REF: 2016-1-INF-2264 v2
Target: P
Date: 22.03.2018

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-1 VinCERTcore
Applicant: B62913926

References:

[EXT-2869] Certification request of VinCERTcore
[EXT-3859] Evaluation Technical Report of VinCERTcore.

The product documentation referenced in the above documents.

Certification report of the product vinCERTcore v4.0.5.5733, as requested in [EXT-2689] dated 25/11/2015, and evaluated by the laboratory “Applus Laboratories”, as detailed in the Evaluation Technical Report [EXT-3859] received on 16/03/2018.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product vinCERTcore v4.0.5.5733.

The product vinCERTcore v4.0.5.5733 is a software server which provides all the functionality for certificate management and centralized digital signature. It uses an external user repository and a HSM (external to the TOE) which will hold all the sensible cryptographic material.

Developer/manufacturer: Víntegris, S.L.
Sponsor: Víntegris, S.L.
Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
ITSEF: Applus Laboratories.
Protection Profile: None.
Evaluation Level: Common Criteria v3.1 R4 EAL4+ALC_FLR.2.
Evaluation end date: 16/03/2018.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory “Applus Laboratories” 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 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product vinCERTcore v4.0.5.5733, a positive resolution is proposed.

TOE SUMMARY

vinCERTcore v4.0.5.5733 is a software server which provides all the functionality for certificate management and centralized digital signature. It uses an external user repository and works with a HSM (out of ST scope) which will hold all the sensible cryptographic material. Additionally it uses a set of external IT products to provide the overall functionality.

The management of certificates of vinCERTcore allows end-users to manage the certificate creation flow in the system using the external vinCERTweb product (out of scope of evaluation) and storing them in the HSM. The operative can be performed in two different ways:

- Importing user’s digital certificates.
- Generating new certificates which can be enrolled in an external CA.

The management of certificates of vinCERTcore also allows authorized end-users delegate the usage of the certificates. This is accomplished using the related functionalities on vinCERTweb.

It's required a vinCERTagent software (out of scope of evaluation) installed for digital signature purposes. This agent is compatible with CSP and PKCS#11 and it is installed on user's device and transparently, communicates with vinCERTcore allowing users to perform digital signature through it. End users can use any of their allowed certificates which are stored in vinCERTcore. Digital signatures are always performed remotely in the vinCERTcore HSM (out of scope of evaluation). Password protected key usage is also supported.

The vinCERTagent and the vinCERTweb external modules connect to the vinCERTcore in order to authenticate end-users. They present the necessary dialogs to allow end-users to perform multiple factor authentication against the Active Directory and the Radius Server (both external to the TOE).

The administration of the TOE is performed using an SSH console connected to the TOE by Active Directory users with a privileged role. Once single-factor has been satisfied, they are allowed to start the TOE on maintenance mode which permits the sensitive operatives such as configuration management, backup and restores and audit data review and export.

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 Common Criteria v3.1 R4.

Assurance Class	Assurance components
ADV: Development	- ADV_ARC.1 Security architecture description - ADV_FSP.4 Complete functional specification - ADV_IMP.1 Implementation representation of the TSF - ADV_TDS.3 Basic modular design
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
ASE: Security Target evaluation	- ASE_CCL.1 Conformance claims - ASE_ECD.1 Extended components definition - ASE_INT.1 ST introduction - ASE_OBJ.2 Security objectives - ASE_REQ.2 Derived security requirements - ASE_SPD.1 Security problem definition - ASE_TSS.1 TOE summary specification
ATE: Tests	- ATE_COV.2 Analysis of coverage - ATE_DPT.1 Testing: security enforcing modules - ATE_FUN.1 Functional testing - ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	- AVA_VAN.3 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

FAU_ARP.1
FAU_GEN.1
FAU_GEN.2
FAU_SAA.1
FAU_SAR.1
FAU_SAR.2
FAU_SAR.3
FAU_STG.2
FCS_CKM.4
FCS_COP.1
FDP_ACC.1/Management
FDP_ACF.1/Management
FDP_ACC.1/Signer
FDP_ACF.1/Signer
FDP_ETC.1

FDP_ETC.2
FDP_ITC.1
FDP_ITC.2
FDP_RIP.1
FDP_ROL.1
FDP_SDI.2
FDP_UIT.1/Backup-archive
FDP_UIT.1/Audit-archive
FIA_AFL.1
FIA_ATD.1
FIA_UAU.1
FIA_UAU.5
FIA_UAU.6
FIA_UID.1
FIA_USB.1
FMT_MOF.1
FMT_MSA.1/Key-Regen
FMT_MSA.1/Signatory
FMT_MSA.3
FMT_SMF.1
FMT_SMR.2
FPT_TDC.1
FPT_TST.1
FTA_SSL.3
FTA_SSL.4
FTA_TSE.1
FTP_ITC.1
FTP_TRP.1

IDENTIFICATION

Product: vinCERTcore v4.0.5.5733
Security Target: Security Target for vinCERTcore 4.0.5.5733, version 1.12, 05 March 2018.
Protection Profile: None.
Evaluation Level: Common Criteria v3.1 R4 EAL4+ALC_FLR.2.

SECURITY POLICIES

The use of the product vinCERTcore v4.0.5.5733 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.Crypto_Management
S.SecurityOfficer will maintain the TOE cryptography strength within an acceptable level based on risk assessment, this means that:

- He will change the Infrastructure and Control KEYs with the necessary regularity.
- He will change the key algorithms and key lengths if they become unsuitable.
- He will change the compromised or suspected to be compromised keys.
- He will apply a configuration using only algorithms and algorithm parameters defined by the ETSI/TS 102 176 [6] series for TOE SCD setup.

Policy 02: P.Standard_Time_Source
The TOE uses the system time where it is installed as a Time Source. To ensure the accuracy of the System Time Source, system clock must be set by Organization Administrators, who are responsible for the proper maintenance of system clock.

Policy 03: P.HSM_Backup
The TOE expects that Organization's S.Operator or S.Administrator be in charge of the HSM backup procedures. Those backup procedures will be subjected to the following restrictions:

- All HSM keys will be stored in a protected state.
- If any key is exported from the HSM, it will be protected to ensure its confidentiality and integrity to the same or higher security level as within the HSM. Wherever the key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength will be used.
- Backup, storage and restoration of keys in the HSM are only performed by authorized personnel. Master keys used to protect both user and working keys shall be backed up, stored and reloaded under at least dual control. Such master keys will only be held outside the HSM in protected form.

Policy 04: P.Audit_Review
Authorized auditor(s) regularly review audit records produced by the TOE, respond promptly to any indication of an attempted or actual security issues.

Policy 05: P.Storage_Review
Organization's personnel must prevent system's storage exhaustion.

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.Trained&Trusted
It is assumed that all TOE users are sufficiently trained in order to operate the TOE securely. It is assumed in addition that every TOE privileged role, including R.Administrator, R.Operator, R.SecurityOfficer and R.Auditor, are trusted and not malicious towards the system.

Assumption 02: A.No_Malware
It is assumed that no malware will be able to attack the TOE directly from the same operating system.

Assumption 03: A.Configuration
It is assumed that the TOE will be properly installed and configured according to the vinCERT Administration Guide and vinCERT Installation Guide. The TOE is considered well configured when all internal tests are successfully executed. The initial tests covers connection to all external products.

Assumption 04: A.Trusted_IT_Products
It is assumed that the following external IT products which the TOE communicates with are trusted and reliable. Also the personnel responsible for its administration is trusted and not malicious towards the system:

- HSM
- PKI (vinCERTcamgr)
- AD
- RADIUS
- DB
- SMTPS

Assumption 05: A.Trusted_Agents
It is assumed that the product's external components vinCERTagent, vinCERTweb and the O.S. on which these ones operate are trusted and not malicious towards the system.

Assumption 06: A.Trusted_O.S.
It is assumed that the O.S. on which the TOE is running is trusted and not malicious towards the system in any way.

Assumption 07: A.Trusted_SCA
It is assumed that the signatory will use only a trustworthy SCA. The SCA creates and sends the DTBS or the DTBS/R the R.Signer wishes to sign in an appropriated

form to be signed by the TOE. It is also implemented in compliance with functional requirements of CWA 14170.

Assumption 08: A.Certified_HSM
It is assumed that the HSM component will be hardware based and It'll meet the requirements identified in EN 419241 and/or will be a trustworthy system which is assured to EAL 4+ or higher in accordance to ISO/IEC 15408, or equivalent security criteria, or will meet the requirements identified in FIPS PUB 140-2 level 3 or higher.

Assumption 09: A.No_Physical_Access
It is assumed that no threat agents and users have direct physical access to the TOE

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product vinCERTcore v4.0.5.5733, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4+ALC_FLR.2 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.Key_Divulg
An attacker may steal SCDs and/or KEYs and thus make unauthorized use of them.

Threat 02: T.SigF_Misuse
An attacker misuses the signature-creation function of the TOE to create digital signature for data the signatory has not decided to sign.

Threat 03: T.User_Impersonation
A threat agent may gain access to User credentials or use tampering techniques to impersonate him, then he can use functions permitted to the victim that are forbidden to the threat agent.

Threat 04: T.Sig_Forgery
Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery.

Threat 05: T.Config_Access
A threat agent may modify the TOE configuration provoking malfunctions or deliberately change of security parameters that may compromise the correct operation of TSF.

Threat 06: T.Audit_Access

A threat agent may access the audit data and either read it without permission, modify it, delete it, or denying its generation; so attacks or signature related events could be concealed. In this threat it is also considered the possibility for an external effect to deny the audit data generation (e.g.: Storage exhaustion).

Threat 07: T.Audit_Archive
A threat agent may alter the audit data inside an audit archive so important events in the archive could be changed or deleted.

Threat 08: T.Backup_Archive
A threat agent may alter the Backup data inside a Backup archive. This can lead in malfunctions or TSF operation fail when the Backup is restored.

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.Competent_Users
The operational environment shall ensure that all (human) TOE users and those users managing the operational environment are competent to manage, operate, and use the TOE and to maintain the security and privacy of the data it handles.

Environment objective 02: OE.Configured
The operational environment shall ensure that the TOE will be installed and configured properly for its startup and execution in a secure way.

Environment objective 03 : OE.Secure_Env
The operational environment shall ensure that every external element from which the TOE requires resources are secure, trusted, reliable and non-hostile towards it, including:

- HSM
- PKI (vinCERTcamgr)
- Active Directory
- RADIUS Authentication Server
- Database
- SMTPS
- vinCERTagent
- vinCERTweb
- O.S. on which the TOE is being executed
- The server on which the TOE is being executed

Environment objective 04: OE.Secure_SCA

The SCA used by any S.User shall be a trustworthy SCA, not malicious against the TOE or its environment and shall be compliant with CWA 14170 standard.

Environment objective 05: OE.Audit_Review
The operational environment shall ensure that:
Audit records produced by the TOE are regularly reviewed.
Any indication of an attempted or actual security issue is responded to.
Audit records are regularly archived to prevent audit data storage exhaustion.

Environment objective 06: OE.Certified_HSM
The operational environment shall ensure that the HSM that will be integrated with the TOE will be hardware based and It'll meet the requirements identified in EN 419241 and/or will be a trustworthy system which is assured to EAL 4+ or higher in accordance to ISO/IEC 15408, or equivalent security criteria, or will meet the requirements identified in FIPS PUB 140-2 level 3 or higher.

Environment objective 07: OE.Standard_Time_Source
The operational environment shall ensure that the Time Source provided from the TOE operating system comes from an organization's standard time source and is managed by the organization Operators.

Environment objective 08: OE.Secured_RADIUS
The operational environment shall ensure that the communication channel with the external trusted IT product RADIUS server is protected in integrity and confidentiality.

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

LOGICAL ARCHITECTURE

The TOE comprises the eight subsystems shown in Figure 1.

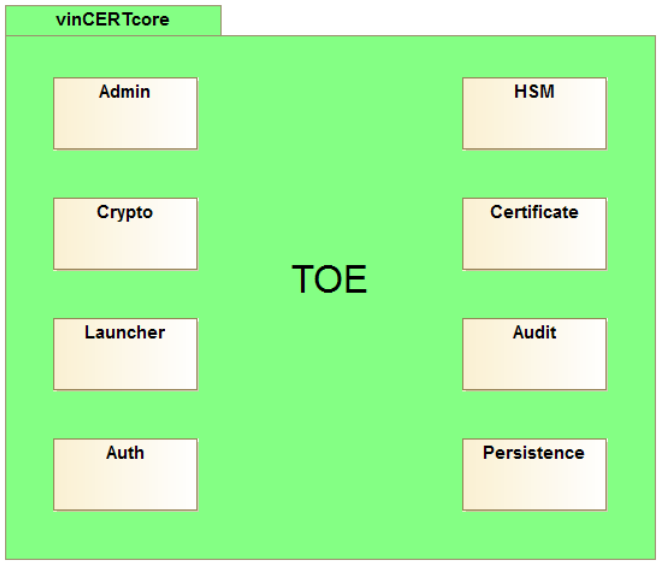


Figure 1: TOE subsystems

The functions assigned to each of these subsystems are detailed below:

Admin subsystem provides operations for managing certificates and policies. It exposes an HTTPS service which is used by vinCERTweb.

Crypto subsystem provides operations for requesting signature function to HSM subsystem and the related cryptography. It exposes an HTTPS service which is used by vinCERTagent.

Launcher subsystem is responsible for initiating vinCERTcore and provides an SSH service that allows SSH clients to connect to it in order to perform privileged operations.

Auth subsystem is responsible for centralized user authentication. It permits first factor and second factor authentication mechanisms. Both vinCERTweb and vinCERTagent connects (out of scope of ST) to this subsystem to allow end-user authentication to the TOE.

HSM subsystem is responsible for interacting with the organization's HSM or its respective middleware.

Certificate subsystem holds the operatives of certificate management, policy management and the related security.

Audit subsystem is used to allow the generation of an Audit trail which will be trustworthy and could be used as a legal evidence of signature. It also monitors the

actions that occurs in vinCERTcore and is capable of apply countermeasures in case of attack or failure.

Persistence subsystem provides the wrapper functions necessary for let the Database be used by the other TOE subsystems.

PHYSICAL ARCHITECTURE

The TOE is a software server that is provided as a MSI installable package. Once this package is executed a semiautomatic wizard will aid to perform a secured installation and minimal configuration.

DOCUMENTS

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

- AGD_PRE.1 Preparative procedures (v.1.5).
- nebulaCERT-vinCERTcore-Instalacion y configuración (v.1.7).
- nebulaCERT-Entorno-Instalacion y configuración (v.1.7).
- AGD_OPE.1 Operational user guidance (v.1.5).
- nebulaCERT-vinCERTcore-Administracion (v.1.5).
- nebulaCERT-Entorno-Administracion (v.1.5).
- nebulaCERT-Guia de uso (v.1.3).

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters

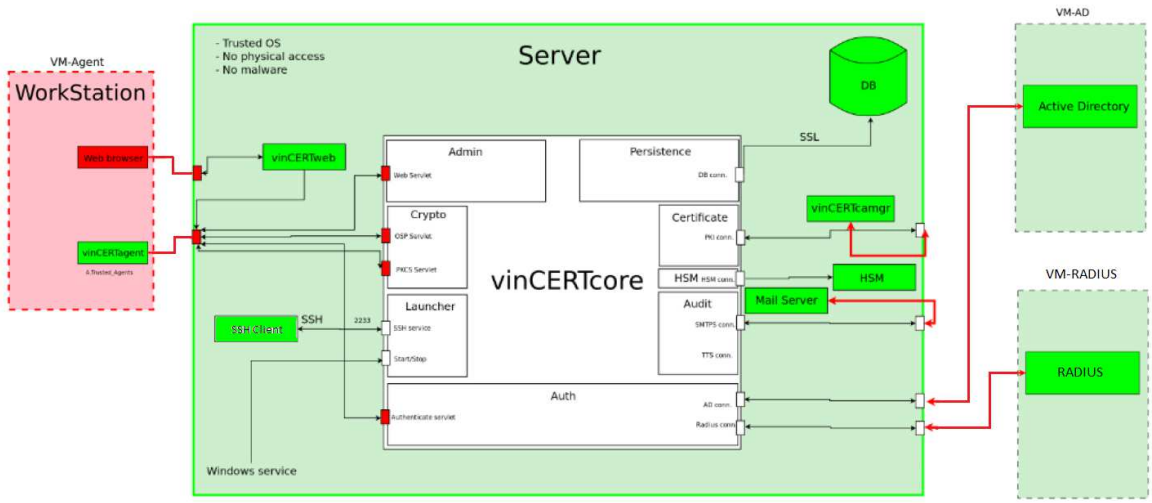
values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the Security Target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the Security Target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Enhanced Basic” has been successful in the TOE’s operational environment as defined in the Security Target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE under evaluation is “vinCERTcore v4.0.5.5733”. The following figure depicts the detailed deployment diagram for the evaluated configuration (the TOE is shown in white).



EVALUATION RESULTS

The product vinCERTcore v4.0.5.5733 has been evaluated against the Security Target for vinCERTcore 4.0.5.5733 v1.12, 05/03/2018.

All the assurance components required by the evaluation level EAL4+ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory “Applus Laboratories” 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 the Common Criteria v3.1 R4 and the CEM 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.

1. vinCERTagent component is considered as a non-TOE component. However, the laboratory recommends to protect this component by the use of environmental protection as it is an entity that is used to communicate with the TOE.
2. The warnings made in the guidance documentation about how to configure the TOE to fulfill eIDAS (CEN/TS) regulation are made for applicability in future use of the TOE. The evaluation does not include the analysis of the fulfillment with this regulation.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product vinCERTcore v4.0.5.5733, a positive resolution is proposed. However, the following certifier recommendation must be taken into account:

1. It must be noted that the manufacturer has assigned a LOW level to the TOE confidentiality, according to the risk analysis carried out within the company. As a consequence, the evaluation has been carried out without analyzing those security measures related to TOE confidentiality protection.

GLOSSARY

CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SFR	Security Functional Requirement
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.

SECURITY TARGET

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

Security Target for vinCERTcore 4.0.5.5733 v1.12, 05/03/2018

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.sogisportal.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.

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

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.