REF: 2015-32-INF-1640 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 26.05.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-32 CCN-TP-PP

Applicant: Centro Criptológico Nacional

References:

[EXT-3020] Certification request of CCN-TP-PP

[EXT-3030] Evaluation Technical Report of CCN-TP-PP.

The product documentation referenced in the above documents.

Certification report of the Protection Profile for Trusted Platform for secure communications v1.1, as requested in [EXT-3020] dated 01/12/2015, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3030] received on 26/02/2016.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Protection Profile for Trusted Platform for secure communications v1.1.

The TOE type is a mobile device that provides trusted mechanisms for secure communications with external entities (other devices). It can be used, for example for voice and data communications applications using a trusted channel. The trusted channel is a VPN providing confidentially, integrity and end-points authenticity.

The TOE covered by this PP is part of a mobile infrastructure for secure communications that consists of a handset, trusted external entities and a key generation system. The TOE is limited to the mobile device (the handset).

Sponsor: Departamento de Productos y Tecnologías de Seguridad del Centro Criptológico Nacional.

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

ITSEF: Epoche & Espri S.L.U.

Evaluation Level: Common Criteria v3.1 R4 – EAL 4 + ALC_FLR.2.

Evaluation end date: 26/02/2016.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.2) 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 EAL4 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 [CC_P3] and the CEM v3.1 R4 [CEM].

Considering the obtained evidences during the instruction of the certification request of the product Protection Profile for Trusted Platform for secure communications v, a positive resolution is proposed.

TOE SUMMARY

The TOE type is a mobile device that provides trusted mechanisms for secure communications with external entities (other devices). It can be used, for example for voice and data communications applications using a trusted channel. The trusted channel is a VPN providing confidentially, integrity and end-points authenticity.

The TOE covered by this PP is part of a mobile infrastructure for secure communications that consists of a handset, trusted external entities and a key generation system. The TOE is limited to the mobile device (the handset).

The TOE connects to the internet using either a mobile network or wi-fi networks, but in either case, the communication with trusted external entities is through trusted

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

channels so that the IP traffic is sent and/or received using the trusted channel. Trusted channels are used for application communications, for remote administration of the TOE or for sending audit records to an external entity.

The TOE allows applications installed in the mobile device to communicate securely with the protected networks over a trusted channel called VPN tunnel. These protected networks are behind a VPN endpoint. Most of application data flowing from the handset to the VPN endpoint is done through the VPN tunnel. Bypass capability is implemented for specific and allowed applications.

Depending on the applications running in the TOE and using the VPN tunnel, at its end-point, additional services can be installed (e.g. app-market, update server, NTP- and voice- and messaging-servers).

The mobile device could also serve as an external “crypto-modem” by connecting the mobile device to a computer using USB. In case of the TOE implements that feature, all ip-traffic to and from the computer using this interface will be routed inside and protected by the VPN-tunnel.

In addition, the TOE supports white listing for software applications, user data storage encryption and integrity control.

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.2, according to [CC_P3] and the [CEM].

Class	Family/Component
ADV Development	ADV_ARC.1: Security architecture description ADV_FSP.4: Complete functional specification ADV_TDS.3: Basic modular design ADV_IMP.1: Implementation representation of the TSF
AGD Guidance Documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ALC Life-Cycle Support	ALC_CMC.4: Production support, acceptance procedures and automation ALC_CMS.4: Problem tracking CM coverage ALC_DEL.1: Delivery procedures ALC_DVS.1: Identification of security measures ALC_LCD.1: Developer defined life-cycle model ALC_TAT.1: Well-defined development tools ALC_FLR.2: Flaw reporting procedures

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ASE Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_TSS.1: TOE summary specification ASE_SPD.1: Security problem definition
ATE Tests	ATE_COV.2: Analysis of coverage ATE_DPT.1: Testing: basic design ATE_FUN.1: Functional testing ATE_IND.2: Independent testing - sample
AVA Vulnerability Assessment	AVA_VAN.3: Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4 [CC_P3]:

TOE Security Functional Requirements	Description
Extended Components	
FDP_DSK	Protection of Stored Data
FDP_ZER	Zeroization
FPT_SBT	Secure Boot and Operation continuity
FPT_TUD	Trusted Updates
FPT_TST.2	Extended integrity and self test
FCS_RNG	Random Number Generation
Components from CC Part 2	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_RNG.1	Random Number Generation
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_DSK.1 Extended	Protection of Data on Disk
FDP_ZER.1	Extended – Zeroization
FIA_UAU.2/KEK	User Authentication before any action
FIA_UAU.2/PIN	User Authentication before any action
FIA_UAU.2/KEY-admin	User Authentication before any action
FIA_AFL.1	Authentication failure handling
FMT_SMF.1	Specification of management functions

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TOE Security Functional Requirements	Description
FMT_SMR.1	Security management roles
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FPT_FLS.1	Failure with preservation of secure state
FPT_SBT.1	Secure Boot and Operation continuity
FPT_STM.1	Reliable time stamps
FPT_TST.2	Extended Integrity and self test
FPT_TUD.1	Trusted Update
FPT_PHP.1	Passive detection of physical attack
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.2	User-initiated locking
FTP_ITC.1/VPN-tunnel	Trusted Channel (Application communications)
FTP_ITC.1/CIK-tunnel	Inter-TSF Trusted Channel
FTP_ITC.1/REM-ADM	Inter-TSF Trusted Channel (remote administration)
FTP_ITC.1/AUDIT	Inter-TSF Trusted Channe

IDENTIFICATION

Protection Profile title: Protection Profile for Trusted Platform for secure communications v1.1

Evaluation Level: Common Criteria version 3.1 revision 4 EAL 4 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Protection Profile for Trusted Platform for secure communications v 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.SECURE_MGMNT

The TOE consuming organization shall be responsible for establishing a security policy which will define the processes to manage the TOE security. At least this policy should include that only authorized personnel (authority) may have access to security management functionalities and, whenever not necessary, this functionality shall be disabled.

Policy 02: P.CRYPTO_MGMNT

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

The TOE consuming organization shall be responsible for establishing a specific policy to manage the TOE cryptographic assets and their delivery.

Policy 03: P.SECURE_USE

The TOE consuming organization shall be responsible for establishing a specific policy which will define the TOE specific use policy applicable to users, establishing at least the different data which the TOE can manage and how a user shall handle that data.

Policy 04: P.VPN_BYPASS

The TOE shall implement a VPN-tunnel bypass capability managed by the corresponding VPN-policy for applications.

Policy 05: P.AUDIT

The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The audit trail shall be protected for unauthorized modification and loss of audit trail data. The TOE shall provide authorized administrators with the ability to review the audit trail. The TOE shall provide management functionality to enable the capacity of sending the audit trail to an external entity.

Policy 06: P.RNG

The TOE must implement random number generators meeting the requirements of strength and quality metrics specified in [AIS20] and [AIS31].

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.NOEVIL

It assumed that those users belonging to the authority, who are authorized to securely manage the TOE and its operational environment, are trustworthy and they have been trained sufficiently to carry out these security management tasks in a proficient manner.

Assumption 02: A.SINGLEUSER

It is assumed that the TOE is used and under the control of a single user only.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Assumption 03: A.KEYS

It is assumed that the crypto-material (e.g. keys used for the encryption of TOE data storage or the key provided to the user) entered into the TOE are of good quality, not disclosed and only distributed to the appropriate handsets and users.

Assumption 04: A.APPS

It is assumed that all applications that are white-listed does not reveal sensitive user data on the screen lock without user authentication.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Protection Profile for Trusted Platform for secure communications v, although the agents implementing attacks have the attack potential according to the **enhanced basic attack potential** of EAL4 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.

Threat 01: T.UNAUTH_INST

A legitimate user or an attacker manages to install applications in the TOE which are not authorized by the consumer organization.

Threat 02: T.CRYPT_COMPROMISE

A legitimate user or an attacker retrieves or modifies cryptographic assets such as all the keys and certificates stored and managed by the TOE. This includes also the possible modification of the cryptographic mechanisms. This threat covers the use case for legitimate users, but only when the legitimate user is not authorized to retrieve these assets.

Threat 03: T.USR_DATA

An attacker retrieves, access or modifies user data stored or to be transmitted, protected by the TOE. This threat applies to all the external interfaces of the TOE (3G, Wi-Fi, USB, NFC, Bluetooth, etc.). VPN interface is addressed in other threats.

Threat 04: T.VPN_CONFIG

A legitimate user or an attacker is able to modify the VPN configuration data and/or the software components and modules which handle the VPN connection. This threat covers the use case for legitimate user in these cases:

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- when the legitimate user is not authorized to modify the VPN configuration;
- whenever the user modifies the software components.

Threat 05: T.CONF_DATA

A legitimate user or an attacker is able to modify the security configuration data which is managed by the TOE. This threat covers the use case for a legitimate user, but only when the legitimate user is not authorized to modify this data.

Threat 06: T.UNAUTH_BOOT

An attacker manages to bypass the initial encryption mechanism used to encrypt the TOE and is able to boot and start up the TOE.

Threat 07: T.BYPASS

An attacker manages to access to TOE services, functions, installed applications or user data bypassing the TOE authentication mechanisms which unlocks these TOE features.

Threat 08: T.UNAUTH_VPN

An attacker or a legitimate user manages to redirect or extract confidential communications outside the VPN tunnel, bypassing the security mechanisms established to force the TOE applications to communicate through this channel.

Threat 09: T.ATTACK_VPN

An attacker is able to disclose information or undetected modify information that is communicated between the TOE and endpoint of the VPN tunnel.

Threat 10: T.UNAUTH_COM

An attacker manages to establish an unauthorized communication channel, extract information or access TOE assets using some of the TOE available interfaces.

Threat 11: T.UNAUTH_ADMIN

An unauthorized user or attacker manages to access administrative, configuration or development functionalities established within the TOE.

Threat 12: T.OS_MOD

An unauthorized user or attacker manages to modify operating system or core component software of the TOE.

Threat 13: T.HW_TAMPER

An attacker manages to open the handset through the standard opening mechanisms (screws, covers) without leaving any evidence of the attack.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.SECURE_MGMNT

The consuming organization shall be responsible for establishing a security policy which will define the processes to manage the TOE security and its operational environment. At least this policy should include that only authorized personnel may have access to security management functionalities and, whenever not necessary, this functionality shall be disabled.

Environment objective 02: OE.CRYPTO_MGMNT

The TOE consuming organization shall be responsible for establishing a specific policy to manage the TOE cryptographic assets and their delivery.

Environment objective 03: OE.SECURE_USE

The TOE consuming organization shall be responsible for establishing a specific policy which will define the TOE and its operational environment specific use policy applicable to users, establishing at least the different data which the TOE can manage and how a user shall handle that data.

Environment objective 04: OE.NOEVIL

Those users who are authorized to securely manage the TOE shall be trustworthy, and they shall be trained sufficiently to carry out these security management tasks in a proficient manner.

Environment objective 05: OE.SINGLEUSER

The TOE is used and under the control of a single user only.

Environment objective 06: OE.KEYS

Crypto-material (e.g. keys used for the encryption of TOE data storage or the key provided to the user) entered into the TOE are of good quality, not disclosed and only distributed to the appropriate handsets and users.

Environment objective 07: OE.APPS

Applications that are whitelisted are trustworthy.

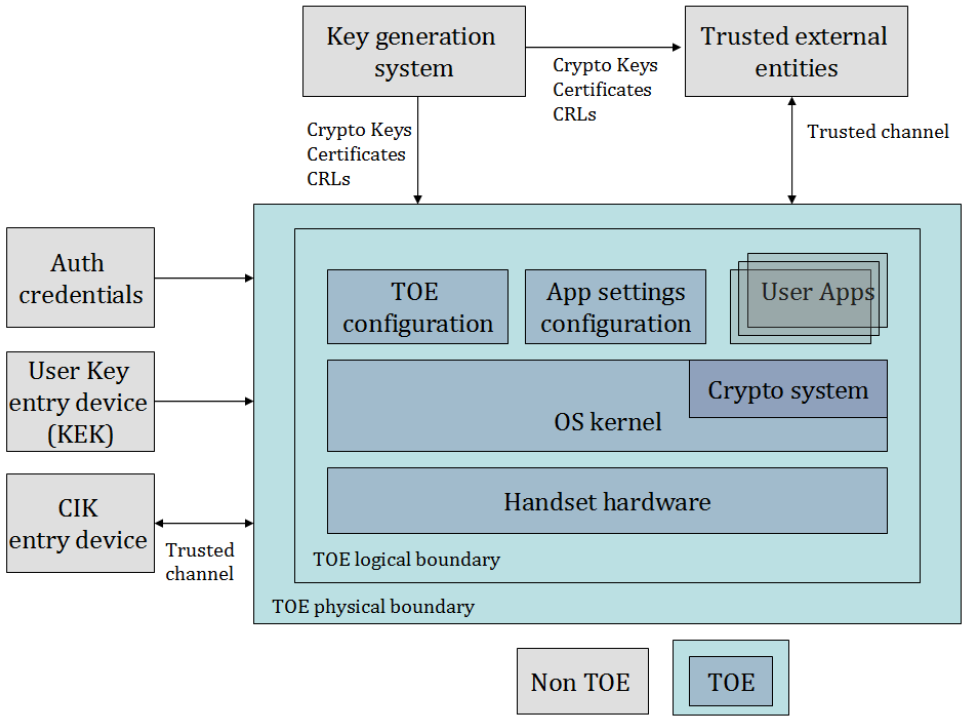
The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ARCHITECTURE

The following figure shows the TOE scope:



DOCUMENTS

The protection profile only includes the following document:

Protection Profile for Trusted Platform for secure communications v1.1.

PRODUCT TESTING

N/A

EVALUATED CONFIGURATION

N/A

EVALUATION RESULTS

The Protection Profile for Trusted Platform for secure communications v1.1 has been evaluated for EAL 4 + ALC_FLR.2 level.

All the assurance components required by the evaluation level EAL4 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.2, as defined by Common Criteria v3.1 R4 [CC_P3] and the CEM v3.1 R4 [CEM.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

There are no comments/recommendations from the evaluation team.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Protection Profile for Trusted Platform for secure communications v1.1, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
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 Final, September 2012.

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

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

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

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

SECURITY TARGET

N/A

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es