CIFS.

D. RFCs:

- RFC1001 - Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods;
- RFC1002 - Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications;
- RFC1321 - The MD5 Message-Digest Algorithm;
- RFC2104 - HMAC: Keyed-Hashing for Message Authentication;
- RFC2119 - Key words for use in RFCs to Indicate Requirement Levels;
- RFC2307 - An Approach for Using LDAP as a Network Information Service;
- RFC2743 - Generic Security Service Application Program Interface Version 2, Update 1;
- RFC4178 - The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism;
- RFC5716 - Requirements for Federated File Systems;
- RFC7533 - Administration Protocol for Federated File Systems.

2.2.3. Transfer of data over UDP (L32)

A. Description

- Interface ON-CS-DD-L02 offers UDP client connectivity operations.

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over UDP.
- Examples:
  - Syslog;
  - SNMP.

C. Protocols:
- UDP.

D. Standards:
- RFC768 - User Datagram Protocol;
- RFC8085 - UDP Usage Guidelines.

2.2.4. Transfer of data over TCP (L33)

A. Description
- Interface ON-CS-DD-L02 offers TCP client connectivity operations;
- Interface ON-CS-DD-L02 offers TCP (streaming) server connectivity operations. At Interface ON-CS-DD-L02 the proxy service will listen for incoming TCP connections from a high domain service that is expecting TCP (streaming) data from a low domain service. (At Interface-LDP the proxy service initiates a TCP connection to the low domain service after which the low domain service starts streaming data destined for the high domain service.)

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over unidirectional TCP streams.
- Examples:
  - Functional area services;
  - Database replication.

C. Protocols:
- TCP.

D. Standards:
- RFC793 - Transmission Control Protocol;
- RFC7414 - A Roadmap for Transmission Control Protocol (TCP).

2.2.5. Transfer of data over HTPP(S) and REST (L34)

A. Description
- Interface ON-CS-DD-L02 offers HTTP(S) and REST client operations.

B. Maps to IERs:
- Low domain services send/stream data to services in high domain over HTTP(S) or REST.

C. Protocols:
- HTTP(S);
- REST.

D. Standards:
- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1
- RFC7231 - Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content;
- RFC2818 - HTTP Over TLS.

2.2.6. Transfer of e-mail (L35)

A. Description:

- Interface-LDP offers SMTP server operations.

B. Maps to IERs:
   - Low domain user sends e-mail to high domain user;
   - Low domain mail server transfers e-mail to high domain mail server.

C. Protocols:
   - SMTP.

D. Standards:
   - RFC 1869 - Defines the capability for SMTP service extensions, creating Extended SMTP, or ESMTP;
   - RFC 1891 - Delivery Status Notification (DSN) extension to SMTP;
   - RFC 5321 - The Simple Mail Transfer Protocol; it consolidates, updates, and clarifies several previous documents;
   - RFC 2822 - Internet (i.e. e-mail) Message Format, which obsoletes RFC 822;
   - RFC 4409 - Message Submission for Mail.

2.3. Interface ON-CS-DD-L04 operations

2.3.1. Management and configuration

0035 Interface ON-CS-DD-L04 offers operations to configure and manage the technical service ‘Data Diode Service’.

3. DEPENDENT SERVICE INTERFACES

0036 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
Interface-DNS	Domain name services – low domain interface	C3 Taxonomy
Interface-IPv4	IPv4 Routed Access Services – low domain interface	C3 Taxonomy
Interface-IPv6	IPv6 Routed Access Services – low domain interface	C3 Taxonomy
ON-Infra-NETW-L04	Domain name services – high domain interface	IaaS SDP
ON-Infra-NETW-L04	IPv4 Routed Access Services – high domain interface	IaaS SDP
ON-Infra-NETW-L04	IPv6 Routed Access Services – high domain interface	IaaS SDP
ON-CS-EL	Enterprise Logging Service – required by Data Diode Service 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