Security Operating System

(SOS)

SECURITY TARGET

EAL2

Table of Contents

CHANGE HISTORY

Date	Ver./Rev.	Description		
14/07/2007	**1.0**	Start Edition.		
		Author:	Marta Pardo	
		Review by:		**Date**
		Marta Pardo		14/09/2007
14/12/2007	**1.2**	Change		
		Author:	Carlos Jiménez	
		Review by:		**Date**
		Miguel Bañón		14/12/2007
13/02/2008	**1.3**	Change (product description, SFRs, TOE Summary Specification)		
		Author:	Jorge López Hernández-Ardieta	
		Review by:		**Date**
		Carlos Jiménez		27/02/2008
28/02/2008	**1.4**	Change: - Product description: No VM ware software is actually needed. - Security Functional Requirements: Administrator user. - TOE Summary Specification: updated.		
		Author:	Jorge López Hernández-Ardieta	
		Review by:		**Date**
06/03/2008	**1.5**	Change: - Security Functional Requirements: Deleted FPT_TST.1 and FMT_SMR.1 SFRs.		
		Author:	Jorge López Hernández-Ardieta	
		Review by:		**Date**
		Jose Emilio Rico		02/04/2008
04/04/2008	**1.6**	Change: - Introduction - Payload coverage - Rationales		
		Author:	Jorge López Hernández-Ardieta	

Date	Ver./Rev.	Description	
		Review by:	**Date**
		Jose Emilio Rico	09/04/2008
18/08/2008	**1.7**	Changes: - Included CRC integrity assurance mechanism. - Included user password-based authentication as an additional measure for increasing the security of the product. - Update the document to be consistent with previous changes.	
		Author: Jorge López Hernández-Ardieta	
		Review by:	**Date**
31/08/2008	**1.8**	Changes: - Added confidentiality SFRs. - Modified SOS philosophy from payload secure transportation (integrity) and execution to payload secure transportation (integrity and confidentiality)	
		Author: Jorge López Hernández-Ardieta	
		Review by:	**Date**

DISTRIBUTION AND APPROVAL HISTORY

Addressee	Ver. /Rev.	Number of Copies	Distribution Page Code and Date
Name and or Position and Organization.	Nº	Nº	

Introduction

ST reference

1 **Title:** SOS Security Target EAL2

2 **Version:** 1.8

3 **Author:** Secuware

4 **Publication date:** 31st August 2008

TOE reference

5 Security Operating System (SOS), Version 4.1.0.276

TOE overview

TOE usage

6 Secuware Security Operating System (SOS) is a software product to securely transport and access confidential information (payload) in even untrusted environments.

7 Secuware's security technology completely isolates resources of the physical host machine, ensuring that payload and SOS sensitive information cannot be accessed or modified by Internet-borne malware or unauthorised users.

8 SOS can be easily created and configured by a security administrator through a Graphical User Interface (GUI). This GUI tool, which is part of the evaluated TOE, allows selecting the payload to be inserted into SOS image, as well as the authentication credentials for future SOS loads and payload accesses.

9 There are six possible configurations respecting SOS user authentication:

- No authentication

  SOS image will be loaded without requiring the user to present any credentials.

- Password only

The user will have to provide a password when loading the SOS image.

- Single User Mode

  The user will have to insert the authorised Spanish electronic Identification Card (eDNI) when loading the SOS image.

- Single User Mode with password

  The user will have to insert the authorised eDNI and provide this password when loading the SOS image.

- Multiuser Mode

  The user will have to insert an eDNI when loading the SOS image.

- Multiuser Mode with password

  The user will have to insert an eDNI and provide a password when loading the SOS image.

10 “Password only”, “Single User Mode with password” and “Multiuser Mode with password” are the security configurations evaluated and certified under Common Criteria EAL2 requirements.

11 Although current certified configuration uses the eDNI as the security token, SOS supports more than 25 security tokens, including cryptographic tokens and biometric devices. Additional functionalities not certified but included in Secuware SOS cover auto-enrolment capabilities for end users and challenge-response mechanism, what remarkably increases the usability and security of the product. On the other hand, SOS can be completely customized according to the customer necessities.

12 SOS could also be used as a Secure Signature Creation Environment that, by means of a Secure Signature Creation Device (SSCDev) like the eDNI, offers a completely secure environment for the generation of legally-binding and non-repudiation electronic signatures on the payload.

13 SOS contributes to solutions of mobility, portability and flexibility using customized design of high security. Due to small SOS’s size, it could be sent through the network for recovery, diagnostic and remote management purposes, providing that the payload has been properly programmed. This allows making the most of Intel Intel® vPro™ technology, which simplifies management of desktops PCs with its

hardware-assisted capabilities. Intel® vPro™ remotely inventories, diagnoses, and repairs PCs with built-in manageability.

TOE type

14 The TOE comprises the GUI tool, called SOS Generator, and the resulting SOS image. SOS image can be considered as a security operating system based on a full encryption floppy-size image which allows authorised users to transport and access the payload in a secure manner. SOS image has been designed to be loaded under a physical environment. For instance, and due to its small size, SOS image can be encapsulated on a floppy R/O image.

15 Every time SOS boots, a new and completely clean environment is created, effectively preventing any malware from entering into the system.

16 TOE guarantees the integrity and confidentiality of the payload as well as the integrity of the TOE itself. Any change in the content of the SOS image (including the payload) will lead to a rejection of the booting. The TOE relies in the enciphering of the binary image of the secured operating system and a CRC 32-bit verification mechanism to protect SOS from unauthorized modifications.

17 Pre-boot authentication mechanism (PBA) assures that only the authorised user can load SOS and therefore access the payload it contains, guaranteeing its confidentiality. In case of configuring the SOS image for requiring user authentication, the user must authenticate to the SOS presenting his/her credentials. The credentials include the smart card **eDNI** (Spanish electronic Identification Card) and a user password.

18 In case of using a configuration based on an external user secret (password), the security of the product is highly increased. SOS configurations that imply the knowledge of a user password are the configurations recommended by Secuware and certified under CC EAL2 requirements, as well as the configurations that completely assure the integrity of SOS at the same time that the access to the payload is controlled.

19 The TOE does not rely on its IT environment to achieve any of its required security properties. However, it is supposed that the platform where SOS is loaded is free from any keylogger or malware that could compromise the password provided by the user. Therefore, it is assumed the existence of a secure communication channel between the user and the TOE for the password transference.

20 The asset of this TOE is the integrity and confidentiality of the user data (payload) and the integrity of the TSF itself.

- TOE guarantees the integrity and confidentiality of the payload. TOE guarantees also that the payload does not compromise the overall security of the TOE, even if it has malicious behaviour.
- TOE guarantees the integrity of the TOE itself, assuring that only unmodified SOS images can be launched.
- Pre-boot Authentication (PBA) ensures that only authorised users can load the SOS image and access the payload.
- SOS can run from a floppy disk – due to its small size – on an insecure environment or PC.
- The TOE originally doesn't have any default user definition. During SOS image creation stage, the authorised user (s) credentials can be configured for future authentication processes and TOE image encryption.

TOE components

Logical and Physical boundaries

21 Next Figure 1 shows the TOE logical boundary. The referenced elements are further described in next sections.

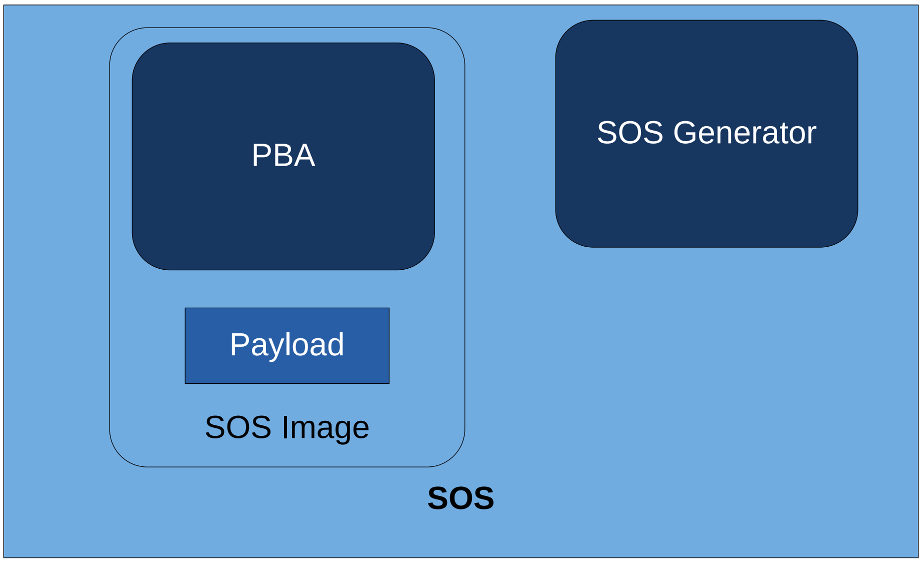

Figure 1 TOE logical boundary

22 Due to TOE nature (software product), there is no physical boundary.

SOS Generator

23 It is the Graphical User Interface tool used by the security administrator for generating SOS images. With this tool the administrator can configure:

- Payload to include in the SOS image to generate.
- eDNI-based Authentication data and password-based credentials, if desired.

Pre Boot Authentication (PBA)

24 PBA is the kernel of the Security Operating System. The principal PBA functionalities are encrypting and decrypting data transparently, user authentication and integrity verification. The pre-boot authentication feature prevents attackers from breaking into the system to attack secure environment.

Payload

25 The payload is part of the TOE, as the main asset to protect. It does not enforce any security properties of the TOE, and it can even be untrusted. In any case, the secure access to the payload is always ensured by the TOE.

26 Payload integrity and confidentiality is assured by TOE Security Functions, but payload behaviour is completely out of the scope of TOE evaluation. However, TOE assures that payload behaviour – even malicious behaviour – does not compromise the claimed security requirements.

Platform requirements

27 Following hardware requirements are needed for executing Secuware Security Operating System:

- SOS must be executed in a physical environment, like a floppy disk or by using Intel® vPro™ technology, among others. Therefore, depending on the mode of operation desired for SOS, the hardware or infrastructure requirements varies.
- Any Personal Computer or Server with basic memory and processor capabilities.

28 Following software requirements are needed for executing Secuware Security Operating System:

- SOS does not need any special software for its execution.

PP conformance claims

CC Conformance Claim

29 This Security Target complies with the Common Criteria, version 3.1, release 2, September 2007, for both the content and presentation requirements.

30 All functional and assurance security requirements laid out in this Security Target comply with parts 2 and 3 respectively of the above mentioned Common Criteria version. There are no extended requirements.

31 Evaluation Assurance Level 2 (EAL2).

PP Claim, Package Claim

32 This Security Target does not comply with any Protection Profile, but rather reflects the unique security properties of the TOE.

Security Problem Definition

TOE assets

SOS assets

33 The assets of the TOE are the user data (payload), the TSF itself and the information managed by the TSF to enforce the security properties of the TOE.

- **A.INT**;

34 The integrity of the assets is ensured to be maintained across invocations of the TOE execution. Any modification of the integrity of the TOE or of the TOE user data will result in a denial of service, thus avoiding its running in a compromised state.

35 This includes:

1. The integrity of the User Data (payload);
2. The integrity of the TSF itself (PBA);
3. The integrity of the user authentication credential.

- **A.CONF**;

36 Payload confidentiality is ensured to be maintained across invocations of the TOE execution, but only under the SOS configurations compliant to Common Criteria EAL2 requirements. The user must be correctly authenticated in order to access the payload included in the SOS image.

37 This includes:

4. The confidentiality of the User Data (payload);

Threats

Expected threats to the TOE assets

38 The expected attackers are qualified so as to have a basic attack potential, in accordance with the security assurance given by 0.

39 These expected attackers may be any malware or untrusted IT element in the TOE environment. The attacks may be launched off line over the

stored TOE at the environment file disk, or online to a running TOE instance.

- **T.INT;**

40 The TOE will be subject to attacks from untrusted IT elements from its IT environment. Any malware or untrusted IT element in the TOE environment, or even an untrusted user having access to the TOE may try to modify the integrity of the TOE payload or the TOE itself.

- **T.IMP;**

41 An unauthorized user attempts to impersonate a legitimate user, or to gain unauthorized execution of the TOE or unauthorized access to the payload. Thus, this threat is focused on compromising the confidentiality of the payload as well as subverting the access control mechanism implemented by the TOE.

Assumptions

- **AS.SECCHANNEL;**

42 It is assumed that the environment where the TOE is loaded is free from any keylogger or malware that could compromise the password provided by the user. Therefore, it is assumed the existence of a secure communication channel between the user and the TOE for the password transference.

Security Objectives

Security Objectives for the TOE

- **O.DETECTSOS;**

43 The TOE shall detect any attack against the integrity of the TOE, including the TSF or the TSF information.

- **O.DETECTPLD;**

44 The TOE shall detect any attack against the integrity of the User Data (Payload).

- **O.DENY;**

45 On the event of an integrity compromise, the TOE shall not be loaded or the payload be available to the user.

- **O.MNT;**

46 The TOE shall allow configuring the authorized users as well as the payload to be contained in the SOS image.

- **O.ACC;**

The TOE shall implement an access control mechanism, so that only authorized users can launch it and access the payload it contains.

Security Objectives for the TOE Environment

- **OE. SECCHANNEL;**

The TOE Environment shall provide the user with a secure communication channel between the user and the TOE for the password transference, in order to avoid the password compromise by any keylogger or malware.

Security Objectives rationale

47 The following table shows the trivial correspondence between the security objectives applicable to the TOE and the countered threat. Each threat is addressed by the defined security objectives.

Table 1 Security problem definition and security objectives

	T.INT	**T.IMP**
O.DETECTSOS	x	
O.DETECTPLD	x	
O.DENY	x	
O.MNT		x
O.ACC		x

48 Next, the rationale for each matching is provided:

49 **T.INT** sets that the TOE can be subject to integrity attacks over the TOE or the payload. These attacks can be carried out by untrusted IT elements from its IT environment, including any malware or untrusted IT element, or even untrusted users having access to the TOE. **O.DETECTSOS** indicates that the TOE shall detect any attack against the integrity of the TOE, including the TSF or the user authentication data. With **O.DETECTPLD** the TOE shall detect any attack against the integrity of the payload. Furthermore, **O.DENY** security objective obliges the TOE not to load or make the payload available on the event of an integrity compromise. Therefore, it is demonstrated that T.INT is fully countered by O.DETECTSOS, O.DETECTPLD and O.DENY.

50 **T.IMP** sets that an unauthorized user attempts to impersonate a legitimate user, or to gain unauthorized execution of the TOE or unauthorized access to the payload. This threat is counteracted by **O.MNT**, which allows creating and managing authorized users, and **O.ACC**, enforcing an access control mechanism, so that only authorized users can launch the TOE and access the payload. Payload confidentiality is thus assured since only authorised users can access the payload information.

51 The following table shows the trivial correspondence between the security objective applicable to the TOE Environment and the assumption identified above. The assumption is addressed by the defined security objectives.

	AS.SECCHANNEL
OE. SECCHANNEL	x

52

53 The correspondence is trivially seen.

Security Requirements for the TOE

Security Functional Requirements

FPT_FLS.1 **Failure with preservation of secure state**

FPT_FLS.1.1 **The TSF shall preserve a secure state when the following types of failures occur: [assignment: *unauthorized compromise of the integrity of the TSF or of the TSF data.*].**

FDP_SDI.2 **Stored data integrity monitoring and action**

FDP_SDI.2.1 **The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors of the SOS payload*] on all objects, based on the following attributes: [assignment: *payload signature as defined at TOE generation.*].**

FDP_SDI.2.2 **Upon detection of a data integrity error, the TSF shall [assignment: *enter into failure with preservation of secure state*].**

FIA_UID.1 **Timing of identification**

FIA_UID.1.1 **The TSF shall allow [assignment:**

- ***Invocation of login help*] on behalf of the user to be performed before the user is identified.**

FIA_UID.1.2 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

FIA_UAU.1 **Timing of authentication**

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **The TSF shall allow [assignment:**

- ***Invocation of login help*]** **on behalf of the user to be performed before the user is authenticated.**

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- ***For the Administrator, the configuration of***
  1. ***Payload;***
  2. ***Authorised User(s);***
- ***For the User, nothing.*].**

FDP_ACC.2 Complete access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: *"SOS access control SFP"*] on [assignment:

- ***Subjects: User(s)***
- ***Objects: the TOE itself.*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FMT_MSA.1 Management of security attributes

Dependencies: FDP_ACC.2 Complete access control

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **The TSF shall enforce the [assignment: *"SOS access control SFP"*] ~~to restrict the ability~~ avoiding to [selection: *change_default, query, modify, delete*] the security attributes [assignment: *User(s) eDNI number(s), CRC values and payload signature.*] to [assignment: *any user*].**

FMT_MSA.3 **Static attribute initialisation**

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MSA.3.1 **The TSF shall enforce the [assignment: *"SOS access control SFP"*] to provide [selection: *permissive*] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment: *the Administrator*] to specify alternative initial values to override the default values when an object or information is created.**

FDP_ACF.1 **Security attribute based access control**

Dependencies: FDP_ACC.2 Complete access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 **The TSF shall enforce the [assignment: *"SOS access control SFP"*] to objects based on the following: [assignment:**

- ***Subjects: User(s) and the corresponding eDNI number(s) and the user password, if required.***
- ***Objects: the TOE itself and its identity.***].

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *only authorised user(s) can launch the payload*].**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *any user not properly authenticated*].

FDP_ITC.1 Import of user data without security attributes

Dependencies: FDP_ACC.2 Complete access control

FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [assignment: *SOS access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *no additional importation control rule*].

Security Assurance Requirements

54 The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

- EAL2

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation of evidence elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C **The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.**

ADV_FSP.2 **Security-enforcing functional specification**

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D **The developer shall provide a functional specification.**

ADV_FSP.2.2D **The developer shall provide a tracing from the functional specification to the SFRs.**

Content and presentation of evidence elements:

ADV_FSP.2.1C **The functional specification shall completely represent the TSF.**

ADV_FSP.2.2C **The functional specification shall describe the purpose and method of use for all TSFI.**

ADV_FSP.2.3C **The functional specification shall identify and describe all parameters associated with each TSFI.**

ADV_FSP.2.4C **For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.**

ADV_FSP.2.5C **For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.**

ADV_FSP.2.6C **The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.**

ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D **The developer shall provide the design of the TOE.**

ADV_TDS.1.2D **The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.**

Content and presentation of evidence elements:

ADV_TDS.1.1C **The design shall describe the structure of the TOE in terms of subsystems.**

ADV_TDS.1.2C **The design shall identify all subsystems of the TSF.**

ADV_TDS.1.3C **The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.**

ADV_TDS.1.4C **The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.**

ADV_TDS.1.5C **The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.**

ADV_TDS.1.6C **The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.**

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

AGD_OPE.1.1D **The developer shall provide operational user guidance.**

Content and presentation of evidence elements:

AGD_OPE.1.1C **The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.**

AGD_OPE.1.2C **The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**

AGD_OPE.1.3C **The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**

AGD_OPE.1.4C **The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

AGD_OPE.1.5C **The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**

AGD_OPE.1.6C **The operational user guidance shall, for each user role, describe the security measures to be followed in order**

to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C **The operational user guidance shall be clear and reasonable.**

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D **The developer shall provide the TOE including its preparative procedures.**

Content and presentation of evidence elements:

AGD_PRE.1.1C **The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**

AGD_PRE.1.2C **The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D **The developer shall provide the TOE and a reference for the TOE.**

ALC_CMC.2.2D **The developer shall provide the CM documentation.**

ALC_CMC.2.3D **The developer shall use a CM system.**

Content and presentation of evidence elements:

ALC_CMC.2.1C **The TOE shall be labelled with its unique reference.**

ALC_CMC.2.2C **The CM documentation shall describe the method used to uniquely identify the configuration items.**

ALC_CMC.2.3C **The CM system shall uniquely identify all configuration items.**

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D **The developer shall provide a configuration list for the TOE.**

Content and presentation of evidence elements:

ALC_CMS.2.1C **The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.**

ALC_CMS.2.2C **The configuration list shall uniquely identify the configuration items.**

ALC_CMS.2.3C **For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.**

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D**The developer shall document procedures for delivery of the TOE or parts of it to the consumer.**

ALC_DEL.1.2D**The developer shall use the delivery procedures.**

Content and presentation of evidence elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation of evidence elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.2 Derived security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation of evidence elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C **The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.**

ASE_CCL.1.8C **The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.**

ASE_CCL.1.9C **The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**

ASE_CCL.1.10C **The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

ASE_SPD.1 **Security problem definition**

Dependencies: No dependencies.

Developer action elements:

ASE_APD.1.1D **The developer shall provide a security problem definition.**

Content and presentation of evidence elements:

ASE_SPD.1.1C **The security problem definition shall describe the threats.**

ASE_SPD.1.2C **All threats shall be described in terms of a threat agent, an asset, and an adverse action.**

ASE_SPD.1.3C **The security problem definition shall describe the OSPs.**

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_OBJ.2 **Security objectives**

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation of evidence elements:

ASE_OBJ.2.1CThe statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2CThe security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3CThe security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4CThe security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5CThe security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation of evidence elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation of evidence elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C **The statement of security requirements shall be internally consistent.**

ASE_TSS.1 **TOE summary specification**

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.2 Derived security requirements

ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ASE_TSS.1.1D **The developer shall provide a TOE summary specification.**

Content and presentation of evidence elements:

ASE_TSS.1.1C **The TOE summary specification shall describe how the TOE meets each SFR.**

ATE_COV.1 **Evidence of coverage**

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D **The developer shall provide evidence of the test coverage.**

Content and presentation of evidence elements:

ATE_COV.1.1C **The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Rationale for the Security Requirements

55 The following table shows the trivial correspondence between the security objectives applicable to the TOE and the defined security functional requirements. How these security objectives are implemented by fulfilment of the functional security requirements is trivial.

Table 2 Security objectives and functional requirements

	O.DETECTSOS	O.DETECTPLD	O.DENY	O.MNT	O.ACC
FPT_FLS.1 Failure with preservation of secure state	x		x		
FDP_SDI.2 Stored data integrity monitoring and action		x	x		
FIA_UID.1 Timing of identification					x
FIA_UAU.1 Timing of authentication					x
FMT_SMF.1 Specification of Management				x	

	O.DETECTSOS	O.DETECTPLD	O.DENY	O.MNT	O.ACC
Functions					
FDP_ACC.2 Complete access control					x
FMT_MSA.1 Management of security attributes				x	x
FMT_MSA.3 Static attribute initialisation				x	x
FDP_ACF.1 Security attribute based access control					X
FDP_ITC.1 Import of user data without security attributes				x	

56 **O.DETECTSOS** specifies that the TOE shall detect any attack against the integrity of the TOE, including the TSF or the user authentication data. This objective is fulfilled by **FPT_FLS.1 Failure with preservation of secure state**, through which the TSF shall preserve a

secure state when unauthorized compromise of the integrity of the TSF or of the TSF data occurs.

57 **O.DETECTPLD** specifies that the TOE shall detect any attack against the integrity of the User Data (Payload). This objective is covered by **FDP_SDI.2 Stored data integrity monitoring and action**, through which the TSF shall monitor user data stored in containers controlled by the TSF for integrity errors of the SOS payload on all objects, based on the payload signature as defined during TOE generation, and that upon detection of a data integrity error, the TSF shall enter into failure with preservation of secure state.

58 **O.DENY** specifies that on the event of an integrity compromise, the TOE shall not load or make the payload available. This objective is fulfilled by two SFRs. **FPT_FLS.1 Failure with preservation of secure state** sets that the TSF shall preserve a secure state when unauthorized compromise of the integrity of the TSF or of the TSF data occurs. And **FDP_SDI.2 Stored data integrity monitoring and action**, which indicates that the TSF shall monitor user data stored in containers controlled by the TSF for integrity errors of the SOS payload on all objects, based on the payload signature as defined during TOE generation, and that upon detection of a data integrity error, the TSF shall enter into failure with preservation of secure state.

59 **O.MNT** specifies that the TOE shall allow creating and managing authorized users as well as the payload to contain. Four SFRs cover this objective. **FMT_SMF.1 Specification of Management Functions**, which indicates that the TSF shall be capable of allowing the administrator to configure, by using SOS Generator tool, the Payload and the authorised user(s), if required. **FMT_MSA.1 Management of security attributes**, which sets that the TSF shall enforce the SOS access control SFP to avoid any user to change_default, query, modify or delete the security attributes user(s) eDNI number(s), CRC values, and payload signature. **FMT_MSA.3 Static attribute initialisation**, through which the TSF shall enforce the SOS access control SFP to provide permissive default values for security attributes that are used to enforce the SFP, and allow the Administrator to specify alternative initial values to override the default values when an object or information is created. **FDP_ITC.1 Import of user data without security attributes**, which indicates that the TSF shall enforce the SOS access control SFP when importing user data, controlled under the SFP, from outside of the TOE and ignore any security attributes associated with the user data when imported from outside the TOE.

60 **O.ACC** specifies that the TOE shall implement an access control mechanism, so that only authorized users can launch it. This objective is covered by six SFRs. **FIA_UID.1 Timing of identification**, through which the TSF shall allow invocation of login help on behalf of the user to be performed before the user is identified, and require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. **FIA_UAU.1 Timing of authentication**, which sets that the TSF shall allow invocation of login help on behalf of the user to be performed before the user is authenticated, and that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. **FDP_ACC.2 Complete access control**, which indicates that the TSF shall enforce the SOS access control SFP on user(s) and the TOE itself and all operations among subjects and objects covered by the SFP. It also indicates that the TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP. **FMT_MSA.1 Management of security attributes**, which sets that the TSF shall enforce the SOS access control SFP to avoid any user to change_default, query, modify or delete the security attributes user(s) eDNI number(s), CRC values and payload signature. **FMT_MSA.3 Static attribute initialisation**, through which the TSF shall enforce the SOS access control SFP to provide permissive default values for security attributes that are used to enforce the SFP, and allow the Administrator to specify alternative initial values to override the default values when an object or information is created. **FDP_ACF.1 Security attribute based access control**, through which the TSF shall enforce the SOS access control SFP to objects based on User(s) and the corresponding eDNI number(s), the user password, if required, the TOE itself and its identity. It also allows the TSF to enforce that only authorised user(s) can launch the payload. Finally, this SFR sets that the TSF shall explicitly deny access of any user not properly authenticated to objects.

61 There are two non-satisfied dependencies:

- FMT_MSA.1 depends on FMT_SMR.1
- FMT_MSA.3 depends on FMT_SMR.1

62 In both cases, the justification lies in the nature of SOS, which avoids associating users with roles. SOS image is a secured black box with no administration or management tool/interfaces. The only moment where certain data can be configured is at SOS generation. And this process is carried out only by the security administrator. The user receives the configured and generated SOS image as a closed IMG file which can be sent through the network or booted from a floppy disk.

63 The person managing the SOS generator tool is therefore supposed to be the security administrator, and the person loading the SOS image, the user.

64 The Security Assurance Requirements (SAR) have been selected according to an Evaluation Assurance Level 2 (EAL2). EAL2 has been selected due to market and clients demand.

TOE Summary Specification

TOE Security Functions

65 Each security function description contains the security requirements to which it corresponds, explaining how it specifically satisfies each of its related requirements.

Integrity Protection

FPT_FLS.1 Failure with preservation of secure state and FDP_SDI.2 Stored data integrity monitoring and action

66 The TOE relies in advanced encryption and CRC checksums verification to protect its assets from unauthorised modifications. The security mechanisms that enforces integrity protection relies in the secrecy of an external user password and his/her eDNI in order to accomplish such protection. Therefore, once the user has been properly authenticated, SOS PBA can verify if the integrity of the payload and the TOE itself has been maintained by checking the CRC 32-bit values of the protected information..

67 If any modification of the SOS image is performed, either to the TSF or the user data (payload), the TOE will detect it due to CRC verification failure and therefore neither the SOS image will be loaded nor the payload available.

Identification and Authentication

FIA_UID.1 Timing of identification and FIA_UAU.1 Timing of authentication

68 TOE permits adding identification/authentication mechanism for the booting process in order to restrict the access to the payload. There are mainly six possibilities during TOE image generation:

- No authentication: sometimes it is desirable to allow the access to the payload freely. SOS image will be loaded without requiring the user to present any credentials.

- Password only: the user will have to provide a password when loading the SOS image.

- Single User Mode: the user will have to insert the authorised Spanish electronic Identification Card (eDNI) when loading the SOS image.

- Single User Mode with password: the user will have to insert the authorised eDNI and provide this password when loading the SOS image.

- Multiuser Mode: the user will have to insert an eDNI when loading the SOS image.

- Multiuser Mode with password: the user will have to insert an eDNI and provide a password when loading the SOS image.

69 "Password only", "Single User Mode with password" and "Multiuser Mode with password" are the security configurations evaluated and certified under Common Criteria EAL2 requirements.

Access Control

FDP_ACC.2 Complete access control and FDP_ACF.1 Security attribute based access control

70 If authentication mechanism was configured during SOS image creation, then no subject can access the content (including the payload) of the SOS image if not properly authenticated.

71 The authentication mechanism (PBA) obliges the user to provide the authorised credentials, which cover the eDNI and the user password. If the eDNI-based authentication is enabled, the eDNI number is extracted by the TOE and compared to the authorised eDNI number kept in a secure manner inside the SOS image. If the password-based authentication mechanism has been configured, the user must insert it prior to payload access, increasing the security of the product.

72 The PBA is executed before the payload is decrypted and made available, protecting the TOE against any possible masquerade attack or payload confidentiality compromise.

Management

FMT_SMF.1 Specification of Management Functions, FMT_MSA.1 Management of security attributes and FMT_MSA.3 Static attribute initialisation

73 There are two possible users: the security administrator and the user. During SOS image creation (using SOS Generator), the security administrator configures the payload to include inside the SOS image as well as the credentials of the authorised user(s).

74 During SOS image usage, only authorised users can access the payload.

Profile configuration

FDP_ITC.1 Import of user data without security attributes

75 During SOS image creation, the security administrator uses the SOS Generator to select the payload and the user(s) credentials, if required. In this case, the authorised eDNI number/asterisk and/or password must be indicated.

TOE Security Assurance Measures

76 Next, the assurance measures applied for satisfying the EAL2 assurance requirements are described.

Development

77 Secuware provides SOS functional specification and basic design, giving an overall overview of the product interfaces description and modular decomposition. Security Architecture is also provided in order to understand the underlying security measures for assuring domain separation, safe initialization and start-up, and anti-tampering and non-bypassibilty properties for the TOE Security Functions.

78 The related documentation is the following:

- SOS Security Architecture (ADV_ARC.1).doc
- SOS Functional Specification (ADV_FSP.2).doc
- SOS Basic Design (ADV_TDS.1).doc

79 Assurance requirements fulfilled:

- ADV_ARC.1
- ADV_FSP.2
- ADV_TDS.1

Guidance Documents

80 Secuware documentation describes the steps necessary for a customer to achieve a secure acceptance of the SOS delivery in accordance to the delivery procedures, as well as the guideline to be followed in order to install SOS in a secure manner. User guidance and operational procedures are also included.

81 The related documentation is the following:

- SOS Operational User Guidance (AGD_OPE.1).doc
- SOS Preparative Procedures (AGD_PRE.1).doc

82 Assurance requirements fulfilled:

- AGD_OPE.1
- AGD_PRE.1

Life-Cycle support

83 SOS documentation covers how the product is managed throughout its life-cycle, uniquely identifying each release and assuring a correct configuration management. Also, secure delivery to end users and partners is also provided, assuring integrity protection against unauthorised modifications and proof of origin.

84 The related documentation is the following:

- Use of a CM System (ALC_CMC.2).doc
- SOS Parts of the TOE CM coverage (ALC_CMS.2).doc
- Delivery Procedures (ALC_DEL.1).doc

85 Assurance requirements fulfilled:

- ALC_CMC.2
- ALC_CMS.2
- ALC_DEL.1

Tests

86 SOS documentation also describes the test plan which identifies the tests performed and the scenarios prepared for each test.

87 The related documentation is the following:

- SOS Evidence of Coverage (ATE_COV.1).doc
- SOS Functional Testing (ATE_FUN.1).doc

88 Assurance requirements fulfilled:

- ATE_COV.1

- ATE_FUN.1