Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/22

(Certification No.)

Prodotto: Distributed Services Platform v1.28.0-E-96

(Product)

Sviluppato da: Pensando Systems, Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 11 marzo 2022

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Distributed Services Platform v1.28.0-E-96

OCSI/CERT/CCL/09/2020/RC

Version 1.0

11 March 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	11/03/2022

2 Table of contents

1 Document revisions 5
2 Table of contents 6
3 Acronyms 8
4 References 10
4.1 Criteria and regulations 10
4.2 Technical documents 11
5 Recognition of the certificate 12
5.1 European Recognition of CC Certificates (SOGIS-MRA) 12
5.2 International recognition of CC certificates (CCRA) 12
6 Statement of certification 13
7 Summary of the evaluation 14
7.1 Introduction 14
7.2 Executive summary 14
7.3 Evaluated product 14
7.3.1 TOE architecture 15
7.3.2 TOE security features 16
7.4 Documentation 17
7.5 Protection Profile conformance claims 17
7.6 Functional and assurance requirements 17
7.7 Evaluation conduct 17
7.8 General considerations about the certification validity 18
8 Evaluation outcome 19
8.1 Evaluation results 19
8.2 Recommendations 20
9 Annex A – Guidelines for the secure usage of the product 21
9.1 TOE delivery 21
9.2 Identification of the TOE 21
9.3 Installation, initialization and secure usage of the TOE 22
10 Annex B – Evaluated configuration 23
10.1 TOE operational environment 23

11 Annex C – Test activity 24
11.1 Test configuration 24
11.2 Functional tests performed by the Developer 24
11.2.1 Testing approach 24
11.2.2 Test results 25
11.3 Functional and independent tests performed by the Evaluators 25
11.3.1 Testing approach 25
11.3.2 Test results 25
11.4 Vulnerability analysis and penetration tests 26

3 Acronyms

AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSC	Distributed Services Card
DSP	Distributed Services Platform
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPFIX	Internet Protocol Flow Information Export
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MAC	Media Access Control
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PP	Protection Profile
PSM	Policy and Services Manager
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
SAR	Security Assurance Requirement

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UI	User Interface
VM	Virtual Machine

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[DSC25] “Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition”, Version 3.0, Pensando Systems, Inc., August 2021

[DSC100] “Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition”, Version 2.0, Pensando Systems, Inc., August 2021

[DSPDBP] “Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide”, Version 1.7, Pensando Systems, Inc., August 2021

[DSPGDS] “Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Guidance Documentation Supplement”, Version 0.4, Corsec Security, Inc., 26 January 2022.

[DSPLDAP] “Pensando Policy and Services Manager, LDAP Server Configuration Guide”, Version 1.5, Pensando Systems, Inc., September 2020

[DSPRN] “Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E”, Version 3.1, Pensando Systems, Inc., August 2021

[DSPTG] “Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide”, Version 2.0, Pensando Systems, Inc., August 2021

[DSPUG] “Pensando Policy and Services Manager, Enterprise Edition User Guide”, Version 2.0, Pensando Systems, Inc., July 2021

[ETR] “Pensando Distributed Services Platform v1.28.0-E-96” Evaluation Technical Report, v1, CCLab Software Laboratory, 25 February 2022

[ST] “Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Security Target”, Version 0.6, Corsec Security, Inc., 26 January 2022

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all declared assurance components.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Distributed Services Platform v1.28.0-E-96”, also referred to in the following as “DSP”, developed by Pensando Systems, Inc.

The TOE is a combination of software and firmware providing network services at an interface level for servers in an enterprise datacenter. The platform consists of Distributed Services Cards (DSC) that are installed on each server and a Policy and Services Manager (PSM) cluster that manages the DSCs from a single point within the datacenter.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Distributed Services Platform v1.28.0-E-96” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Distributed Services Platform v1.28.0-E-96
Security Target	“Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Security Target”, Version 0.6 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Pensando Systems, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	1st December 2020
Evaluation ending date	25 February 2022

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE “Distributed Services Platform v1.28.0-E-96” is a combination of software and firmware providing network services at an interface level for servers in an enterprise datacenter. It is comprised of three instances of the Policy and Services Manager (PSM) node software and multiple instances of Distributed Services Card (DSC) firmware. The PSM node software and DSC firmware run on virtual machines (VMs) and DSC hardware in the operational environment, respectively. Both sets of these components run on separate server hosts.

The TOE has the ability to generate audit records for events pertaining to management of alert policies, alert destinations, TOE user accounts, authentication methods, roles, mirror sessions, and DSC hosts. It can also generate audit records for non-management activities including authentication, password changes, and node failures. All audit records contain the identity of the TOE user that performed the operation that caused an audit if it is applicable. Based on the generated audit events, the TOE can setup rules that will monitor for administrator-defined criteria to send alerts to the syslog server in the operational environment. These alerts can be used to notify TOE users of potential security violations. The TOE also provides two areas for reviewing the audit events generated by the TOE, which are restricted to TOE users with the role of AdminRole or with the All permission. The TOE utilizes the host's time source to provide reliable timestamps for audit events.

The TOE provides multiple areas of management within its interfaces including alert policies, alert destinations, accounts, roles, authentication methods, DSC hosts, and mirrored sessions. The TOE has one predefined role, AdminRole, and can maintain any number of administrator-defined roles. It can also preserve its secure state and will be fully functional in the event of a PSM node fails.

For a detailed description of the TOE, consult sects. 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE consists of multiple copies of DSC firmware and a three-node cluster of the PSM software. The same DSC firmware runs on multiple DSCs that differ in interface type and form factor but can be deployed in any datacenter server. The cards are managed by the PSM cluster via the DSC firmware.

Figure 1 illustrates the physical scope and the physical boundary of the TOE.

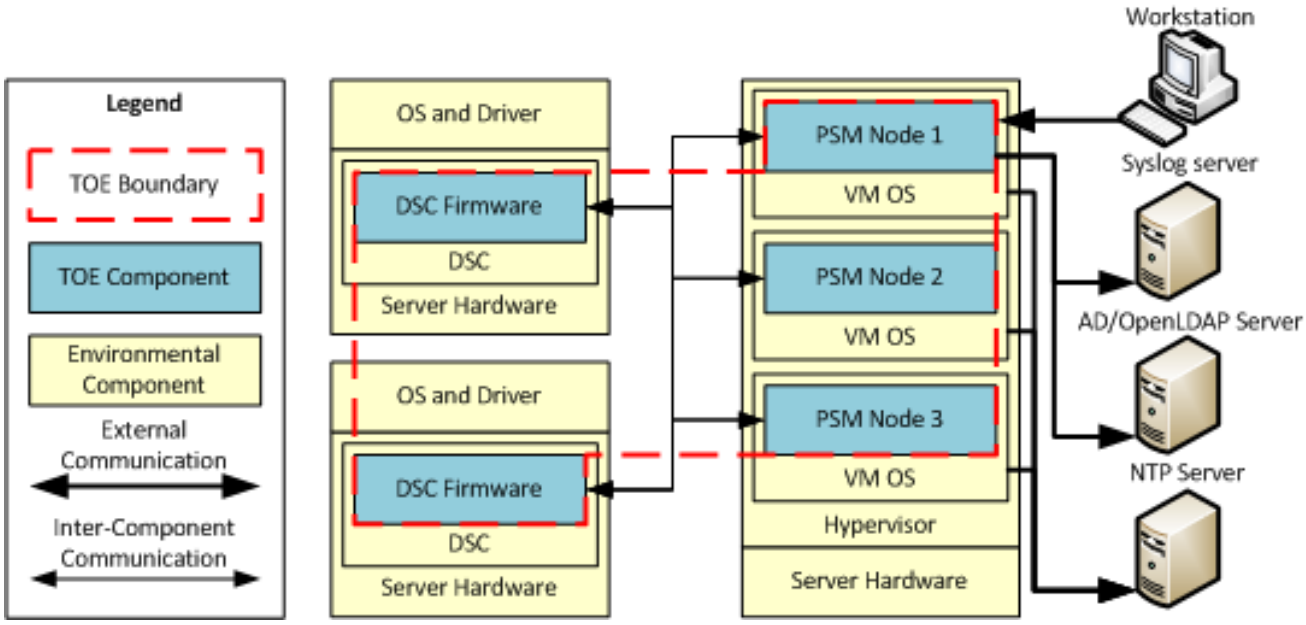

Figure 1 - Physical TOE Boundary

The PSM cluster allows for configuration and delivery of network data and observability policies to Pensando DSCs from a central location. Each node in the PSM cluster runs on a VM. A leader node is elected during the initial configuration and the nodes work in quorum when making decisions. The architecture of the nodes consists of Docker containers and microservices that are controller by Kubernetes. A PSM cluster can manage thousands of DSCs and their firmware.

The DSC firmware is installed on a Pensando Capri chip that is available on the Pensando DSC-25 and Pensando DSC-100 cards. The DSC firmware provides telemetry and analytics, mirroring, and IPFIX exports from the server on which they are installed to allow datacenter administrators to see and understand the network traffic at each server. The DSC firmware communicates with the PSM cluster through a TLS channel with mutual authentication.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Security Audit**: the TOE generates audit records for startup and shutdown of audit functions, authentication, password changes, node failures, and management operations. It is able to associate audit records with the TOE user that caused the audited event. Audit records are presented in a human-readable manner and are only viewable if the account has the AdminRole assigned to it or a role with the All permission assigned to it.
  The TOE will also monitor audit events for administrator-defined criteria and send an alert to a syslog server once the criteria is met.

- **Identification and Authentication**: The TOE maintains the following security attributes for each local account: full name, email, roles, login name, password, and authentication type. When setting a password, the TOE will also enforce its password complexity rules. When typing a password, the TOE obfuscates the characters using the bullet character.
  The TOE requires authentication and identification before any action can be taken within the TOE except for viewing the internal REST API documentation. When authenticating to the TOE, TOE users can use one of the following authentication methods: local and directory-based authentication.

- **Security Management**: the TOE provides management functions for security-related functionality including the management of alert policies, alert destinations, accounts, roles, authentication methods, mirror sessions, and DSC hosts. The TOE creates the default AdminRole when first setup but is capable of maintaining any administrator-defined role created by the TOE users.

- **Protection of the TSF**: the TOE preserves a secure state when a PSM node fails. While a node is down, the TOE still provides all of its functionality. The TOE provides reliable timestamps by utilizing the system's time, which is synchronized to an NTP server.

- **Resource Utilization**: the TOE ensures that it provides all of its functionality while a PSM node has failed.

- **TOE Access**: while using the TOE's Web UI, TOE users have an option to terminate their own session by clicking on the sign out link.

- **Trusted Path/Channel**: the TOE provides trusted channels between itself and the AD/OpenLDAP server in the operational environment using TLS connections. The TOE also provides trusted paths between itself and remote TOE users using TLS connections to secure authentication and all TSF-related activities.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 25 February 2022 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 8 March 2022. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Distributed Services Platform v1.28.0-E-96" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	Pass
Tests	**Class ATE**	Pass

Assurance classes and components		Verdict
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “Distributed Services Platform v1.28.0-E-96” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions described in sect. 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([DSPRN], [DSPUG], [DSPLDAP], [DSPTG], [DSPDBP], [DSC25], [DSC100], [DSPGDS]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The TOE includes the Distributed Services Card (DSC) firmware v1.28.0-E-96, the Policy and Services Manager (PSM) software v1.28.0-E-96, and the guidance documentation listed in sect. 9.3.

The TOE Developer, Pensando Systems, Inc., provides the DSC firmware to customers by physical and electronic packages while the PSM software is only provided in electronic format.

For physical packaging, the DSCs are packaged at the manufacturing site. The DSC firmware is installed on a DSC and put into an anti-static bag. Twelve of the bagged cards are placed into a single box for shipping. Each DSC is labeled with its product information and MAC address. The product information is also printed on a label and attached to the box. Customers send their designated shipping carrier to go to the Pensando factory and pick up the DSCs that the customers purchased.

For electronic packaging, both the DSC firmware and PSM software are available separately to customers in .tgz files to be downloaded from the Pensando Support Portal (a Pensando Support Portal account is needed). The TOE documentation can also be downloaded from the Pensando Support Portal.

9.2 Identification of the TOE

The TOE software, firmware, and documentation are uniquely versioned for easy identification.

Customers must first verify their tracking information when receiving physical hardware. The product labels on the boxes will also be checked to confirm proper products and serial numbers.

When receiving the TOE components electronically, the SHA-256 checksums can be used to verify that the .tgz files have not been tampered with. The checksums are available with the files on the Downloads page of the Pensando Support Portal.

To confirm the correct TOE version after installation, the customer can view the PSM software version from the Web UI by clicking on the “Information” icon in the top right and selecting the “About” option. The version information is listed as “Build Version”. To view the DSC firmware version, click on the “System” menu on the left and select the “DSC” sub-menu. The version information is listed in the “Distributed Services Cards” table in the “Version” column.

9.3 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E [DSPRN]
- Pensando Policy and Services Manager, Enterprise Edition User Guide [DSPUG]
- Pensando Policy and Services Manager LDAP Server Configuration Guide [DSPLDAP]
- Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide [DSPTG]
- Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide [DSPDBP]
- Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition [DSC25]
- Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition [DSC100]
- Pensando DSP Guidance Documentation Supplement [DSPGDS]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Distributed Services Platform v1.28.0-E-96”, developed by Pensando Systems, Inc.

The name and version number uniquely identify the TOE and its components, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The components of the TOE in the evaluated configuration are:

- Pensando Distributed Services Card Firmware v1.28.0-E-96 running on the Capri chip that is attached to the DSC-25 and DSC-100 in the operational environment on separate servers.
- Pensando Policy and Services Manager v1.28.0-E-96 running in a three-node cluster on VMs in the operational environment.

The following functionalities are not part of the evaluated configuration of the TOE:

- functionality provided by the DSC driver on the host’s OS;
- functionality that is covered by only the Enterprise Pro service level agreement;
- RADIUS authentication.

10.1 TOE operational environment

The TOE relies on the operational environment to properly function. To host the PSM node cluster, a PSM Host Server must be available in the operational environment, running a hypervisor on which the three PSM node VMs are loaded. To run the DSC Firmware, the DSC-25 and DSC-100 cards are needed, which are installed into separate DSC Host Servers in the operational environment.

The TOE also relies on external servers to execute functionality including an NTP server for time synchronization, an AD or OpenLDAP server for directory-based authentication and resolving expanded group, and a syslog server for receiving alerts.

TOE users will also be able to manage the TOE from a workstation in the operational environment that connects to the PSM cluster.

Please refer to sect. 1.5 of the Security Target [ST] for more details on software and hardware minimum requirements for the TOE operational environment

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Evaluators executed all the test cases on the test environment which was provided by the Developer. The Developer also provided all the resources needed for testing.

The TOE test setup was prepared according to the Developer's test documentation. The evaluated version of the TOE was installed in a three-node cluster using VMs running on VMware ESXi. Pensando Distributed Services Card Firmware is running on a Capri chip that is attached to one DSC-25 and one DSC-100 on separate servers. The test environment included the following items:

- a general-purpose computer running Kali Linux 2021.3 Release;
- a server running the VMware ESXi version 6.7.0 hypervisor (Dell PowerEdge R640);
- one DSC-25 card and one DSC-100 card hosted on two separated servers (Dell PowerEdge R640 and HPE ProLiant DL360);
- network infrastructure;
- a server running Microsoft Windows Server 2019 Standard Edition providing NTP functionality and syslog collector (Kiwi Syslog Server 9.7.2.1).

The Evaluators installed the TOE following the steps described in sect. 2.2 "Secure Installation" of the document [DSPGDS].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer's test approach is to provide a specific functional test for each behavioral implication of the SFRs claimed in the Security Target [ST]. The Developer's tests focus on covering all TOE's security behaviors and ensuring that the functional testing is thorough without being unnecessarily detailed.

The Developer's test documentation includes a total of 5 test cases mapping the TSFIs listed in the Functional Specification document (Web UI and REST API).

All of the defined TSFIs are exercised by the following test cases:

- Test Case 01 – User Access
- Test Case 02 – Alerts, Events, and Audit Events
- Test Case 03 – REST API
- Test Case 04 – Secure Connections
- Test Case 05 – Node Failure

The Evaluators analysed the Developer's functional tests and coverage and found them to be complete and accurate.

11.2.2 Test results

For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and expected test results.

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators ran all tests on the test environment provided by the Developer. The TOE test setup was prepared according to the Developer's test plan and the preparative procedures supplied in the document [DSPGDS]. Before initiating the testing activity, the Evaluators verified that the test environment was properly set up and the TOE was configured correctly and in a known state.

The Evaluators repeated all the steps in each of Developer's test case and checked the expected results.

To further exercise the REST API and WEB UI TSFIs, the Evaluators devised the following additional test cases, derived from Developer's test cases:

- Evaluator Test Case 01 – Fulfilment of password complexity requirement
- Evaluator Test Case 02 – Verifying syslog messages with Wireshark
- Evaluator Test Case 03 – Leader node change

11.3.2 Test results

All Developer's tests were run successfully. The Evaluators verified the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators passed, i.e., all the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE test setup already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluators first performed a search of public domain sources to identify potential vulnerabilities in the TOE. This activity revealed a number of potential vulnerabilities in the Elasticsearch package.

The Evaluators examined the above vulnerabilities and concluded that they are not applicable to the TOE. Elasticsearch (port 9200) is used in the TOE for exchanging data between PSM cluster nodes. This communication is protected by TLS with certificate-based authentication and open ports are not reachable from outside the TOE.

The Evaluators then focused on the ST, guidance documentation, functional specification, TOE design and security architecture description evidence to identify possible potential vulnerabilities in the TOE. This analysis revealed the following areas of concern:

- Brute Force attack to the PSM login page
- Remote Code Execution in the System Upgrade functionality

The Evaluators conducted penetration tests to verify the exploitability of the above potential vulnerabilities in the TOE's operational environment, considering a Basic attack potential.

Based on the vulnerability analysis and the penetration testing results, the Evaluators concluded that none of the identified potential vulnerabilities are applicable to the TOE. The TOE is therefore resistant to an attack potential of Basic in its intended operational environment. No exploitable or residual vulnerabilities have been identified.