Certification Dossier Code:	2021-4
Certification Report Creation Date:	21st February 2024
Certification Report Code:	2021-4-REP-73 (internal) 2021-4-REP-85 (public)
NASK RWA code:	OSiC.8711.9.2021

Certification Report

[2021-4] Certification Report on SimplySign Signature Activation Module (SAM) EAL4+AVA_VAN.5

COMMON CRITERIA

CERTIFICATE

Certification Identification: **2021-4** | Type of Product: **Products for Digital Signatures**

Product Name and Version: **SimplySign Signature Activation Module (SAM), version 6.2.0**

Target of Evaluation:

SimplySign Signature Activation Module (SAM), version 6.2.0

Certificate holder/Manufacturer: **Asseco Data Systems S.A., Jana z Kolna 11, 80-864 Gdańsk, Poland**

Assurance Package: **EAL 4 + AVA_VAN.5**

Name of Certification Body:

NASK National Research Institute, Standardisation and Certification Centre, 12 Kolska, Warsaw, 01-045, Poland

Certification Report Identifier: **2021-4-REP-73**

The IT Product identified in this certificate has been evaluated at an Evaluation Facility accredited and approved under the rules of the Polish IT Security Evaluation and Certification Scheme (PC1) using the Common Methodology for IT Security Evaluation, April 2017 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, April 2017 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and conjunction with the complete Certification Report. The evaluation has been conducted following the provisions of the IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NASK National Research Institute or any other organisation that recognises or gives effect to this certificate. No warranty of the IT Product by NASK National Research Institute or any other organisation that recognises or gives effect to this certificate is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact NASK National Research Institute (Certification Body) or look at the NASK's website.

AC 223

Certificate Identifier: 2/PC1/AC223/2024

Certificate decision date: 05.04.2024

Certificate expiry date: 04.04.2029

Paweł Krzysztof Kostkiewicz 2024.04.25 19:13:15 +02'00'

NASK National Research Institute
Certification Body Manager

NASK

Table of content

Introduction

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been tested at an approved Laboratory (IT security evaluation facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the NASK-PC1 Scheme, and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report, and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

1. Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by an approved Laboratory under the oversight of the Certification Body, which is managed by the NASK - National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria based cybersecurity evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. **The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the Laboratory**. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

Recognition of the certificate

European Recognition of 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 up to EAL4. A higher recognition levels are provided for IT-Products related to certain SOGIS Technical Domains only.
The current list of signatory nations and approved certification schemes can be found on https://www.sogis.eu/.
The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. This certificate is recognized under SOGIS-MRA up to EAL4.

International Recognition of CC Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the Common Criteria (Common Criteria Recognition Arrangement, CCRA) became effective in September 2014. It covers Common Criteria certificates based on: collaborative Protection Profiles, assurance components up to EAL2 augmented by ALC_FLR and certificates for PP and cPP.
The current list of signatory nations and of collaborative Protection Profiles can be found on https://www.commoncriteriaportal.org .
The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition. This certificate is recognized under CCRA up to EAL2.

Executive Summary

This document constitutes the Certification Report for the certification file of the product: **SIMPLYSIGN SIGNATURE ACTIVATION MODULE (SAM)**

TOE Version:	6.2.0
Developer:	Asseco Data Systems S.A.
Sponsor:	Asseco Data Systems S.A.
Security Target:	Security Target for SimplySign Signature Activation Module (SAM), version 1.25 LITE, date of issue 2024-02-01
Protection Profile:	Security Target claims strict conformance to the following Protection Profile: • EN 419 241-2 [7]: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing, February 2019.

Laboratory/ITSEF:	Information Technology Security Evaluation Facility of National Institute of Telecommunications - ITSEF NIT
Evaluation Level:	Common Criteria version 3.1 release 5, Evaluation Assurance Level EAL 4+ AVA_VAN.5
Evaluation end date:	December 2023 (Final ETR ver.1.1, issue date 02.02.2024)
Expiration Date:	04/04/2029

All the assurance components required by the evaluation level EAL 4 + AVA_VAN.5 of Common Criteria standard have been assigned a "PASS" verdict. Consequently, the laboratory ITSEF NIT assigned the "PASS" VERDICT to the whole evaluation due all the Evaluator actions are satisfied for the EAL 4 + AVA_VAN.5, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5. Considering the obtained evidences during the process of the certification of the SimplySign Signature Activation Module (SAM), a positive resolution by Certification Body is proposed.

Documentation available for users

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

[EXT-1191] [EVD-ST-V1.25]	**Security Target SimplySign, v. 1.25, issue date 01.02.2024 (confidential document – LITE version available)**
[EXT-1182] [EVD-AGD_PRE-V0.95]	**SimplySign SAM Preparative guidance v. 0.95, issue date 01.02.2024 (confidential document)**
[EXT-1181] [EVD-AGD_OPE-V0.94]	**SimplySign SAM Operational Guidance, v. 0.94, issue date 01.02.2024 (confidential document)**

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

Security Target for SimplySign Signature Activation Module (SAM), version 1.25, issue date 2024-02-01

The public version of this document is published along with this certification report on the Certification Body website.

2. TOE Summary

TOE Overview

SimplySign is a TW4S system (Trustworthy System Supporting Server Signing) that offers a remote digital signature as a service. The Target of the Evaluation (TOE) is the SimplySign Signature Activation Module (SAM). It is a software component which ensures that signer's signing key is only used under the sole control of the signer for the intended purpose.

The SimplySign system consists of local (a Signer with a Signing Application) and remote environment, using an EN 419 221-5 compliant Cryptographic Module (CM) [8] to generate the signing key and create the digital signature value (Figure 1). The Signer is in the local environment and interacts with the Signing Application (that includes Signer Interaction Component - SIC) which communicates with the SimplySign SSA (Server Signing Application) in the remote environment to use the signing service. The signature operation is performed using the Signature Activation Protocol (SAP), which requires Signature Activation Data (SAD) be provided at the local environment, and next transfers SAD to the remote environment.

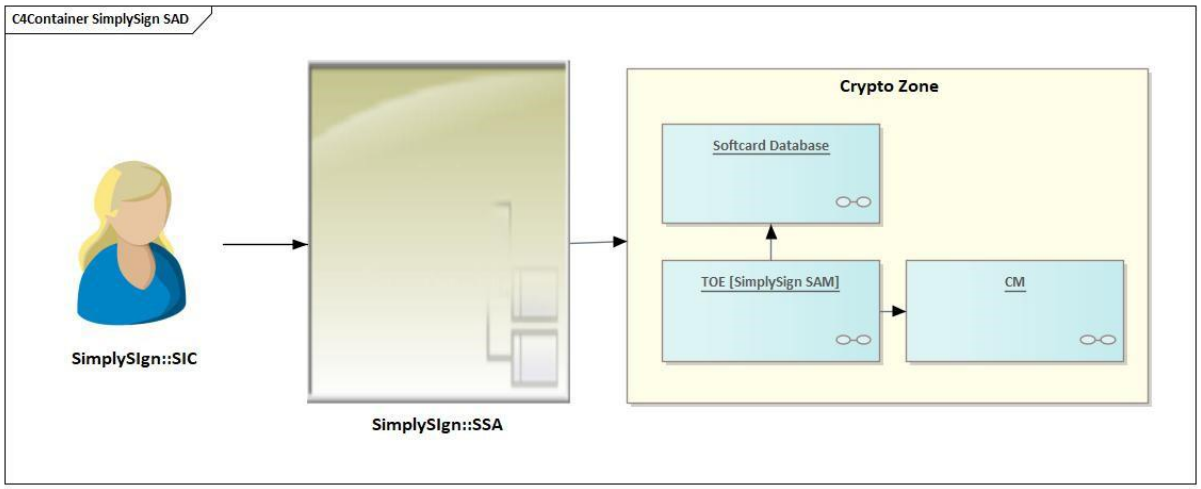

Figure 1: SimplySign System

SimplySign SAM (TOE) is a software component that operates in a dedicated tamper-protected environment called CryptoZone (see Figure 1).

Signer is a person who has the signing key under his/her sole control after being connected to the SimplySign system. It is recognized in the SimplySign system as a card (electronic form) with unique card number.

The TOE along with the CM (the CM is provided as a module embedded in the CryptoZone and connected to the TOE through a trusted channel) provides the necessary functionality to protect the Signer attributes needed to generate a digital signature. Other components (external components needed by the Signer to interact with the TOE, as presented in Figure 2) are parts of the SimplySign SSA environment.

To ensure the signer has sole control of his signing key, the signature operation is authorized by a SimplySign SAM (the TOE), which verifies Signature Activation Data (SAD) received from signer through SimplySign SSA and activates the signing key within a Cryptographic Module (CM). SAD verification means that the SAM checks validity and integrity of SAD elements as well as verifies that the signer is authenticated.

The TOE is composed of three modules: CKS (Cloud Key Service) application, which works with PKCS library and CipherTools library. The TOE interacts with the Cryptographic Module, which is a separate HSM (Hardware Security Module) connected to the TOE through a trusted channel. Both the CM and the SAM are installed on a hardware appliance (called CryptoZone) that is located within a tamper protected environment. Moreover, the TOE interworks with Softcard Database – a module that is deployed on the same hardware appliance as the TOE. The TOE operates in two configurations: PKCS or CipherTools, depending on which API (library) is supported by the CM module.

The TOE and the CM act together the Qualified Signature Creation Device (QSCD).

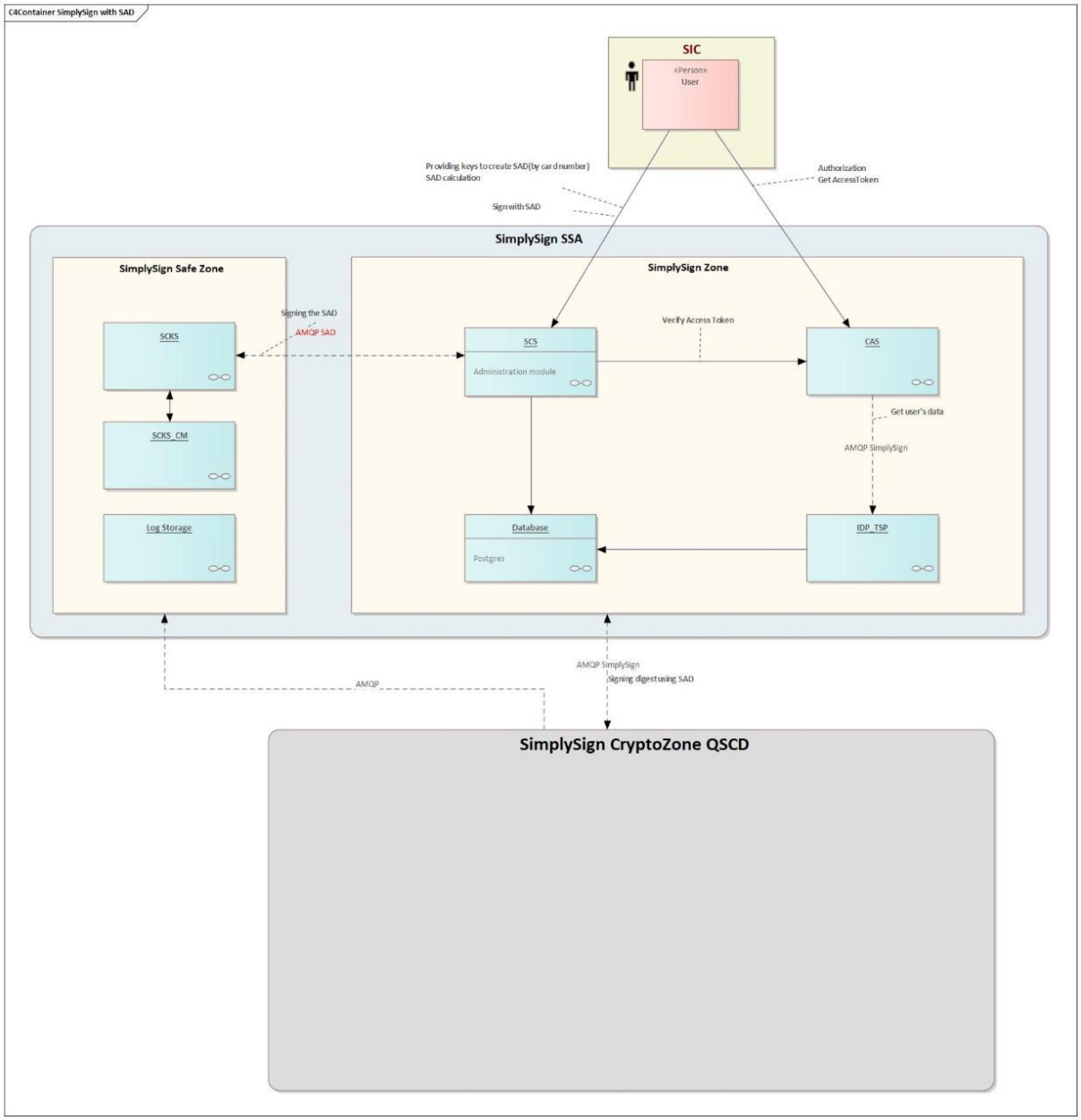

Figure 2: Required non-TOE Components

TOE consists of the following components:

1) Main TOE application called CKS;
2) Additional libraries and configuration files for PKCS and CT configurations;

that are supplemented by guidance documentation: SimplySign SAM Preparative guidance and SimplySign SAM Operational guidance.

Moreover, the following supporting package is provided together with the TOE (that package is not TOE components):

TOE supporting tools that are used for export/import cryptographic keys.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 4+AVA_VAN.5, according to Common Criteria v3.1 Revision 5.

Assurance Class	Assurance Component
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
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: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Security Functional Requirements

Functional requirement	Description
FAU: Security audit	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
FCS: Cryptographic support	FCS_COP.1 Cryptographic operation
	FCS_CKM.1Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FCS_RNG.1 Generation of random numbers
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_ETC.2 Export of user data with security attributes
	FDP_IFC.1 Subset information flow control
	FDP_IFF.1 Simple security attributes
	FDP_ITC.2 Import of user data with security attributes
	FDP_UCT.1 Basic data exchange confidentiality
	FDP_UIT.1 Data exchange integrity
FIA: Identification and authentication	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_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
FMT: Security management	FMT_MSA.1 Management of security attributes
	FMT_MSA.2 Secure security attributes
	FMT_MSA.3 Static attribute initialisation
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.2 Restrictions on security roles
FPT: Protection of the TSF	FPT_PHP.1 Passive detection of physical attack
	FPT_PHP.3 Resistance to physical attack
	FPT_RPL.1 Replay detection
	FPT_STM.1 Reliable time stamps
	FPT_TDC.1 Inter-TSF basic TSF data consistency
FTP: Trusted Paths/Channels	FTP_TRP.1 Inter-TSF Trusted path
	FTP_ITC.1 Inter-TSF trusted channel

Identification

Product:	SimplySign Signature Activation Module (SAM), version 6.2.0
Security Target:	Security Target for SimplySign Signature Activation Module (SAM), version 1.25, date of issue 2024-02-01

Security Policy

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.RANDOM

The TOE is required to generate random numbers that meet a specified quality metric. These random numbers shall be suitable for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes.

OSP.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities as appropriate by TSPs. This includes generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

3. Assumptions and Clarification of Scope

The assumptions are constraints to the conditions used to assure the security properties and functionalities introduced by the Security Target. All assumptions are to be taken into consideration when calculating the attack potential and affect the vulnerability of the product (mostly in terms of reduction). In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its usage and 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. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

Usage Assumptions

The Security Target [EVD-ST-V1.25] contains 4 assumptions related to the usage of the TOE.

A.PRIVILEGED_USER

It is assumed that all personnel administering the TOE are trusted, competent and possesses the resources and skills required for his tasks and is trained to conduct the activities he is responsible for.

A.SIGNER_ENROLMENT

The Signer shall be enrolled and certificates managed in conformance with the regulations given in eIDAS [5]. Guidance for how to implement an enrolment and certificate management system in conformance with eIDAS [5] are given in e.g. ETSI EN 319 411-1 [9] or for qualified certificate in e.g. ETSI EN 319 411-2 [10].

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

It is assumed that the Signer will not disclose his authentication factors.

A.SIGNER_DEVICE

It is assumed that the device and SIC used by Signer to interact with the SSA and the TOE is under the Signer's control for the signature operation, i.e. protected against malicious code.

Environmental Assumptions

The 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 Security Target [EVD-ST-V1.25] makes 6 assumptions on the environment of the TOE.

A.CA

It is assumed that the qualified TSP that issues Signer qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in eIDAS [5].

A.ACCESS_PROTECTED

It is assumed that the TOE operates in a protected environment that limits physical access to the TOE to authorised Privileged Users. The TOE software and hardware environment (including client applications) is installed and maintained by Privileged Users in a secure state that mitigates against the specific risks applicable to the deployment environment.

It is assumed that any audit generated by the TOE are only handled by authorised personal in a physical secured environment. The personal that carries these activities should act under established practices.

It is assumed that where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities must provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment.

A.AUTH_DATA

It is assumed that the SAP is designed in such a way that the activation of the signing key is under sole control of the Signer with a high level of confidence. If SAD is received by the TOE, it shall be assumed that the SAD was submitted under the full control of the Signer by means that are in possession of the Signer.

A.TSP_AUDITED

It is assumed that the TSP deploying the SSA and TOE is a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [5] and audited to be compliant with the requirements for TSP's given by eIDAS [5].

A.SEC_REQ

It is assumed that the TSP establishes an operating environment according to the security requirements for SCAL2 defined in EN 419 241-1 [6].

A.CERTIFICATION_AUTHORITY

It is assumed that the certificate for the R.SVD contains the R.SVD.

Clarification of Scope

Threats

The Security Target [EVD-ST-V1.25] defines threats which have been taken into consideration during the evaluation process.

T.ENROLMENT_SIGNER_IMPERSONATION

An attacker impersonates Signer during enrolment. As examples, it could be:

- by transferring wrong R.Signer to TOE from RA,
- by transferring wrong R.Reference_Signer_Authentication_Data to TOE from RA.

The assets R.Signer and R.Reference_Signer_Authentication_Data are threatened.

Such impersonation may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

An attacker is able to obtain whole or part of R.Reference_Signer_Authentication_Data during enrolment. This can be during generation, storage or transfer to the TOE or transfer between the Signer and TOE. As examples, it could be:

- by reading the data
- by changing the data, e.g. to a known value

The asset R.Reference_Signer_Authentication_Data is threatened.

Such data disclosure may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

The threats on enrolment are threats on the environment in case external authentication is supported by the TOE.

T.SVD_FORGERY

An attacker modifies the R.SVD during transmission to the RA or CA. This results in loss of R.SVD integrity in the binding of R.SVD to the signing key and to R.Signer.

The asset R.SVD is threatened.

If the CA relies on the generation of the key pair controlled by the TOE as specified in ETSI EN 319 411-1 [9] clause 6.3.3 d) then an attacker can forge signatures masquerading as the Signer.

T.ADMIN_IMPERSONATION

Attacker impersonates a Privileged User and updates R.Reference_Signer_Authentication_Data, R.Signing_Key_Id or R.SVD.

The assets R.Reference_Signer_Authentication_Data, R.SVD and R.Signing_Key_Id are threatened.

Such data modification may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

Attacker discloses or changes (e. g. to a known value) R.Reference_Signer_Authentication_Data during update and is able to create a signature.

The assets R.Reference_Signer_Authentication_Data and R.Signing_Key_Id are threatened. Such data disclosure may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of Signer.

T.AUTHENTICATION_SIGNER_IMPERSONATION

An attacker impersonates the Signer using forged R.Reference_Signer_Authentication_Data and transmits it to the TOE during SAP and uses it to sign the same or modified DTBS/R(s).

The assets R.Reference_Signer_Authentication_Data, R.SAD and R.Signing_Key_Id are threatened.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED

An attacker is able to modify R.Reference_Signer_Authentication_Data inside the TOE or during maintenance.

The asset R.Reference_Signer_Authentification_Data is threatened.

Such data modification may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.SAP_BYPASS

An attacker bypasses one or more steps in the SAP and is able to create a signature without the Signer having authorised the operation.

The asset R.SAD is threatened.

T.SAP_REPLAY

An attacker replays one or more steps of SAP and is able to create a signature without the Signer having authorised the operation.

The asset R.SAD is threatened.

T.SAD_FORGERY

An attacker forges or manipulates R.SAD during transfer in SAP and is able to create a signature without the Signer having authorised the operation.

The asset **R.SAD** is threatened.

T.SIGNATURE_REQUEST_DISCLOSURE

An attacker obtains knowledge of R.DTBS/R or R.SAD during transfer to TOE.

The asset R.DTBS/R and R.SAD is threatened.

If the R.DTBS/R or R.SAD do not require encrypted data then this threat is mitigated.

T.DTBSR_FORGERY

An attacker modifies R.DTBS/R during transfer to TOE and is able to create a signature on this modified R.DTBS/R without the Signer having authorised the operation on this R.DTBS/R.

The asset R.DTBS/R is threatened.

T.SIGNATURE_FORGERY

An attacker modifies R.Signature during or after creation or during transfer outside the TOE.

The asset R.Signature is threatened.

T.PRIVILEGED_USER_INSERTION

An attacker is able to create R.Privileged_User including R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as a Privileged User.

The assets R.Privileged_User and R.Reference_Privileged_User_Authentication_Data are threatened.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION

An attacker modifies R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as the Privileged User.

The asset R.Reference_Privileged_User_Authentication_Data is threatened.

T.AUTHORISATION_DATA_UPDATE

Attacker impersonates Privileged User and updates R.Authorisation_Data or R.Authorisation_Data2 and may be able to activate a signing key.

The asset R.Authorisation_Data2, R.Authorisation_Data and R.Signing_Key_Id are threatened.

T. AUTHORISATION_DATA _DISCLOSE

Attacker discloses R.Authorisation_Data or R.Authorisation_Data2 during update and is able to activate a signing key.

The asset R.Authorisation_Data2, R.Authorisation_Data and R.Signing_Key_Id are threatened.

T.CONTEXT_ALTERATION

An attacker modifies system configuration R.TSF_DATA to perform an unauthorised operation.

The assets R.Signing_Key_Id, R.SVD, R.SAD, R.Reference_Signer_Authentication_Data and R.TSF_DATA are threatened.

T.AUDIT_ALTERATION

An attacker modifies system audit and is able hide trace of TOE modification or usage.

The assets R.SVD, R.SAD, R.Signer, R.Reference_Signer_Authentication_Data, R.DTBS/R, R.Signature, R.AUDIT and R.TSF_DATA are threatened.

T.RANDOM

An attacker is able to guess system secrets R.RANDOM and able to create or modify TOE objects or participate in communication with external systems.

Security Policy

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.RANDOM

The TOE is required to generate random numbers that meet a specified quality metric. These random numbers shall be suitable for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes.

OSP.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities as appropriate by TSPs. This includes generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

4. Architectural Information

Physical scope

The TOE is a SAM software component that operates in dedicated hardware appliance. The appliance constitutes tamper-protected environment called CryptoZone. TOE is connected to the CM (embedded in the hardware appliance) through a trusted channel. The CM is installed with its software that provides the CM API.

The physical boundary of the TOE shall be tamper-protected in accordance with the requirements of EN 419241-1 [6].

The TOE operates in two configurations: PKCS or CT, depending on which API (library) of the CM module is used (PKCS#11 or CipherTools, respectively). Both configurations (PKCS and CT) represent TOE evaluated configurations.

TOE consists of the following components:

1) Main TOE application called CKS;
2) Additional libraries and configuration files for PKCS and CT configurations.

that are supplemented by guidance documentation: *SimplySign SAM Preparative guidance* and *SimplySign SAM Operational guidance*.

Moreover, the following supporting package is provided together with the TOE (that package is not TOE components):

TOE supporting tools that are used for export/import cryptographic keys;

Delivery of the TOE

The TOE (SimplySign SAM) is delivered in a tamper-protected TOE archive file: *CKS_v6.2.0.0.zip*.

The TOE, along with the associated documentation (*SimplySign SAM Preparative guidance* and *SimplySign SAM Operational guidance*) is placed in Artifactory repository system as a single archive file (ZIP file or TAR file – according to client requirements). TOE delivery is accomplished by emailing to a client a link to the archive file and a checksum calculated as the SHA256 or SHA512 hash value of the TOE archive file. TOE main archive file *CKS_v6.2.0.0.zip* includes the following components presented in the table below.

No	Type	Description	Name of the archive/file
1.	Software	Main TOE application called *CKS*	CKS_v6.2.0.0.zip
2.	*Software*	*TOE supporting tools (non-TOE component)*	*toeTools-1.0.1.tar*

No	Type	Description	Name of the archive/file
3.	Documentation	Preparative guidance	AGD_PRE for SimplySign SAM v.0.95.pdf
4.	Documentation	Operational guidance	AGD_OPE for SimplySign SAM v.0.94.pdf

Logical scope

The TOE (SimplySign SAM) provides a system for creating digital signatures as required by the eIDAS regulation. This chapter describes the logical security features offered by the TOE.

Roles & Available Functions

The TOE maintains the following roles: Privileged User and Unprivileged User – a Signer:

a) **Privileged User** - there is only one Privileged User in SimplySign SAM, which is SimplySign SSA. It executes various TOE specific operations, e.g., creates and manages Signers.

b) **Signers** - can request remote signing operations by interacting with SimplySign SSA and next authorizes these operations using the Signature Creation Application (SCA) to provide the required authentication data and SAD.

To activate a signing key in the TOE, the Signer had to be authenticated using SimplySign SSA (delegated authentication). The SAD is also required to activate Signer's signing key, because one of the SAD elements is a PIN code provided by the Signer in the SCA and next verified by the TOE (direct authentication).

Privileged User is created and authenticated during TOE initialization, by TLS certificate.

Privileged User and Signers can generate signing keys and Signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a Signer, as well as can disable a signing key identifier to be used by a Signer.

Moreover, the role of System Administrator is considered. System Administrator configures the TOE by editing the configuration files, and administrates TOE application from the level of operating system account (start/stop TOE application, checking the status of TOE service etc.). This role is not implemented as a TOE functionality. System Administrator is authenticated at the operating system level, using operating system accounts.

Signature operation

The TOE allows Signers to carry out remote signature. For signing operations, the TOE offers the following features:

- Signer can provide DTBS/R(s) for signing.
- The link between the Signer's authentication data, DTBS/R(s) and the Signer's key identifier is provided by the Signature Activation Data (SAD). The SAD is securely exchanged with the TOE using Signature Activation Protocol (SAP). Within the TOE, the following actions are performed:

- the TOE receives Signer's authorization request, with SAD and DTBS/R(s),
- the TOE verifies delegated authentication assertion and SADs provided by the Signer, and checks if the SAD binds together the Signer authentication, a DTBS/R(s) and signing key identifier,
- based on signing key identifier assigned to the Signer, the TOE activates the signing key within CM using Signer's Authorization Data,
- the TOE uses CM to create signature.

UTC time is the component of the SAD. This time is verified in the TOE (SimplySign SAM) after the SAD has been decrypted. It is assumed that "not too much" time can elapse between the creation of the SAD and its verification. Additionally, the TOE remembers its last value for a given Signer's AT and rejects repetitions. This way, TOE defends itself against a replay attack.

Audit

All events related to TOE security and Signers are recorded. SimplySign SSA provides access to logs intended for security auditing.

The event log covers all security relevant events. Each record is protected to prevent modifications, records are chained to prevent deletion. All audit records created by actions of Privileged User, and those created by requests handled by the TOE, are stored in the Log Storage component of SimplySign SSA. The connection between the TOE and Log Storage Component is provided using AMQP protocol secured with TLS. The audit trail does not include any data which allow to retrieve sensitive information.

Trusted Communication

TOE implements and enforces the following trusted communication methods and protocols:

- CM: the TOE (SimplySign SAM) communicates with the CM, located in the same hardware appliance, by direct calls of CM's vendor specific APIs. The API requires the TOE to transmit to the CM: a user card reference, a user PIN, a user private key reference. Upon successful verification of the PIN, the CM activates the user's private key and enables the signing of DTBS/R(s). Communication with the CM is only possible through the provided API of the CM vendor (the CM is part of QSCD, certified to meet the requirements of EN 419 221-5 [8]).
- SimplySign SSA: communicates with the TOE (SimplySign SAM) by exchanging AMQP protocol messages that are transferred through TLS channel established between the SSA and the TOE.
- Signature Creation Application: The Signature Creation Application (SCA) connects indirectly to the TOE, via SimplySign SSA, using an authenticated TLS channel between SimplySign SSA and the TOE.

5. Product Documentation

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

1. [EXT-1191] [EVD-ST-V1.25]	Security Target Simplysign, v. 1.25, issue date 01.02.2024 2024 (confidential document – LITE version available)
2. [EXT-1182] [EVD-AGD_PRE-V0.95]	SimplySign SAM Preparative guidance v. 0.95, issue date 01.02.2024 (confidential document)
3. [EXT-1181] [EVD-AGD_OPE-V0.94]	SimplySign SAM Operational Guidance, v. 0.94, issue date 01.02.2024 (confidential document)

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as: **Security Target for SimplySign Signature Activation Module (SAM), version 1.25, issue date 2024-02-01.**

The public version of this document is the same as complete Security Target described above and it is published along with this certification report on the Certification Body website.

6. IT security evaluation

The Evaluation Assurance Level EAL 4+ AVA_VAN.5 requires the independent and penetration testing provided by Evaluator and vulnerability analysis for a High attack potential.

The Evaluator has performed an installation and configuration of the TOE and its environment according to the [EVD-ST-V1.25] documentation. Installation and configuration of the TOE for AVA activities are the same as configuration used to execute the independent tests and is consistent with the evaluated configuration according to Security Target.

The Evaluator has examined set of developer test cases and selected test cases for independent testing. The sample has been chosen to cover all relevant TOE functionalities which refer to the Signer. The Evaluator noted that Signer (or any subject claiming to be him) is the only external entity that interacts with the TOE from outside TOE operational environment, which is tightly secured in accordance with security objectives for operational environment specified in the Security Target [EVD-ST-V1.25].

Evaluated Configuration

The test environment consists of following components.

This section includes description of the test environment that has been prepared to repeat developer's tests and perform independent tests by the Evaluator. The test environment consists of following components (see Figure 3):

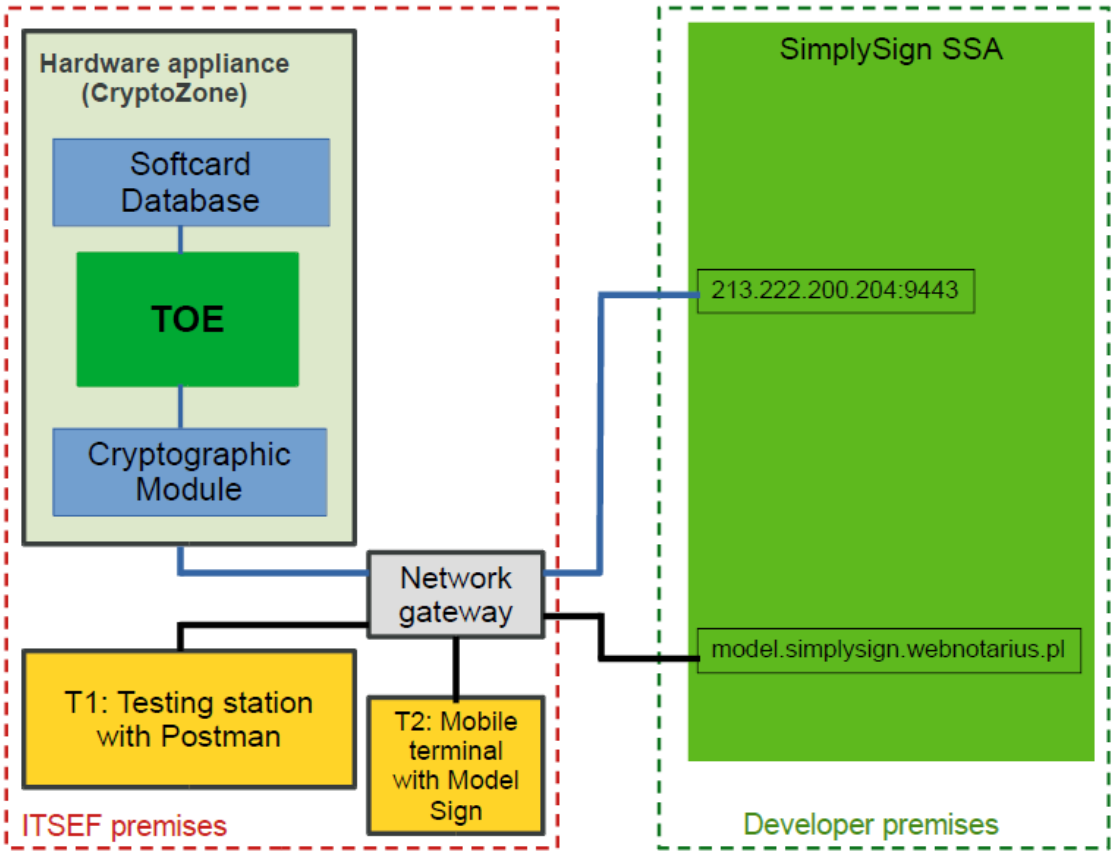

Figure 3: Test environment

- Hardware: DELL PowerEdge R740 server appliance.
- Software: Red Hat Enterprise Linux Server 7 x86_64 with PGBouncer, rsync and PostgreSQL Database packages.
- Cryptographic Module: certified nCipher nShield Solo XC, in the form of PCIe card installed on the server's motherboard
- Testing workstation T1 (Dell Latitude 5421 running Windows10 Pro 64bit, S/N: 2JJC4J3) with installed the following tools:

  Postman v9.16.0,

  Win64 OpenSSL v1.1.1q.
- Mobile terminal T2 (Samsung Galaxy S10, S/N: RF8M72ADJ0X) with installed mobile app Model Sing v.6.2.0, which is used for generation of authentication tokens.

Network infrastructure was established to provide:

- VPN connection between ITSEF network gateway and SimplySign SSA platform; the connection end point on SimplySign SSA side is: IP addres 213.222.200.204, port 9443; TOE hardware appliance IP address of used network interface is 192.168.1.154.
- Standard internet connection between T1 and T2 devices and SimplySign SSA platform; the connection end point on SimplySign SSA side is defined by hostname: model.simplysign.webnotarius.pl.

Testing station T1 is not directly connect to the TOE, but all interaction with the TOE is performed through SimplySign SSA platform. On the other hand, mobile terminal T2 is used only for user authentication in SimplySign SSA platform (to obtain access token) and it does not interact with TOE in any case.

To summarise, the network environment is shown in Figure 4:

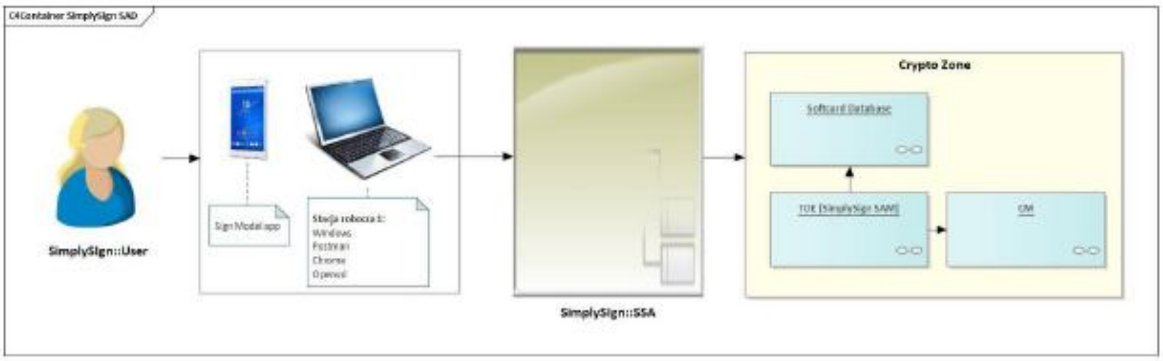

Figure 4: Network environment

Functional testing

The Evaluation Assurance Level EAL 4+ AVA_VAN.5 requires the Developer to deliver design information and test results, consistent with good commercial practise.

The Evaluator's task is divided into two activities. The Evaluators shall confirm the Developer's tests results using the sampling strategy described in details by the Common Criteria methodology. Additionally, the Evaluator's task is to devise and perform their own subset of tests which are intended to be the supplementary for the tests prepared by the Developer.

Developer testing

The Developer's testing verify the functionality of their corresponding TSFI either directly or indirectly (using the interface to test other functionality). The correspondence between the test documentation and TSFIs described in the functional specification is accurate.

The Developer prepared 47 tests cases and 13 tests precondition and conducted extensive testing campaign that includes performing of 276 tests: common set of specified 138 tests has been executed twice, for each of two TOE configuration mode: PKCS and CT.

All the tests have obtained a PASS verdict.

Evaluator testing

The Evaluator has examined set of developer test cases and selected test cases for independent testing. The sample has been chosen to cover all relevant TOE functionalities which refer to the Signer. The Evaluator noted that Signer (or any subject claiming to be him) is the only external entity that interacts with the TOE from outside TOE operational environment, which is tightly secured in accordance with security objectives for operational environment specified in the Security Target [EVD-ST-V1.25].

The Evaluator considers the selected subset of tests (27 test cases) as enough to confirm the validity of the developer's test results.

Additionally the Evaluators independently devised and conducted 10 independent test cases.

The final verdict takes into account the results of the developer's tests that were repeated by the Evaluator and the results of the tests devised by the Evaluator. The final result of Evaluator testing is PASS as all the test cases are assigned a PASS verdict.

All the 37 test cases have obtained a PASS verdict.

Penetration testing

The Evaluation Assurance Level EAL 4+ AVA_VAN.5 requires the independent and penetration testing provided by Evaluator and vulnerability analysis for a High attack potential.

The attack potential used for this evaluation is consistent with EAL 4+ AVA_VAN.5: High attack potential. The developed test plan was based on vulnerability survey of the evaluation evidence as well as the information available in the public domain was performed by the Evaluator covers development and operational vulnerabilities. TOE configuration used to execute the penetration test plan was consistent with the evaluated configuration according to the Security Target.

The vulnerability analysis, which identifies the presence of potential vulnerabilities, has been completed with a set of penetration tests to check if the potential vulnerabilities may be exploited in the TOE operational environment. The penetration tests have been performed with the assumption that the potential attack is HIGH.

The evaluation of documentation analysis and tests resulted in the 30 vulnerability notes, which represented a potential vulnerability. Analysis of the assumptions for the environment showed that, that only 4 of 30 vulnerability notes were can classified as applicable and therefore considered exploitable vulnerabilities. At the end, 4 vulnerabilities had an attack potential at the EAL level corresponding to the TOE evaluation and these vulnerabilities were used for the 4 penetration tests.

All penetration tests resulted with FAIL verdict, which is the proof for the resilience of the product and fulfilment of the assumptions of the Security Problem Definition.

Vulnerabilities and penetration tests summary

The following table summarizes the vulnerabilities and the status for the TOE under the Security Target [ST]:

Id.	Source	PenTest	Score	Exploited (Y/N)	Residual (Y/N)	Attack potential
0003-VUL-001	**AGD**	***0003-PT-001***	***n/a***	***N***	***N***	**-**
0003-VUL-002	**ADV**	***0003-PT-003***	***21***	***N***	***N***	***High***
0003-VUL-003	**ADV**	***0003-PT-005***	***24***	***N***	***N***	***High***
0003-VUL-004	**ADV**	***0003-PT-006***	**21**	***N***	***N***	***High***

Table 1: Summary of the potential vulnerabilities for the TOE, referenced as [TOE].

After providing all planned tests the Evaluator concluded that there were not exploitable vulnerabilities in the TOE operational environment according to the scope of this evaluation.

Evaluation verdicts

The Evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential Basic.

The Certifier reviewed the work of the Evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
ADV: Development	ADV_ARC.1 Security architecture description	PASS	CONFORMANT
	ADV_FSP.4 Complete functional specification	PASS	CONFORMANT

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
	ADV_IMP.1 Implementation representation of the TSF	PASS	CONFORMANT
	ADV_TDS.3 Basic modular design	PASS	CONFORMANT
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS	CONFORMANT
	AGD_PRE.1 Preparative procedures	PASS	CONFORMANT
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	PASS	CONFORMANT
	ALC_CMS.4 Problem tracking CM coverage	PASS	CONFORMANT
	ALC_DEL.1 Delivery procedures	PASS	CONFORMANT
	ALC_DVS.1 Identification of security measures	PASS	CONFORMANT
	ALC_LCD.1 Developer defined life-cycle model	PASS	CONFORMANT
	ALC_TAT.1 Well-defined development tools	PASS	CONFORMANT
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS	CONFORMANT
	ASE_ECD.1 Extended components definition	PASS	CONFORMANT
	ASE_INT.1 ST introduction	PASS	CONFORMANT
	ASE_OBJ.2 Security objectives	PASS	CONFORMANT
	ASE_REQ.2 Derived security requirements	PASS	CONFORMANT
	ASE_SPD.1 Security problem definition	PASS	CONFORMANT
	ASE_TSS.1 TOE summary specification	PASS	CONFORMANT
ATE: Tests	ATE_COV.2 Analysis of coverage	PASS	CONFORMANT
	ATE_DPT.1 Testing: basic design	PASS	CONFORMANT
	ATE_FUN.1 Functional testing	PASS	CONFORMANT
	ATE_IND.2 Independent testing - sample	PASS	CONFORMANT
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis	PASS	CONFORMANT

Evaluator Comments/Recommendations

Recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and shall to be considered when using the product.

The following usage recommendations are given:

- The TOE shall be operated in strictly defined trusted operational environment: the SimplySign system. SimplySign is a TW4S (Trustworthy System Supporting Server Signing) operated by Certum - a part of Asseco Group (TOE developer);
- The TOE operates with Cryptographic Module of nShield Solo XC family (provided by Entrust), which shall be certified in accordance with EN 419221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services;
- The user guidance must be read and understood to operate the TOE in an adequate manner according to the Security Target.

7. Certifier Recommendations

All the assurance components required by the evaluation level EAL 4 + AVA_VAN.5 of Common Criteria standard have been assigned a "PASS" verdict. Consequently, the laboratory assigned the "PASS" VERDICT to the whole evaluation due all the evaluation requirements are satisfied for the EAL 4 + AVA_VAN.5, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5.

Considering the obtained and validated evidence during the certification process of the product SimplySign Signature Activation Module (SAM), evaluation, **a positive resolution is proposed.**

8. Acronyms

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

9. Bibliography

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

1. [CC31p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5

2. [CC31p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5

3. [CC31p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5

4. [CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

5. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

6. EN 419241-1:2017, Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements

7. EN 419241-2:2019 Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing, February 2019.

8. EN 419221-5:2016, Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services

9. ETSI EN 319 411-1 v1.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

10. ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

References

List of normative documents

SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, v3.0, 8.01.2010

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02.07.2014

ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 17025 General requirements for competence of calibration and testing laboratories

ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

ISO/IEC 19790 Information Technology - Security Techniques - Security requirements for cryptographic modules

PC1 v. 2.4 IT Security Evaluation and Certification Scheme

List of related documents

[EXT-1178] [FIN-ETR-V1.1]	**Final Evaluation Technical Report, v. 1.1, issue date 02.02.2024 (ITSEF confidential document)**
[EXT-1191] [EVD-ST-V1.25]	**Security Target Simplysign, v. 1.25, issue date 01.02.2024 (confidential document)**
[EXT-1256] [EVD-ST-V1.25 Lite]	**Security Target Simplysign, v. 1.25 LITE, issue date 01.02.2024**
[EXT-1182] [EVD-AGD_PRE-V0.95]	**SimplySign SAM Preparative guidance v. 0.95, issue date 01.02.2024 (confidential document)**
[EXT-1181] [EVD-AGD_OPE-V0.94]	**SimplySign SAM Operational Guidance, v. 0.94, issue date 01.02.2024 (confidential document)**
[EXT-994] [EVD-ADV_FSP-V0.95]	**Functional Specification for SimplySign SAM, v. 0.95, issue date 12.07.2022 (confidential document)**
[EXT-1071] [EVD-ADV_ARC-V0.93]	**Security Architecture for SimplySign SAM, v. 0.93, issue date 12.07.2022 (confidential document)**
[EXT-1072] [EVD-ADV_TDS-V0.95]	**TOE Design for SimplySign SAM, v. 0.95, issue date 11.07.2022 (confidential document)**
[EXT-1073] [EVD-ADV_IMP-V0.91]	**Implementation Representation for SimplySign SAM, v. 0.91, issue date 23.09.2022 (confidential document)**
[EXT-1198] [EVD-AVA_VAN-v1.2]	**Vulnerability Analysis SimplySign, v1.2, issue date 02.02.2024 (ITSEF confidential document)**
[EXT-1197] [EVD-PEN_TEST-v1.2]	**Penetration Tests Plan and Report SimplySign SAM, v1.2, issue date 02.02.2024 (ITSEF confidential document)**
[EXT-1138] [EVD-AVA_VA-V2.0]	**P-0003_VA-02_1.0_AppSecVerificationSheet, v.1.0 (ITSEF confidential document)**
[EXT-1186][ALC_CMS-v0.96]	**ALC_CMS for SimplySign SAM, v0.96, issue date 01.02.2024 (confidential document)**
[EXT-1187][ALC_DEL-v0.94]	**ALC_DEL for SimplySign SAM, v0.94, issue date 01.02.2024 (confidential document)**

[EXT-1084] [TP-ATE_DEV-V.0.93]	**ATE EAL4 Test Plan and Report from Developer, v.0.93, issue date 14.02.2023 (confidential document)**
[EXT-1195] [TPR-ATE_LAB-V1.2]	**Independent Test Plan and Report SimplySign SAM, v1.2, issue date 02.02.2024 (ITSEF confidential document)**
[EXT-1086] [TP-ATE_DEV-V1.2]	**Attachment1 Opis ogólnych warunków, v.1.2, issue date 24.02.2023(confidential document)**
[EXT-1087] [TP-ATE_DEV-V0.93]	**Attachment2 Specyfikacja przypadków testowych, v.0.93, issue date 14.02.2023 (confidential document)**
[EXT-1088] [TR-ATE_DEV-V0.93]	**Attachment3 Test Report from Developer CT, v.0.93, issue date 14.02.2023 (confidential document)**
[EXT-1089] [TR-ATE_DEV-V0.93]	**Attachment4 Test Report from Developer PKCS, v.0.93, issue date 14.02.2023 (confidential document)**

Created by: Krzysztof Teresiński
Reviewed by: Diana Starodąb
Approved by: Paweł Kostkiewicz

Podpisany elektronicznie przez
NASK - PIB
29.10.2024
12:48:45 +01'00'