Certificate: vinCERTcore v4.0.5.5733

Certification Report

Developer and sponsor: Víntegris, S.L.
Evaluation facility: Applus LGAI Technological Center S.A.
Compliance: EAL4+

Target of Evaluation

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

Assumed Attacker Model

All of the following is assumed: All users are sufficiently trained, using priviledged roles, no malware can attack the TOE from the same operation system, proper installation and configuration, all external IT products are trusted and not malicious, all external components are trusted and not malicious, the OS is trusted, only trusted SCA and secure HSM used, no physical access to TOE.

Device scrutinization

No further description was given apart from the set of assumptions.

Security Assurance Requirements (SARs)

The assurance requirements are EAL4 + ALC_FLR.2

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_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

ALC_CMC.4 Production support, acceptance procedures and automation
ALC_CMS.4 Problem support, acceptance procedures and automation
ALC_DEL.1 Delivert 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_CCL.1 Conference 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_COV.2 Analysis of coverage
ATE_DPT.1 Testing: security enforcing modules
ATE_FUN.1 Functional testing
ATE_IND.2 Ondependent testing – sample
AVA_VAN.3 Vulnerability analysis

Security Functional Components (SFRs)

FAU_ARP.1 - Security alarms
FAU_GEN.1 - Audit data generation
FAU_GEN.2 - User identity association
FAU_SAA.1 - Potential violation analysis,
FAU_SAR.1 - Audit review
FAU_SAR.2 - Restricted audit review
FAU_SAR.3 - Selectable audit review
FAU_STG.2 - Guarantees of audit data availability
FCS_CKM.4 - Cryptographic key destruction
FCS_COP.1 - Cryptographic operation,
FDP_ACC.1/Management - Subset access control
FDP_ACF.1/Management - Security attribute based access control
FDP_ACC.1/Signer - Subset access control
FDP_ACF.1/Signer - Key pair deletion
FDP_ETC.1 - Export of user data without security attributes
FDP_ETC.2 - Export of user data with security attributes
FDP_ITC.1 - Import of user data without security attributes
FDP_ITC.2 - Import of user data with security attributes
FDP_RIP.1 - Subset residual information protection
FDP_ROL.1 - Basic rollback
FDP_SDI.2 - Stored data integrity monitoring and action
FDP_UIT.1/Backup-archive
FDP_UIT.1/Audit-archive - Data exchange integrity

FIA_AFL.1 - Authentication failure handling
FIA_ATD.1 - User attribute definition
FIA_UAU.1 - Timing of authentication
FIA_UAU.5 - Multiple authentication mechanisms
FIA_UAU.6 – Re-authenticating
FIA_UID.1 - Timing of identification
FIA_USB.1 - User-subject binding
FMT_MOF.1 - Management of security functions behaviour
FMT_MSA.1/Key-Regen
FMT_MSA.1/Signatory - Management of security attributes
FMT_MSA.3 - Static attribute initialisation
FMT_SMF.1 - Specification of Management Functions
FMT_SMR.2 - Restrictions on security roles
FPT_TDC.1 - Inter-TSF basic TSF data consistency
FPT_TST.1 - TSF testing
FTA_SSL.3 - TSF-initiated termination
FTA_SSL.4 - User-initiated termination
FTA_TSE.1 - TOE session establishment
FTP_ITC.1 - Inter-TSF trusted channel
FTP_TRP.1 - Trusted path

Out of Scope of Certification

- Hardware security model
- External web interface

Critical Evaluation and Conclusions

The independent testing has covered 100% of SFRs (Security Functional Requirements) and TSFIs (TOE Security Function Interface) defined in the functional specification.

Any kind of physical attacks, side channels etc. were sidestepped by a set of rigorous assumptions. Under these conditions, the TOE does not present any exploitable vulnerabilities and all identified vulnerabilites can be considered closed if TOE is installed and operated according to related documentation.

I was missing any description of the testing process, the evaluation results did not convince me, it seems that basically every possible attack is covered by assumptions and therefore not tested.