Reference: 2023-19-INF-4706- v1
Target: Limitada al expediente
Date: 03.02.2026

Created by: CERT15
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-19**
TOE	**PSTgateways Framework version 4.16.8-A**
Applicant	**B82015181 - Autek Ingenieria S.L.U.U**

References

[EXT-8655] 20230607_2023-19_solicitud_certificacion

[EXT-9910] 2025-10-27_2023-19_ETR_v3

Certification report of the product PSTgateways Framework version 4.16.8-A, as requested in [EXT-8655] dated 07/06/2023, and evaluated by Layakk Seguridad Informatica S.L., as detailed in the Evaluation Technical Report [EXT-9910] received on 27/10/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product PSTgateways Framework version 4.16.8-A.

The TOE consists of PSTgateways Framework software that, through two individual devices, provides true network separation.

Developer/manufacturer: Autek Ingenieria S.L.U.U

Sponsor: Autek Ingenieria S.L.U.U

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Layakk Seguridad Informatica S.L..

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL4+ (ALC_FLR.3+AVA_VAN.5).

Evaluation end date: 16/12/2025.

Expiration Date[1]: 16/01/2031

All the assurance components required by the evaluation level EAL4+ (augmented with ALC_FLR.3+AVA_VAN.5) have been assigned a “PASS” verdict. Consequently, the laboratory Layakk Seguridad Informatica S.L. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+ (ALC_FLR.3+AVA_VAN.5), as defined by the Common Criteria v3.1 R5 and the the Common Evaluation Methodology V3.1R5.

Considering the obtained evidences during the instruction of the certification request of the product PSTgateways Framework version 4.16.8-A, a positive resolution is proposed.

TOE SUMMARY

‘PSTgateways’ is a family of boundary protection devices. They are application-level gateways, which allow the secure transmission of information between networks located in two different security domains.

The PSTgateways systems provide real network separation by using two individual appliances (each one connected to one of the aforementioned networks). Each appliance acts as the communication

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

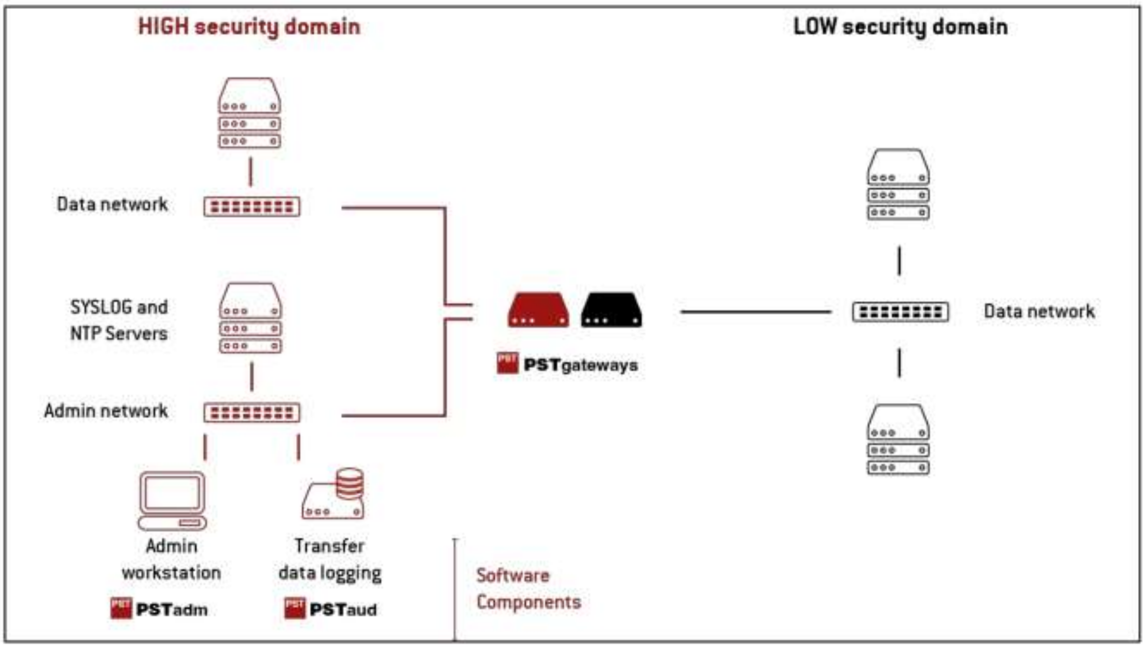
end-point in its associated security domain. This architecture provides a complete break of the TCP/IP stack protocols.

The two appliances constitute the only communication path between the internal (high security domain) and the external network (low security domain). The communication between them is performed through a passive data transfer device which is part of the PSTgateways technology.

All PSTgateways systems share a common architecture and a common base software (PSTgateways Framework) but differ in the set of 'data flow services' (or simply 'services') that they support. Each service supports the transfer of a type of information (e.g.: file transfer, e-mail, etc.), using standard protocols to communicate with both data networks. The services are completely independent from each other, and when possible offer a one way data flow.

All services are organised into channels, allowing independent and parallel handling of multiple data flows with individual settings per channel.

The following diagram illustrates the general PSTgateways deployment components:



A PSTgateways system consists of:

- PSTgateways appliances: two appliances (PSTi and PSTe), each consisting of hardware and firmware elements:
  - The PSTgateways appliance's hardware includes the server and other specific HW components required (not part of the TOE)
  - Each firmware includes the following appliance specific (PSTi or PSTe) components:
    - A minimum operating system.
    - The local administration console, named 'Shell'.

  - The common (service-independent) software component of PSTgateways, named ‘Core’.
  - The service modules.
- A firmware management tool for each appliance, named ‘Restore’.
- Additional software intended for administration and audit event management: ‘PSTadm’ and ‘PSTaud’ software components. This software is to be deployed on general purpose workstations.

The described common (service-independent) software component of the PSTgateways product (‘Core’), together with the local administration console (‘Shell’), the firmware management tool (‘Restore’) and their dependencies, constitute the TOE to be evaluated (PSTgateways Framework), which is described in this document.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4+ and the evidences required by the additional component ALC_FLR.3 and AVA_VAN.5 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1

ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

REQUISITOS FUNCIONALES DE SEGURIDAD
FAU_GEN.1
FAU_GEN.2
FAU_SAR.1/Sec
FAU_SAR.1/Op
FAU_SAR.1/TD
FAU_SAR.2
FAU_STG.EXT1
FAU_STG.1
FCS_CKM.1
FCS_CKM.2
FCS_CKM.4
FCS_COP.1/Cipher-AES
FCS_COP.1/Cipher-CHACHA20
FCS_COP.1/Cipher-RSA
FCS_COP.1/Hash-SHA
FCS_COP.1/KeyedHash
FCS_COP.1/Signature-ECDSA

FCS_COP.1/Signature-RSA
FCS_TLSC_EXT.1
FCS_TLSC_EXT.2
FCS_TLSS_EXT.1
FCS_TLSS_EXT.2
FCS_RBG_EXT.1
FDP_ACC.2
FDP_ACF.1
FDP_IFC.2/IN
FDP_IFC.2/OUT
FDP_IFF.1/IN
FDP_IFF.1/OUT
FIA_AFL.1
FIA_PMG_EXT.1
FIA_UAU.EXT1
FIA_UIA_EXT.1
FIA_UAU.7
FIA_X509_EXT.1
FIA_X509_EXT.2
FMT_MOF.1/LocalConfFuncs
FMT_MOF.1/RootConfFuncs
FMT_MSA.1/LocalConfAttr
FMT_MSA.1/RootConfAttr
FMT_MSA.3
FMT_MTD.1
FMT_SMF.1

FMT_SMR.2
FPT_APW_EXT.1
FPT_FLS.1
FPT_ITC.1
FPT_ITT.1
FPT_SKP_EXT.1
FPT_STM.EXT1
FPT_TRC.1
FPT_TST.EXT1
FPT_TUD_EXT.1
FRU_FLT.1
FTA_MCS_EXT.1
FTA_SSL.EXT1
FTA_SSL.3
FTA_SSL.4
FTA_TAB.1
FTP_ITC.1/Syslog
FTP_ITC.1/PSTaud
FTP_TRP.1

IDENTIFICATION

Product: PSTgateways Framework version 4.16.8-A

Security Target: PSTgateways Framework Security Target Lite 1.0

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL4+ (ALC_FLR.3+AVA_VAN.5).

SECURITY POLICIES

The use of the product PSTgateways Framework version 4.16.8-A shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 (“Organisational security policies”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.4 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product PSTgateways Framework version 4.16.8-A, although the agents implementing attacks have the attack potential according to the High Level of AVA_VAN.5 of EAL5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.2 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE functionality is implemented in the following software components:

- The PSTgateways Framework ‘Core’ component, version 4.16.8, which is the common (service-independent) software component of the PSTgateways products. Part of the ‘Core’ runs on the internal appliance (PSTi) and part on the external appliance (PSTe).
- The PSTgateways Framework ‘Shell’ component version 1.6.3, which is the local administration console for each appliance. Part of the ‘Shell’ runs on the internal appliance (PSTi) and part on the external appliance (PSTe).
- The PSTgateways Framework ‘Restore’ component, version 2.4.2, which is the firmware management tool (‘Restore’) for the internal (PSTi) and external (PSTe) appliances.
- The PSTgateways Framework ‘Dependencies’, version 3.5.4, which are the cryptographic libraries used by the other TOE components to perform cryptographic operations.

The security functions that are implemented by the TOE are described in the following paragraphs, grouped by type:

- TOE Administration:

  The TOE administration can only be performed by defined administrator users, whose associated role is explained in the following paragraphs.

  The TOE implements a hierarchy of administrator roles:

  - One local administrator role, which is a human user with physical access to the TOE, and whose password for using the local administration console (‘Shell’) is initialised during the initial configuration process. The local administrator functions are always exercised from the appliance local physical console.
  - Four remote administrator roles: root, security, service and monitoring. The remote administrators can perform their functions by means of the admAPI. This API is accessible by using a TLS channel and so the administration data communication is managed in a channel that is isolated from the service data flows.

- Identification and authentication of users:

  For the local administrator, the identification is implicitly made by the fact that physical access to the console is required and the physical environmental restrictions will apply. Authentication of that user against the ‘Shell’ component is performed by using a password that has previously been initialised during the initial configuration process. For the ‘Shell’ component, the only action allowed to the local administrator without authentication is the system status check (any other action is not allowed before the Local Administrator has been authenticated to the system). The ‘Restore’ component is accessible without authentication because the local user has to boot from the appliance's DVD and that physical access is considered an implied authentication.

The mutual identification and authentication between the remote users and the TOE relies on a PKI infrastructure provided externally to the TOE.

For remote administrator users, the identification is made through the use of the Common Name of user certificates. The user is required to establish a TLS session with the TOE prior to communicate with it. During this establishment, he must present his certificate to the TOE and the TOE must be able to validate it. The TOE identifies the user using his certificate's Common Name (CN) and authenticates him by verifying his certificate (the TOE has been provisioned with the CA Certificate of the issuing CA by the local administrator during the initial configuration procedure, so it can also authenticate the user). The TOE also authenticates itself to the user during the TLS session establishment by using its appliance certificate. If the identification or the authentication fails, the user is not allowed to interact with the TOE.

- Audit:

  The TOE generates two types of audit events:

  - System Events are generated by the TSF and stored in local event files in the internal appliance PSTi. They are also sent to the configured syslog server(s). These events can also be accessed by using admAPI. There are two types of System Events: Security System Events and Operation System Events.

    The TOE stores the System Events in files that are rotated accordingly with the established policy that is based on file size and maximum file number. The latest event file is overwritten when the maximum file number is reached (a System Event is generated in this case).

    The TOE provides access to the System Events by the use of the admAPI that can be securely accessed by the remote PSTadm workstation. This information is in the form of a human-readable text log file. The access through PSTadm requires the previous establishment of a secure communication channel (using TLS 1.2 or higher). The access to Security System Events is restricted to the Security Administrator roles and the access to the Operation System Events is restricted to Service Administrator roles.

    The System Events can also be sent by the TSF to syslog servers located in the High Security Domain: one for the Operation System Events and one for the Security System Events (Both types of events can be sent to the same server). These transfer operations can also be configured to be protected by TLS 1.2 or higher, that provides mutual authentication, integrity protection and confidentiality protection.

  - Data Transfer Logging Events are directly related with each data flow transfer. Each of these events is associated to a particular service data transfer and the information in them is specific for each service. The Data Transfer Logging Events are sent by the TSF to the configured PSTaud server and they are not accessible through the admAPI.

Data Transfer Logging Events are sent by the TSF to the PSTaud server located in the High Security Domain using the audAPI provided by the PSTaud server, if the Security Administrator has configured the CN (Common Name) of the certificate associated to the remote PSTaud service. The TSF securely transmits these events to the PSTaud server by establishing a secure communication channel (TLS 1.2 or higher) with it, which provides mutual authentication, integrity protection and confidentiality protection. This information is stored by the PSTaud server and is presented to the user accessing the PSTaud software in a structured way.

- TOE access protection:

  The TOE is able to limit the maximum number of administrative connections to prevent DoS attacks coming from the internal network.

- Protection of the TOE:

  The integrity protection of the TOE firmware is provided through the following mechanisms:

  - The TOE is installed in and runs from a read-only partition, so modifications of the TOE are not possible.
  - For each appliance, the local administrator can verify the partition integrity (and therefore the TOE integrity that is located inside it) by booting from the appliance DVD and using the provided TOE firmware management tool ('Restore') to perform the verification of the integrity of the appliance's firmware.

  Every TOE firmware upgrade comes inside a firmware image with an associated signature file. This firmware image signature is verified by the TOE firmware management tool ('Restore') prior to its installation.

  The TOE verifies the signature of the license associated to the PSTgateways particular product. The following features are activated by license:

  - Available services
  - High availability mode

  For some specific services, some parametrisation data can also be loaded from the local administration console ('Shell'). In this case, the parametrisation data is protected by the use of a digital signature.

- High availability:

  The TOE can operate in a High Availability configuration by using two redundant appliances (one in each security domain). The following functionalities apply only when the High Availability configuration is in place.

In High Availability operation mode, one of the internal appliances ("PSTi") must be configured as primary. From that point on, all administration tasks are performed over the primary PSTi, with the exception of "RebootSystem" command and monitoring tasks, which can be performed also on the secondary PSTi.

The TOE uses a synchronisation channel using a dedicated TLS channel between the two instances of the PSTi appliances (located in the High Security Domain) to maintain synchronisation between the redundant parts of the system.

The High Availability feature can be configured in two modes, that are enabled exclusively by the license associated to the system: Active-Active and Active-Passive modes.

The TOE keeps synchronised the configuration, global operating status as well as service operational status.

When the TOE detects a fault condition on any of the PSTgateways systems, it reconfigures the system to rebalance the data flow service load to the healthy system.

When the fault condition disappears:

- In Active-Active mode, the TOE will re-establish the original system configuration.
- In Active-Passive mode, the element that took over the load will continue to do so.

PHYSICAL ARCHITECTURE

The TOE is composed of the following elements:

TOE Component	**Details**	
PSTgateways Framework 'Core' Version 4.16.8	File name	psti
	File format	binary
	SHA256	f6f98ebb1774779a19893e157a6ecc2413c1b185e21b82b0dc07dcabc8401078
	Distribution	PSTi
	File name	servicesi
	File format	binary
	SHA256	ce18b5dc70bfcd89aa0ba67af7f4d66c3ca90681844234844d677a1e468ab34d
	Distribution	PSTi

	File name	pste
	File format	binary
	SHA256	bfb7887d6048664a735ee07c7427a7ae7e0b7f212635e02027083e242201cbdd
	Distribution	PSTe
	File name	servicese
	File format	binary
	SHA256	d7e42c2bc52e9e4385414521be69a95668f9829b835aa1d1857741a2c9cf28ac
	Distribution	PSTe
PSTgateways Framework ‘Shell’ Version 1.6.3	File name	pstshelli
	File format	binary
	SHA256	a21b18aec6a64f4836894f2a3b771617723de95116f8ca5d34c7eb6e53f66862
	Distribution	PSTi
	File name	pstshelle
	File format	binary
	SHA256	553a70adeb38cd131784c9d2a95e896297e5ce95c8b8579efe596406914796ac
	Distribution	PSTe
PSTgateways Framework ‘Restore’ Version 2.4.2	File name	restore
	File format	binary
	SHA256	0d0c7096c6b7716fabdc7be459c255be6186688cbf7078db5865551b3d6401c9
	Distribution	DVD-ROM de PSTi y DVD-ROM de PSTe
PSTgateways Framework ‘Dependencies’	File name	libssl.so
	File format	binary
	SHA256	3f3d7fa76a3c47c7fd303416f769d1ecfebb10428904e048e111

Version 3.5.4		1d3a50593ea3
	Distribution	PSTi, DVD-ROM de PSTi y DVD-ROM de PSTe
	File name	libcrypto.so
	File format	binary
	SHA256	eda3b2a95a3db44826eadd3355b64c448d244e8bf3e2571151fa19dc61955238
	Distribution	PSTi, DVD-ROM de PSTi y DVD-ROM de PSTe

Due to the distributed and intertwined nature of the TOE, the physical components of the TOE are contained in physical entities that contain both physical components of the TOE and other non-TOE components.

The TOE components included in the persistent storage of each appliance (PSTi and PSTe) are pre-installed by personnel from Autek Ingeniería S.L.U. The appliances are then packed and sent to the customer using a shipping service.

The TOE components are also included in three read-only media (DVD/CD) that are sent to the customer using a shipping service and whose integrity can be verified against a hash that is sent inside an email that is digitally signed by Autek Ingeniería S.L.U.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

DOCUMENT	VERSION	UNIQUE IDENTIFIER (SHA256)
Security Target Lite	1.0	3190a3ebc04c786c5ae2a07dece9e80e7b176c58a6b8f609108f88413c6728fb
PSTgateways - Installation and Deployment Guide	12	60742fe3fa1eae6228adc0dc77170e75f729f171b2cd37562aa0232617da8f3c
PST boundary protection devices – Operation Guide	11	d522050bf47356c624f89edcd0d8ceb7aeaa60b07837dc52e8350212097f6841
PSTgateways Framework Secure Use Procedure	0	d238a394c71a3bb6199a694136dd32e8fb53bf0b33d887606d167074093f2e85

PRODUCT TESTING

In order to define an independent testing plan that complements the tests carried out by the Developer, the Laboratory first analyzes the level of coverage of the tests carried out by the Developer for each of the interfaces exposed by the TSF (TSFI) based on their complexity and relevance for compliance with SFRs:

- TSFIs iAdm, iSrvInt and iSrvExt

  The Laboratory considers these interfaces to be the most complex, as they offer a large number of possible interactions with the TOE with potential consequences for the security of the TOE since they allow, for example, the configuration or reconfiguration of the TSF itself or the transfer of information between the two security domains.

  Therefore, although the Develope's test plan has extensively covered these interfaces, the Laboratory has opted to perform additional tests.

- TSFIs iRestore and iShellInt

  The Laboratory considers that these interfaces have a low level of complexity and that access to them is highly restricted (physical access to the equipment console is required), but at the same time they have a significant potential impact on the security of the TOE if any of their functions are implemented incorrectly.

  Therefore, although the Developer's test plan has extensively covered these interfaces, the Laboratory has decided to carry out additional tests (although fewer than those focused on iAdm).

- TSFIs iMon, iAud and iShellExt

  The Laboratory considers these interfaces to be relatively simple, as some are output-only interfaces that the TOE uses solely to send events, while others allow a very limited set of commands, all of which are status queries. Although the reported events are of great importance and their protection is therefore fundamental, the operation of these interfaces themselves is relatively simple.

  Therefore, the Laboratory considers the tests performated by the Developer of these interfaces sufficient to verify that the TOE implements them correctly, and the Laboratory does not propose any additional functional tests on them.

In summary, the Laboratory performs independent testing on 62,5% of the available TSFIs.

For the functional tests repeated by the Laboratory, it was decided to repeat 112 of the 1.505 tests performed by the Developer, representing approximately 8% of the total. However, many of the tests performed by the Developer are not directly related to any SFR. Compared to the subset of tests the Developer idetifies as related to SFR (223 tests), the percentage represented by the tests chosen by the Laboratory for retesting is approximately 50%.

The Laboratory has selected a sample of 112 tests based on the following criteria:

- Since all TSFIs play an important role in SFR compliance, it was decided to run tests on every TSFI without exception. Furthermore, the TOE does not have an excessive number of TSFIs and all of them can be tested, as indicated in [CC-CEM], section [1443] b).
- Approximately 8% of the total tests that the Developer has performed on each TSFI are selected, as indicated by [CC-CEM] in section [1888] for very large sets.
- The tests selected for the sample examine security functionalities in the TOE that meet the security objectives proposed in the ST and protect it against the described threats, as indicated in [CC-CEM] in section [1886].
- The tests verify functionality that contributes to SFR compliance.
- In addition, some of the tests selected for the sample requires a series of steps that, in turn, involve testing other functionalities. These steps are, in themselves, independent tests. Thus, by running just one test, several of those initially proposed by the Developer are also tested.

For the AVA_VAN.5 assessment of a TOE during the vulnerability analysis, the Laboratory reviews the complete CWE list and selects those weaknesses that could apply to the TOE being evaluated. Then, for each occurrence, attack scenarios are prepared on the patterns listed in CAPEC.

Since the evaluation focuses on software security, specifically the ‘Software Development’ and ‘Research Concepts’ views of CWE are considered, as well as the ‘Software’, ‘Communications’ and ‘Supply Chain’ views of CAPEC, as these are the most appropiate for software analysis.

Using the list of attacks scenarios, the attack potential of each one is calculated, eliminating those that do not correspond to the requested AVA_VAN level, and finally, tests are carried out trying to exploit all those that are within the considered attack potential.

Complementing this strategy, the Laboratoy also analyzes the TOE source code for any applicable CWE and even performs a static code analysis.

Furthermore, with the knowledge of the TOE acquired throughout the evaluation, the Laboratory is also able to propose other attack scenarios based on its operation.

EVALUATED CONFIGURATION

The TOE has been evaluated using the following configuration options:

- The configuration of the system has followed the rules in the document ‘PSTgateways Framework Secure Use Procedure’.
- Both HA and non-HA modes of the system were evaluated.
- In HA mode, both Active-Active and Active-Passive operation modes were evaluated.

- Only key sizes that provide a cryptographic strength of 128 bits or higher were used in the evaluation.

EVALUATION RESULTS

The product PSTgateways Framework version 4.16.8-A has been evaluated against the Security Target PSTgateways Framework Security Target Lite 1.0

All the assurance components required by the evaluation level EAL4+(ALC_FLR.3+AVA_VAN.5) have been assigned a “PASS” verdict. Consequently, the laboratory Layakk Seguridad Informatica S.L. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4+ (ALC_FLR.3+AVA_VAN.5), as defined by the Common Criteria v3.1 R5 and the Common Evaluation Methodology V3.1R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

Since all evaluation assurance activities performed during the evaluation yielded positive results, including the tests and the vulnerability analysis, the Laboratory recommends the use of the TOE in its evaluated configuration.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product PSTgateways Framework version 4.16.8-A, a positive resolution is proposed.

GLOSSARY

API	Application Programming Interface
CC	Common Criteria
TOE	Target of Evaluation
PKI	Public Key Infrastructure

TSF	TOE Security Functionality
TSFI	TSF Interface
SFR	Security Functional Requirement
ST	Security Target
CD	Compact Disc
DVD	Digital Versatile Disc
DVD-ROM	Digital Versatile Disc – Read Only Memory
TLS	Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

SECURITY TARGET LITE

Along with this certification report, the lite security target of the evaluation is available in the Certification Body:

- PSTgateways Framework Security Target Lite 1.0

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

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

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.