REF: 2013-17-INF-1269 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 05.02.2014	Approved by: TECNICO

CERTIFICATION REPORT

File: 2013-17 PSTfile

Applicant: B82015181 Autek Ingenieria S.L.

References:

[EXT-2221] PSTfile Certification request.

[EXT-2333] PSTfile Evaluation Technical Report.

The product documentation referenced in the above documents.

Certification report of the product PSTfile, as requested in [EXT-2221] dated 26/06/2013, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-2333] received on 25/10/2013.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product PSTfile v4.4.2.

The TOE is part of a complete product called 'PSTfile Gateway'. The product is made up of two 'appliances' (including hardware, generic software (operating system) and specific software) and additional software installed on general purpose computers.

The TOE consists of specific software that is pre-installed on the appliances and provides the functionality of a secure application level file gateway. In addition, the TOE includes a software tool stored on an auto-start CD-ROM that allows updating of the software installed on the appliances and verifying their integrity.

The use of the TOE is to transfer files (FTP, FTPS and SMB file transfer protocols are supported) between two isolated networks whilst maintaining the networks in isolation and guaranteeing that the only information transferred between the networks is the one transferred by the gateway itself. To do this, the gateway discontinues the TCP/IP protocol stack at all levels.

The TOE provides the security level of EAL2 augmented with ALC_FLR.1.

Developer/Sponsor:

Autek Ingeniería, S.L.

Avda. de Burgos 9, oficina 1.

28036 Madrid

SPAIN

Certification Body:

Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF:Epoche & Espri S.L.U..

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r4 / CEM v3.1 r4 / EAL2+ (ALC_FLR.1).

Evaluation end date: 25/10/2013.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2+ (ALC_FLR.1), as defined by the Common Criteria v3.1 r4 ([CC_P1], [CC_P2] and [CC_P3]) and the Evaluation Methodology [CEM].

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Considering the obtained evidences during the instruction of the certification request of the product PSTfile v4.4.2, a positive resolution is proposed.

TOE SUMMARY

The TOE is part of a complete product called 'PSTfile Gateway'. The product is made up of two 'appliances' (including hardware, generic software (operating system) and specific software) and additional software installed on general purpose computers.

The TOE consists of specific software that is pre-installed on the appliances and provides the functionality of a secure application level file gateway. In addition, the TOE includes a software tool stored on an auto-start CD-ROM that allows updating of the software installed on the appliances and verifying their integrity.

The use of the TOE is to transfer files (FTP, FTPS and SMB file transfer protocols are supported) between two isolated networks whilst maintaining the networks in isolation and guaranteeing that the only information transferred between the networks is the one transferred by the gateway itself. To do this, the gateway discontinues the TCP/IP protocol stack at all levels.

The two networks are not equivalent: one is considered as having a higher security level or classification. The system is administered from the secure network which is also referred to as the internal network. Only digitally signed files will be transferred from the internal to the external network.

A high-availability version of the TOE exists that allows service to be maintained in the event of hardware configuration are described separately. Unless mentioned explicitly, documentation applies to both configurations. Sections that apply to the high-availability configuration only will state this explicitly.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.1, according to [CC_P3].

Assurance Class	Assurance Components
ASE: Security Target evaluation	CCL.1 Conformance claims ECD.1 Extended components definition INT.1 ST introduction OBJ.2 Security objectives REQ.2 Derived security requirements SPD.1 Security problem definition

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

	TSS.1	TOE summary specification
AGD: Guidance documents	OPE.1	Operational user guidance
	PRE.1	Preparative procedures
ALC: Life-cycle support	CMC.2	Use of a CM system
	CMS.2	Parts of the TOE CM coverage
	DEL.1	Delivery procedures
	FLR.1	Basic flaw remediation
ADV: Development	ARC.1	Security architecture description
	FSP.2	Security-enforcing functional specification
	TDS.1	Basic design
ATE: Tests	COV.1	Evidence of coverage
	FUN.1	Functional testing
	IND.2	Independent testing - sample
AVA: Vulnerability Assessment	VAN.2	Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the [CC_P2]:

Class	Components	
FMT	SMR.2	Restrictions on security roles
	SMF.1	Specification on Management Functions
	MSA.1/IFF	Management of security attributes
	MSA.1/ACC	Management of security attributes
	MSA.3/IFF	Static attribute initialization
	MSA.3/ACC	Static attribute initialisation
FIA	UID.1	Timing of identification
	UAU.1	Timing of authentication
FDP	ACF.1	Security attribute based access control
	ACC.2	Complete access control
	IFC.2/IN	Complete information flow control
	IFF.1/IN	Simple security attributes
	IFC.2/OUT	Complete information flow control
	IFF.1/OUT	Simple security attributes
FAU	GEN.1	Audit data generation
	SAR.1	Audit review
	SAR.2	Restricted audit review
FRU	FLT.1	Degraded fault tolerante

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

FPT	FLS.1	Failure with preservation of secure
	TRC.1	Internal TSF consistency
	ITT.1	Basic internal TSF data transfer protection

IDENTIFICATION

Product: PSTfile v4.4.2

Security Target: Declaración de seguridad PSTfile. Revisión 3. 07/10/2013.

Security Target Lite: Security Target Lite. Revision 3.1. 31/01/2014

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 release 4

CEM v3.1 release 4

EAL2+ (ALC_FLR.1).

SECURITY POLICIES

The use of the product PSTfile v4.4.2 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. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: P.SEP

Both networks must remain separate. There should be no possibility of establishing TCP/IP connections between the two networks.

Policy 02: P.CRYPT

The TOE will use cryptography for the following purposes:

- The information (regarding configuration and the one processed by the system) which is stored on the disk drives in the units (PSTi and PSTe) must be encrypted.
- Communications with PSTadm for remote administration and with PSTaud for logging of auditing data must be encrypted.
- The user information sent in the outgoing data flow (from the internal to the external network) must be authorized using a digital signature.

Policy 03: P.ROLES

The product must implement the following roles, which the indicated capabilities:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

1. Root Administrator:
    1. Establishes the CNs of certificates which are considered valid for the administration of the gateway, and their associated permissions.
2. Security Administrator:
    1. Sets monitoring configuration: parameters which affect the system events and transfers logging.
    2. Can obtain a copy of security events files (which are stored locally on the internal unit of the gateway).
    3. Can send system commands (system time set and reboot).
3. Services Administrator:
    1. Establishes all the configuration of services (inbound and outbound file services).
    2. Can start and stop inbound and outbound file services.
    3. Can obtain a copy of operation events files (which are stored locally on the internal unit of the gateway).
4. Monitoring Administrator:
    1. Monitors de operating status of the gateway.
    2. Can reset statistical information of the services (inbound and outbound file services).
5. Local Administrator:
    1. Establishes the local configuration of internal units.
    2. Performs integrity checks of both units and deploys updates.

These roles and capabilities will be implemented through the authentication features that allow the policies and access control functions that regulate the authorized exercise of the capabilities indicated, to be established.

Policy 04: P.AUDIT

The TOE will implement a mechanism to log its activity.

Policy 05: P.AVAIL

A high availability configuration must be possible where a peer element can take over the services of a failing element. (This policy only applies to high availability configuration).

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

Assumption 01: A.PHYSEC

The TOE is deployed in a physically secure environment. Only authorized personnel has physical access to the TOE.

Assumption 02: A.LOCNOEVIL

Administrators with physical access to the TOE will not attempt to circumvent the TOE's security functionality.

Assumption 03: A. SINGLECHAN

There are no channels for information to flow between the networks apart from the TOE itself.

Assumption 04: A. SECPLAT

The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.

Assumption 05: A. NETS

The internal network is an isolated network, securely configured and trustworthy. The external network is a physically controlled network with security measures in place but it is connected by TCP/IP to other networks.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product PSTfile v4.4.2, although the agents implementing attacks have the attack potential according to the *Basic* of EAL2 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 categorized below.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Threat 01: T.INTOUTLEAK

An unauthorized user on the internal network causes data on the internal network to leak to the external network.

Threat 02: T. EXTOUTLEAK

An attacker on the external network gains access to the internal network data through the TOE.

Threat 03: T. EXTINFEED

An attacker on the external network manages to introduce data to the internal network, other than the data available in the configured sources.

Threat 04: T. INTINFEED

An authorized user on the internal network (rogue user or malicious code) manages to introduce data to the internal network through the system, other than the data available in the configured system.

Threat 05: T. INTACCESS

An unauthorized user on the internal network gains remote access to the TOE and alters or deletes security sensitive data on the TOE.

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 categorized below.

Environment objective 01: OE.PHYSEC

No access will be granted to the hardware of either of the two units (except for the Local Administrator). It is assumed that the obvious ways to circumvent the system (for example, connect both units directly through a network cable) are ruled out by physical or organizational measures within the operational environment.

Environment objective 02: OE.SECPLAT

The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself..

Environment objective 03: OE. CRYPT

The cryptographic operations use a third party trusted cryptographic module for the following:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Disk encryption on internal units (PSTi). Encryption is done on internal units with a key that is stored in an external device and is retrieved during each start-up for decryption.
- Disk encryption on external units (PSTe). Encryption is done on external units with a session key. This grants that there will be no persistence between sessions.
- TLS connection establishment for administration and sending of auditing data.
- Verification of the signature of outgoing files.

Environment objective 04: OE. NETS

The internal network is an isolated network, securely configured and trustworthy. The external Network is a physically controlled network with security measures in place but it is connected by TCP/IP to other networks.

Environment objective 05: OE. SEP

Network separation. The hardware architecture must be designed in a way that a different host exists on each of the networks. Communication between the hosts must be made using a passive information exchange device.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

PHYSICAL ARCHITECTURE

The fundamental component of PSTfile consists of two computers called ‘units’, these two unit forms an ‘element’. Each unit is connected to one of the networks. The one connected to the internal network is called PSTi and the one connected to the external network is called PSTe. These are dedicated computers; i.e. no software application is executed on them apart from those of PSTfile. The element also includes the hardware device necessary for communication between the units.

There are two possible configurations:

- Standard: formed by an element.
- High availability: formed by two elements in an active-passive redundancy scheme.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

LOGICAL ARCHITECTURE

Additionally to the software installed on the units, the system is also formed by the following software components, which will run on general purpose stations or servers located on the internal network:

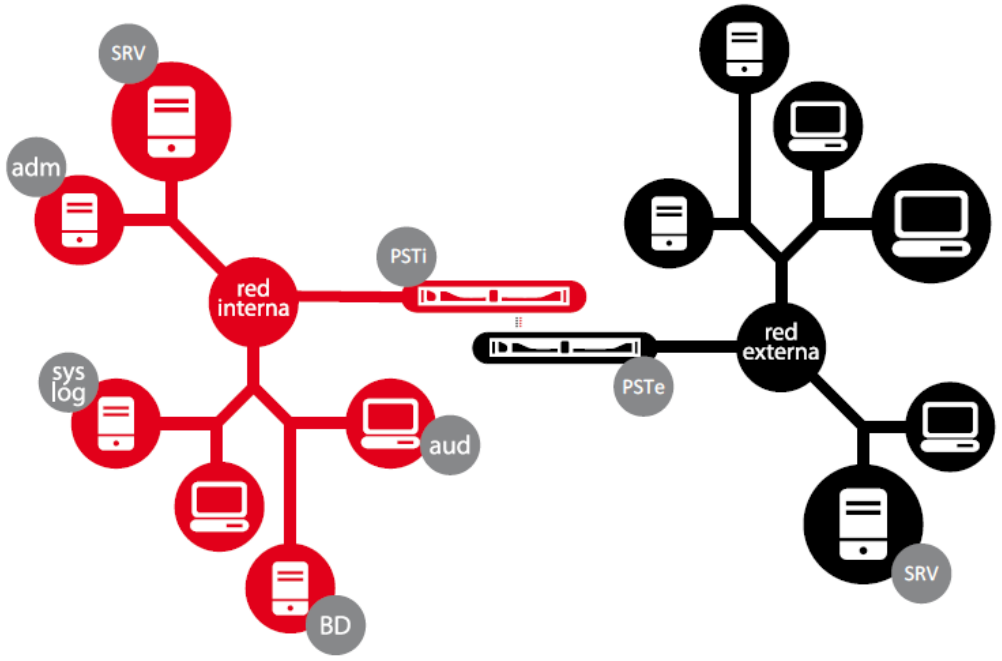
- PSTadm – Administration application.

  The administration of the complete system is carried out from a station on the internal network. The unit located on the external network (PSTe) requires no administration.

- PSTaud – Audit records reception service.

  Activity data (data of the files transferred through the gateway) is recorded on a database separate from PSTfile. The job of PSTaud is to enter the data ir receives from the unit into the database.

  Alternatively, transfer data can be recorded to files on the computer where PSTaud is installed.



DOCUMENTS

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Type	Reference
Security Target	**Security Target Lite** Revision 3.1. 31/01/2014
Installation and Deployment Guide	**Manual de instalación y puesta en servicio** Revisión 2. 03/09/2013
Operation Guide	**Manual de operación** Revisión 2. 02/10/2013

PRODUCT TESTING

The developer has executed tests for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers has been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the appropriate testing scenario to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises, testing all the SFRs defined for the TSFIs of the TOE.

In addition, the lab has extended the tests coverage for every interface, changing the input parameters: searching for critical parameters in the interaction with the TSFIs, wrong behaviour according to specific input values.

It has been checked that the obtained results conform to the expected results.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product PSTfile v4.4.2 it is necessary the disposition of the following software components:

- The main part of the TOE run in two specific servers provided in a inseparable way to the product. It supports S3 series or higher for the servers which their internal units include an internal hardware device for communication between the units. The evaluated configuration uses a customized version of Windows Embedded Standard 2009.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- The environment where the TOE runs includes:
  - PSTadm (Administration application). PSTadm requires a standard PC with enough CPU and memory is needed to run Windows XP SP3 or higher.
  - PSTaud (Audit records reception service). PSTaud requires a standard PC with enough CPU and memory is needed to run Windows XP SP3 or higher.
  - Public Key Infrastructure.
  - Syslog server(s) (Internal network).
  - Database server to store the transfers logs, accessible from the internal network using the ODBC standard. Optionally, text files can be used in order to store the logs.
  - File Transfer Servers (FTP, FTPS or SMB) in both networks.

EVALUATION RESULTS

The product PSTfile v4.4.2 has been evaluated against the Security Target "Declaración de seguridad de PSTfile", revision 3, 07/10/2013.

All the assurance components required by the evaluation level EAL2+ (ALC_FLR.1) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the [CC-P3] and the Evaluation Methodology [CEM] version 3.1 r4.

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.

- It is essential to trust in the Public Key Infrastructure which the product hinge upon.
- Authentication is based on the Common Name, independently of the CA used (the CA must be stored in the TOE), so the CAs stored in the TOE should be reliable.
- Due to the product design it is necessary that the user password accounts are known by the administrators of the product. The users of the product must be aware of it.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- The product allows plain text communication to the file servers but it is recommended to secure those communications in the operational environment.
- It would be advisable not to use certificates which use MD5 as hash algorithm or for authorization sign purposes.
- Revoked certificates: The TOE does not declares any mechanism for the revoked certificates management; although the TOE makes an intensive use of the Operating System for all the operations concerning the use of certificates and their validations, it's possible the TOE to accept a revoked certificate if the URLs of the certificate revocation list distribution points weren't declared during the generation in the PKI. This fact has to be taken into account while the product utilization.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product PSTfile v4.4.2, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
TOE	Target Of Evaluation

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 R4, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 R4, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 R4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1 R4, September 2012.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: “Declaración de seguridad PSTfile revisión 3, 07/10/2013” and a lite version is available on the Certification Body website: “Security Target Lite. Revision 3.1. 31/01/2014”.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es