**Data Diode**

Security Target

Common Criteria - BANPUMP

**Table of Contents**

[**1.** **Security Target Introduction (ASE\_INT.1)** 3](#_Toc157603346)

[**1.1** **Security Target Reference** 3](#_Toc157603347)

[**1.2** **TOE Reference** 3](#_Toc157603348)

[**1.3** **TOE Overview** 3](#_Toc157603349)

[**1.4** **TOE Description** 6](#_Toc157603350)

[**1.4.1** **Physical Scope** 6](#_Toc157603351)

[**1.4.2** **TOE Versions** 7](#_Toc157603352)

[**1.4.3** **Logical Scope** 7](#_Toc157603353)

[**1.5** **Document Overview** 8](#_Toc157603354)

[**2.** **Conformance Claim (ASE\_CCL.1)** 8](#_Toc157603355)

[**2.1** **CC Conformance Claim** 8](#_Toc157603356)

[**2.2** **Protection Profile Claim, Package Claim** 9](#_Toc157603357)

[**2.3** **Conformance Rationale** 9](#_Toc157603358)

[**3.** **Security problem definition (ASE\_SPD.1)** 9](#_Toc157603359)

[**3.1.** **Threats** 9](#_Toc157603360)

[**3.2.** **Assumptions** 9](#_Toc157603361)

[**4.** **Security Objectives (ASE\_OBJ.2)** 10](#_Toc157603362)

[**4.1** **Security objectives for the Target of Evaluation** 10](#_Toc157603363)

[**4.2** **Security objectives for the Operational Environment** 10](#_Toc157603364)

[**4.3** **Security objective rationale** 10](#_Toc157603365)

[**5.** **Security requirements (ASE\_OBJ.2)** 10](#_Toc157603366)

[**5.1** **Security Functional Requirements (SFRs)** 10](#_Toc157603367)

[**5.1.1** **FDP\_IFC.2 Information Flow Control** 10](#_Toc157603368)

[**5.1.2** **FDP\_IFF.1 Simple Security Attributes** 11](#_Toc157603369)

[**5.2** **Security Assurance Requirements (SARs)** 11](#_Toc157603370)

[**5.3** **Extended Component Definition (ASE\_ECD.1)** 12](#_Toc157603371)

[**5.4** **Security Requirements Rationale** 12](#_Toc157603372)

[**6.** **TOE Summary Specification (ASE\_TSS.1 / ASE\_TSS.2)** 13](#_Toc157603373)

[**References** 14](#_Toc157603374)

[**APPENDIX** 15](#_Toc157603375)

[**A.** **Security Objective Rationale** 15](#_Toc157603376)

[**B.** **Security Requirements Rationale** 16](#_Toc157603377)

**List of Figures**

[Figure 1. Protecting downstream confidentiality. 4](#_Toc157603378)

[Figure 2. Protecting upstream integrity. 5](#_Toc157603379)

[Figure 3. The TOE as a single hardware unit. 6](#_Toc157603380)

[Figure 4. Hardware Data Diode functional block diagram. 8](#_Toc157603381)

**List of Tables**

[Table 1. TOE versions. 7](#_Toc157603382)

[Table 2. Threats to the TOE. 9](#_Toc157603383)

[Table 3. Assumptions. 9](#_Toc157603384)

[Table 4. Security Objectives of the TOE. 10](#_Toc157603385)

[Table 5. Security Objectives of the TOE Environment. 10](#_Toc157603386)

[Table 6. Assurance Requirements. 12](#_Toc157603387)

[Table 7. Mapping Threats/Assumptions to Objectives. 15](#_Toc157603388)

[Table 8. Threats/Objectives Rationale. 15](#_Toc157603389)

[Table 9. Assumptions/Objectives Rationale. 16](#_Toc157603390)

[Table 10. Mapping Requirements to Objectives. 16](#_Toc157603391)

[Table 11. Security Requirements/Objectives Rationale. 17](#_Toc157603392)

# **Security Target Introduction (ASE\_INT.1)**

## **Security Target Reference**

|  |  |
| --- | --- |
| **ST Title** | Data Diode Security Target |
| **ST Version** | 1 |
| **ST Status** | Work in progress |
| **ST Classification** | Internal document |
| **Author** | For now, it is based on Frans van Dorsselaer (Fox Crypto B.V.) |

## **TOE Reference**

|  |  |
| --- | --- |
| **Developer Name** | Community project DYODE (https://github.com/wavestone-cdt/dyode) |
| **TOE Name** | Data Diode |
| **TOE Version Number** | 1 |

## **TOE Overview**

The Target of Evaluation (TOE) is a Data Diode, made of fiber optic transceivers and will hereafter be referred to as the TOE throughout this document. The TOE is a unidirectional network, which allows data to travel only in one direction, as shown in Figure 1.

The one-way physical connection of the TOE allows information to be transferred optically from one network (the upstream network) to another network (the downstream network). The unidirectionality of the data flow **ensures the integrity of the upstream network** against threats from the downstream network, and simultaneously **ensures the confidentiality of the downstream network**. To ensure signals can only pass in one direction, and not vice versa, the TOE deploys a single light source as the only connection to the downstream network. Fiber-optic cables are used to connect the TOE to both the upstream and downstream networks in order to minimize electromagnetic coupling. Physical restrictions on the environment ensure that the unidirectionality of the dataflow cannot be bypassed.

**It is important to mention that, once manufactured, there is no way to alter the function of the TOE!**

**Example 1: Protecting downstream confidentiality**

As an example, one practical deployment of the TOE is to protect a High Security Level downstream network from leaking information to a Low Security Level upstream network, as indicated in Figure 1.

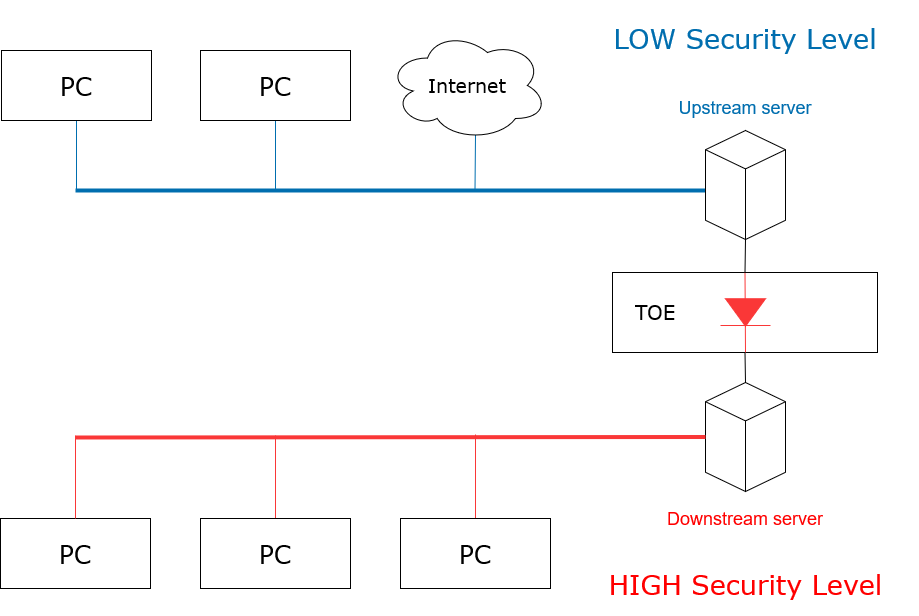


Figure 1. Protecting downstream confidentiality.

This setup (Figure 1) is used to allow an information flow into the protected downstream network, while preventing information leaving the protected downstream network. Therefore, **the confidentiality of the downstream side is ensured**. Examples of upstream data sources that can unidirectionally feed data into the protected downstream network include:

|  |  |
| --- | --- |
| **Internet** | Gathering information from around the world is possible by transferring data from the upstream network (Internet) to the protected downstream network. This is accomplished by using a standard file-transfer communication protocol. |
| **E-mail** | E-mails can be transmitted from the upstream network and received at the protected downstream network, using an e-mail gateway. Therefore, downstream network users can read their e-mails without physically going to a different Security Level. |
| **Logs** | Syslog is normally UDP based, meaning log lines (text) can be sent from the upstream network into the downstream network where logs can not be tampered with. |
| **Intercept** | It is often mandatory for mobile phone service providers to intercept telecom traffic data. Intercepted signals on the upstream network are transformed into digital data and packaged in low-level UDP network packets, which are transmitted to the protected downstream network for analysis by the police or intelligence agencies. |
| **Updates** | Software updates can be deployed at the protected downstream network after being copied from the upstream network. |
| **Printing** | Information located on the upstream network can be transmitted to a printer located on the protected downstream network. |

**Example 2: Protecting upstream integrity**

As a second example, another practical deployment of the TOE is to protect a High Security Level upstream network from being tampered with by a Low Security Level downstream network, as shown in Figure 2.

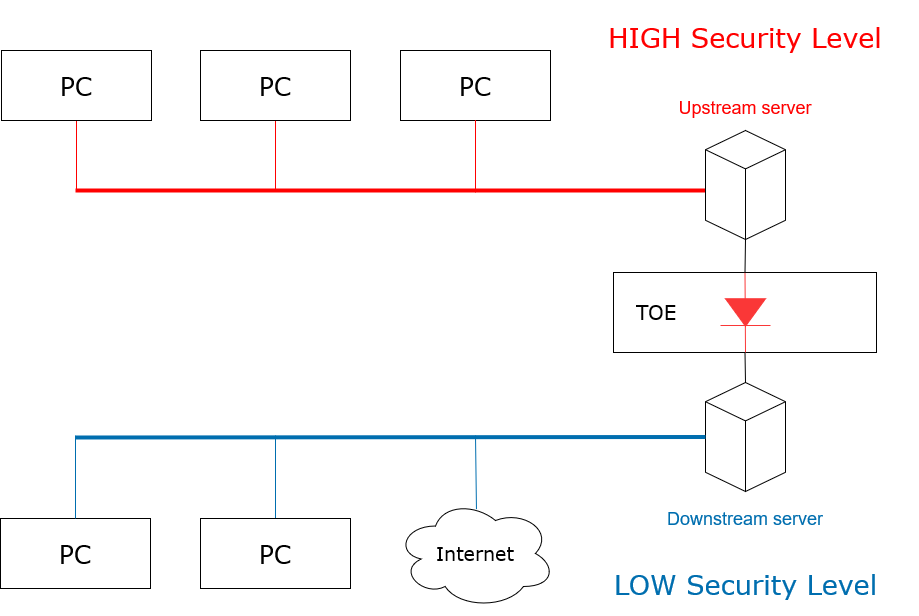


Figure 2. Protecting upstream integrity.

This setup (Figure 2) is used to allow an information flow from the protected upstream network while preventing information from the downstream network to influence the upstream side. Therefore, **the integrity of the upstream side is ensured**. Examples of upstream data sources that can unidirectionally transmit data from the protected downstream network include:

|  |  |
| --- | --- |
| **Industrial Processes** | Processes on the protected upstream network provide the downstream network with real-time process information for monitoring purposes, without allowing downstream side users to influence these critical industrial processes on the protected upstream side. |

The first scenario (Figure 1) highlights only the confidentiality of the downstream network, while the second scenario (Figure 2), highlights only the integrity of the upstream network. In general, however, the TOE separates two distinct security domains and both the integrity of the upstream network and the confidentiality of the downstream network are ensured simultaneously.

## **TOE Description**

### **Physical Scope**

The Target of Evaluation (TOE) consists of a single hardware unit, see Figure 3. The TOE contains only fixed-function physical hardware and does not contain any programmable logic, firmware, software, volatile memory, or persistent memory. The TOE allows information to flow through the device in a single direction from the bidirectional upstream transceiver to the unidirectional downstream transceiver. This is the only function performed by the TOE.

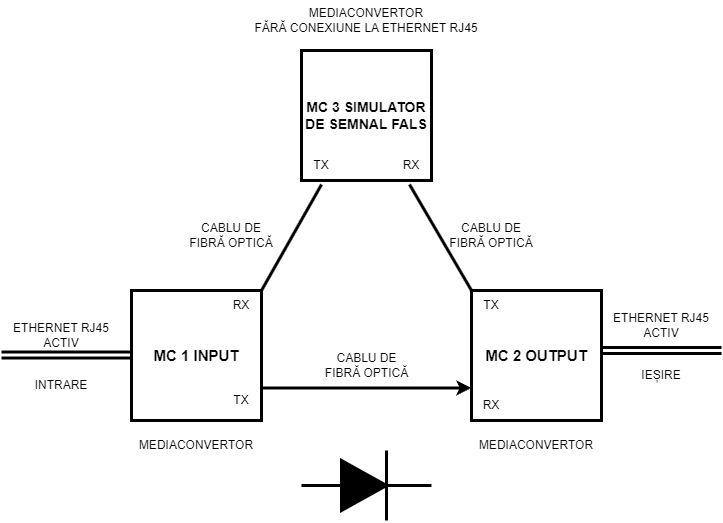
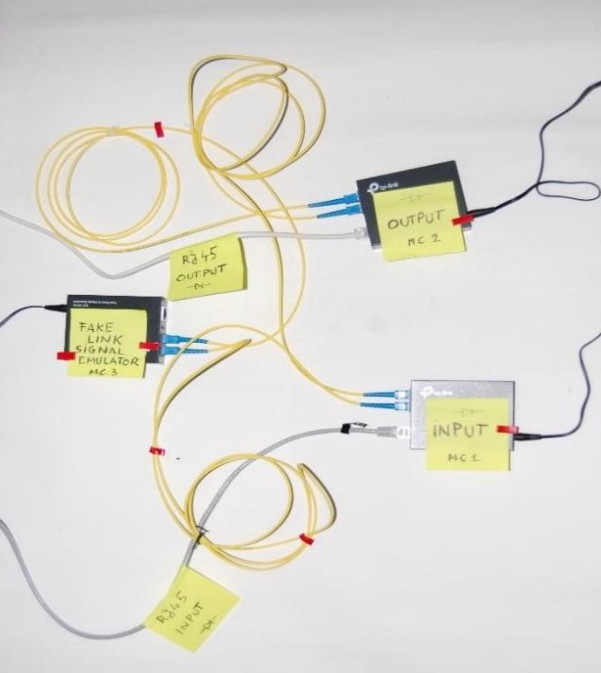


Figure 3. The TOE as a single hardware unit.

The physical scope includes the OE.PHYSICAL environmental objective defined in Section 4.2 which applies to the entire lifecycle of the TOE, including storage and transport.

The picture in Figure 3 is not normative for the identification of the TOE as mediaconverter models and cables may differ.

### **TOE Versions**

The TOE comes in three versions, each with a unique model number that is marked on the TOE casing, see Table 1. The only difference between the TOE versions, with respect to this ST, is the operating speed.

Table 1. TOE versions.

|  |  |  |
| --- | --- | --- |
| **TOE Version** | **Model Number** | **Speed** |
| 1 | TP-Link MC200CM | 1 Gbit/sec |
| 1b | TP-Link MC100CM | 100 Mbit/sec |
| 1c | TP-Link MC200CM-MC100CM with slower (fast ethernet) receiver | 100 Mbit/sec |

### **Logical Scope**

Figure 4 shows the TOE (Hardware Data Diode) functional block diagram consisting of two discrete fiber optical transceivers. The data transfer is implemented in hardware, of the physical Open System Interconnection (OSI) reference model, to guarantee complete unidirectionality.

The TOE has two operational interfaces to establish one-way communication, the Bidirectional Upstream port and Unidirectional Downstream port. At the upstream transceiver light is carried into the Bidirectional Upstream port and converted, with the aid of a photocell, into an electrical signal. The electrical signal spreads through the TOE to the downstream transceiver. The downstream transceiver receives the electrical signal and converts this, using a light source, into light. Finally, the light is offered, through the Unidirectional Downstream port, to the downstream network. The Unidirectional Downstream port is incapable of input and therefore lacks the ability of converting light into an electrical signal.

Consequently, an electrical signal is unable to propagate to the upstream transceiver and therefore incapable to create a covert channel.

Fiber optics is used to transport signals from and to the Bidirectional Upstream port, and from the Unidirectional Downstream port. Electrical signals only transport signals inside the TOE, which is completely enclosed by an aluminum casing.

Unidirectional communication does not work with a network protocol that requires a handshake (acknowledgement). To establish a communication link between the upstream side and the upstream transceiver, a Bidirectional Upstream port is initiated. Data, information, or communication originating at the downstream side is physically unable to flow to the Bidirectional Upstream port via the TOE, therefore there is no back channel which could be used as a covert channel. Any network protocol could be used to implement the communication if no handshaking across the TOE is required, e.g. the User Datagram Protocol (UDP) can provide a unidirectional flow of information.

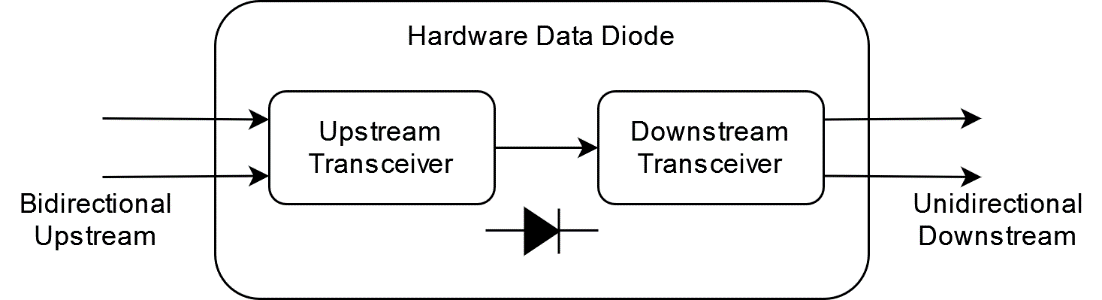


Figure 4. Hardware Data Diode functional block diagram.

## **Document Overview**

The ST has been developed in accordance with the requirements of the Common Criteria (CC) Part 3, Class ASE: Security Target Evaluation and ANNEX A: Specification of Security Targets, of the CC Part 1. The ST contains the following sections:

|  |  |
| --- | --- |
| **Section 1** | ST introduction, provides the identification material for the ST and the TOE, it provides an overview and description of the TOE. |
| **Section 2** | Conformance claims, describes how the ST conforms to the CC. |
| **Section 3** | Conformance claims, describes how the ST conforms to the CC. |
| **Section 4** | Security objectives, are a concise and abstract statement of the intended solution to the problem. |
| **Section 5** | Security requirements, describes the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs). |
| **Section 6** | TOE summary specification, provides potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. |

# **Conformance Claim (ASE\_CCL.1)**

## **CC Conformance Claim**

This Security Target and TOE complies with the following:

|  |  |  |
| --- | --- | --- |
| CC | | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5:   * Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Revision 1, November 2022. * Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Revision 1, November 2022. * Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Revision 1, November 2022. |
| Conformance claim | Part 2 Security functional components | Conformant |
| Part 3 Security assurance components | Conformant |

## **Protection Profile Claim, Package Claim**

This Security Target claims conformance to assurance package EAL7 augmented by ASE\_TSS.2 and ALC\_FLR.3.

## **Conformance Rationale**

None

# **Security problem definition (ASE\_SPD.1)**

## **Threats**

The security problems addressed by the TOE and the TOE environment are identified and detailed in the following table:

Table 2. Threats to the TOE.

|  |  |
| --- | --- |
| **Threat name** | **Threat definition** |
| T.Transfer | A user or process on the downstream network that either (a) accidentally or deliberately breaches the confidentiality of some downstream information by transmitting data through the TOE to the upstream network, or (b) accidentally or deliberately breaches the integrity of the upstream network by transmitting data through the TOE to the upstream network. |

## **Assumptions**

This section describes the assumption made in the process of identifying the threats and security requirements. The assumptions made for the TOE are defined in the following table:

Table 3. Assumptions.

|  |  |
| --- | --- |
| **Assumption name** | **Assumption definition** |
| A.Physical | The intended operation environment shall store and operate the TOE in accordance with the highest of each of the requirements of the upstream network and the downstream network. |
| A.Power | The TOE must be powered in such a way that users or processes on the downstream side cannot control power through the downstream network. This prevents unauthorized agents from controlling the signal carrier of the Bidirectional Upstream port, by toggling the TOE power. |
| A.Network | The only method of interconnecting the upstream network and downstream network is one or more units of the TOE, with all of the units operating in the same data flow direction. This prevents an unauthorized agent from using an untrustworthy product to circumvent the security provided by the TOE. |

# **Security Objectives (ASE\_OBJ.2)**

## **Security objectives for the Target of Evaluation**

This section identifies and describes the security objectives of the TOE.

Table 4. Security Objectives of the TOE.

|  |  |
| --- | --- |
| **Objective name** | **Objective definition** |
| O.Confidentiality | The information on the downstream network is kept confidential from the upstream network. |
| O.Integrity | The information on the upstream network cannot be altered by the downstream network. |

## **Security objectives for the Operational Environment**

The security objectives for the TOE Environment are defined in the following table.

Table 5. Security Objectives of the TOE Environment.

|  |  |
| --- | --- |
| **Objective name** | **Objective definition** |
| OE.Physical | The intended operational environment shall be capable of storing and operating the TOE according to the requirements of the upstream network and of the downstream network. |
| OE.Power | The intended operational environment shall provide power to the TOE such that the TOE power cannot be evaluated or interfered with from the downstream network. |
| OE.NetworkFlow | The only method to interconnect the upstream network and the downstream network is by using one or more units of the TOE. All the units must operate in the same data flow direction. |

## **Security objective rationale**

Appendix A presents the security objective rationale.

# **Security requirements (ASE\_OBJ.2)**

## **Security Functional Requirements (SFRs)**

The TOE uses two subjects: Upstream and Downstream. These represent the input and the output of the TOE. These subjects have no attributes.

This statement of the SFRs does not define other subjects, objects, operations, security attributes or external entities.

The **FFHDD policy** is defined to be the compliancy to FDP\_IFC.2 and FDP\_IFF.1 as specified in sections 5.1.1 and 5.1.2.

### **FDP\_IFC.2 Information Flow Control**

|  |  |
| --- | --- |
| **Dependencies:** | FDP\_IFF.1 Simple security attributes |
| **FDP\_IFC.2.1** | The TSF shall enforce the **FFHDD policy** on **[[Upstream, Downstream], all information]** and all operations that cause that information to flow to and from subjects covered by the SFP. |
| **FDP\_IFC.2.2** | The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP. |

### **FDP\_IFF.1 Simple Security Attributes**

|  |  |
| --- | --- |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | FDP\_IFC.1 Subset information flow control.  FMT\_MSA.3 Static attribute initialization1. |
| **FDP\_IFF.1.1** | The TSF shall enforce the **FFHDD policy** based on the following types of subject and information security attributes: **[[Upstream [], Downstream []], all information []]**. |
| **FDP\_IFF.1.2** | The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **information may flow from Upstream to Downstream**. |
| **FDP\_IFF.1.3** | **<refined away>** |
| **FDP\_IFF.1.4** | **<refined away>** |
| **FDP\_IFF.1.5** | The TSF shall explicitly deny an information flow based on the following rules: **information shall not flow from Downstream to Upstream**. |

## **Security Assurance Requirements (SARs)**

The security assurance requirements for the TOE are the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation. For a detailed description of these components, please refer to the Part 3 of the Common Criteria directly. These requirements are listed in the following table:

1 The dependency to FMT\_MSA.3 is not applicable as there are no security attributes to initialize.

Table 6. Assurance Requirements.

|  |  |
| --- | --- |
| **Assurance Class** | **Assurance Component** |
| ADV: Development | ADV\_ARC.1 – Security architecture description |
| ADV\_FSP.6 – Complete semi-formal functional specification with additional formal specification |
| ADV\_IMP.2 – Complete mapping of the implementation representation of the TSF |
| ADV\_INT.3 – Minimally complex internals |
| ADV\_SPM.1 – Formal TOE security policy model |
| ADV\_TDS.6 – Complete semiformal modular design with formal high level design presentation |
| AGD: Guidance documents | AGD\_OPE.1 – Operational user guidance |
| AGD\_PRE.1 – Preparative procedures |
| ALC: Life-cycle support | ALC\_CMC.5 – Advanced support |
| ALC\_CMS.5 – Development tools CM coverage |
| ALC\_DEL.1 – Delivery procedures |
| ALC\_DVS.2 – Sufficiency of Security Measures |
| ALC\_FLR.3 – Systematic flaw remediation |
| ALC\_LCD.2 – Measurable life-cycle model |
| ALC\_TAT.3 – Compliance with implementation standards – all parts |
| ASE: Security Target evaluation | ASE\_CCL.1 – Conformance claims |
| ASE\_ECD.1 – Extended components definition |
| ASE\_INT.1 – ST introduction |
| ASE\_OBJ.2 – Security objectives |
| ASE\_REQ.2 – Derived security requirements |
| ASE\_SPD.1 – Security problem definition |
| ASE\_TSS.2 – TOE summary specification with architectural design summary |
| ATE: Tests | ATE\_COV.3 – Rigorous analysis of coverage |
| ATE\_DPT.4 – Testing: implementation representation |
| ATE\_FUN.2 – Ordered functional testing |
| ATE\_IND.3 – Independent testing - complete |
| AVA: Vulnerability assessment | AVA\_VAN.5 – Advanced methodical vulnerability analysis |

|  |  |
| --- | --- |
| ADV\_SPM.1.1.D | The developer shall provide a formal security policy model for the **FFHDD policy**. |

## **Extended Component Definition (ASE\_ECD.1)**

All security requirements in this ST are based on components from CC Part 2 and CC Part 3,  
therefore there are no Extended Component Definitions.

## **Security Requirements Rationale**

Appendix B presents the security requirements rationale.

# **TOE Summary Specification (ASE\_TSS.1 / ASE\_TSS.2)**

The TOE protects itself against interference and logical tampering by:

* Consisting only of hardware components. The TOE does not have memory, settings or other parameters that can be changed.
* Having only two interfaces that are accessible to unauthorized agents, which allows for very limited interactions:
  + The upstream interface: the TOE passes data received from the upstream network without interpreting the data.
  + The downstream interface: the TOE ignores all data received here. Therefore, there is no way to tamper or interfere with the TOE settings.

The TOE protects itself against bypass by:

* Being the only connection between the upstream network and downstream network.
* Ensuring that all data flow from the upstream network must pass through the TOE to get to the downstream network, thus preventing bypass around the TOE.

# **References**

1. Common Criteria for Information Technology Security Evaluation. *Part 1: Introduction and General Model, Version 3.1, Revision 5,* April 2017. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf>
2. Common Criteria for Information Technology Security Evaluation. *Part 2: Security Functional Components, Version 3.1, Revision 5,* April 2017. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf>
3. Common Criteria for Information Technology Security Evaluation. *Part 3: Security Assurance Components, Version 3.1, Revision 5,* April 2017. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf>

# **APPENDIX**

# **Security Objective Rationale**

This section presents the rationale behind the security objectives addressing the threats and assumptions associated with the TOE.

Table 7 demonstrates how all threats and assumptions are covered by at least one of the security objectives of the TOE, and that each security objective covers at least one threat or assumption.

Table 8 demonstrates how the objectives of the TOE and the TOE environment counter the threats  
identified in Section 3.1.

Table 9 demonstrates how the objectives of the TOE and the TOE environment address the assumptions  
identified in Section 3.2.

Table 7. Mapping Threats/Assumptions to Objectives.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threats and Assumptions** | T.Transfer | T.Physical | T.Power | T.Network |
| **Objectives** |
| O.Confidentiality | X |  |  |  |
| O.Integrity | X |  |  |  |
| OE.Physical | X | X | X | X |
| OE.Power | X |  | X |  |
| OE.Network |  |  |  | X |

Table 8. Threats/Objectives Rationale.

|  |  |  |
| --- | --- | --- |
| **Threats** | **Objectives** | **Rationale** |
| T.Transfer | O.Confidentiality  O.Integrity  OE.Physical  OE.Power | Both O.Confidentiality and O.Integrity, simultaneously and independently, reduce the threat that data will be transferred from the downstream network to the upstream network, through the TOE.  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized agent has direct physical access to the TOE or any of the TOE components.  OE.Power ensures that the power provided to the TOE cannot be used as a covert channel by the downstream network. |

Table 9. Assumptions/Objectives Rationale.

|  |  |  |
| --- | --- | --- |
| **Assumptions** | **Objectives** | **Rationale** |
| A.Physical | OE.Physical | This assumption is upheld by objective OE.Physical because it ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized agent has direct physical access to the TOE or any of the TOE components. |
| A.Power | OE.Physical  OE.Power | This assumption is upheld by the following objectives:  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized agent has direct physical access to the TOE or any of the TOE components. This can effectively prevent an unauthorized agent or process from interfering with the power supplied to the TOE.  OE.Power ensures that the TOE power cannot be interfered with by an unauthorized agent or process on the downstream network. |
| A.Network | OE.Physical  OE.Network | This assumption is upheld by objective OE.Physical which ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized agent has direct physical access to the TOE or any of the TOE components.  The assumption is also upheld by objective OE.Network which ensures that the TOE is the only method of interconnecting the upstream and downstream networks. |

# **Security Requirements Rationale**

Table 10 provides a mapping between the security requirements and the objectives that have been defined in section 4. Table 11 provides a detailed rationale of this mapping.

Table 10. Mapping Requirements to Objectives.

|  |  |  |
| --- | --- | --- |
| **Objectives** | O.Confidentiality | O.Integrity |
| **SFRs** |
| FDP\_IFC.2 | X | X |
| FDP\_IFF.1 | X | X |

Table 11. Security Requirements/Objectives Rationale.

|  |  |  |
| --- | --- | --- |
| **Objectives** | **Security Functional Requirements** | **Rationale** |
| O.Confidentiality | FDP\_IFC.2 Information flow control policy  FDP\_IFF.1 Simple Security Attributes | O.Confidentiality is achieved through the diode functionality implemented in the TOE, which serves to enforce the FDP\_IFC.2 and FDP\_IFF.1 requirements.  FDP\_IFC.2 defines that the policy of the *Unidirectional flow SFP*: User data cannot flow from the downstream port to the upstream port, while user data can flow from the upstream port via the TOE.  FDP\_IFF.1 identifies the rules for the TOE that are required to enforce the *Unidirectional Flow SFP*.  FDP\_IFF.1 is based on the TOE interface port attributes and user data security attributes. These attributes are defined through FDP\_IFF.1 and are required to achieve the SFP rules and the O.Confidentiality objective.  FDP\_IFF.1 requires that all upstream information be allowed to flow from the upstream input interface port to the downstream output interface port. Additionally, FDP\_IFF.1 requires that no information flows from the downstream output interface port to the upstream input interface port. This is how the FDP\_IFF.1 and FDP\_IFC.2 help achieve the O.Confidentiality objective. |
| O.Integrity | FDP\_IFC.2 Information flow control policy  FDP\_IFF.1 Simple Security Attributes | O.Integrity is achieved through the diode functionality implemented in the TOE, which serves to enforce the FDP\_IFC.2 and FDP\_IFF.1 requirements.  FDP\_IFC.2 defines the policy of the *Unidirectional flow SFP*: User data cannot flow from the downstream port to the upstream port, while user data can flow from the upstream port via the TOE.  FDP\_IFF.1 identifies the rules for the TOE that are required to enforce the *Unidirectional Flow SFP*. FDP\_IFF.1 is based on the TOE interface port attributes and user data security attributes. These attributes are defined through FDP\_IFF.1 and are required to achieve the SFP rules and the O.Integrity objective.  FDP\_IFF.1 requires that all upstream information be allowed to flow from the upstream input interface port to the downstream output interface port. Additionally, FDP\_IFF.1 requires that no information flow from the downstream output interface port to the upstream input interface port. This is how the FDP\_IFF.1 and FDP\_IFC.2 help achieve the O.Integrity objective. |