Declaración de seguridad
“Crypto Token USB”

DOCUMENTO:	DECLARACIÓN DE SEGURIDAD CRYPTO TOKEN USB
AUTOR:	DATATECH SDA S.L.
VERSIÓN:	3.2
FECHA:	20 07 2007

Índice

Índice de tablas

1 Introducción

1.1 Identificación

1.1.1 Identificación de la Declaración de Seguridad

1 **Título:** Declaración de seguridad Crypto Token USB

2 **Versión: 3.2**

3 **Autor:** DATATECH SDA, S.L.

4 **Fecha de publicación: : 20 07 2007**

1.1.2 Identificación del Objeto a Evaluar

5 **Fabricante:** DATATECH SDA, S.L.

6 **Nombre del producto:** Crypto Token USB

7 **Versión:** TK01S1.47

1.2 Resumen

8 Esta declaración de seguridad establece las bases para la evaluación Common Criteria del producto "Crypto Token USB".

1.3 Ajuste a la norma "Common Criteria" ISO/IEC 15408

PPT Pliego de prescripciones técnicas para el desarrollo del "Token cifrador del Ministerio de Defensa (Token USB)"

9 Esta declaración de seguridad cumple con los requisitos de la norma CC v. 2.3, ISO/IEC 15408:2005, partes 2 y 3, y define un nivel de garantía de evaluación EAL3, fortaleza de función baja.

10 La selección del nivel de evaluación, EAL3, se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen dictadas por el PPT.

11 EAL3 ofrece una garantía de seguridad moderada, y requiere de un análisis detallado del producto y de su desarrollo.

2 Descripción del producto a evaluar.

12 El Objeto a Evaluar (OE) es un dispositivo portátil USB, que permite el cifrado “off-line” de datos provenientes del ordenador al que se conecta. Es un dispositivo hardware con firmware embebido. El OE puede ser utilizado por cualquier host USB que implemente el protocolo a nivel de aplicación de los comandos del OE. Para facilitar su uso, el OE se entrega al usuario con una aplicación y drivers para la plataforma Windows, que está fuera del OE.

13 El OE tiene, además de cifrar y descifrar, la capacidad de almacenar datos, en forma de ficheros cifrados, en una memoria interna no volátil. Las capacidades de cifrado del OE se basan en el algoritmo AES, con claves de 256 bits, que se importan y exportan desde el OE, permitiendo el intercambio de ficheros cifrados entre varios OE, .

14 Por último, y para las dos funciones anteriores, el OE es capaz de almacenar de manera segura las distintas claves que utiliza en cada proceso, y de garantizar la confidencialidad del firmware interno que realiza todas estas funciones.

15 El Crypto Token USB está diseñado para su uso en organismos o empresas con administración de los soportes de almacenamiento externo, y cuenta con capacidades para la configuración y gestión del OE por parte de un Administrador, distintas de las operaciones básicas de cifrado y soporte de almacenamiento USB que presta a los usuarios.

16 El OE permite su identificación única mediante un identificador de CPU, lo que resulta de utilidad en la gestión de múltiples Crypto Token USB.

17 Se declaran como activos a proteger por el OE los siguientes:

a) Confidencialidad de aplicación interna del OE.

b) Confidencialidad de los Datos de Usuario: (USER DATA)

   1) Ficheros almacenados y cifrados en la memoria no volátil del Token USB.

   2) Claves de cifrado/descifrado.

c) Confidencialidad de los Datos de los Mecanismos de Seguridad: (TSF DATA)

   1) Códigos PIN y PUK de Administrador y Usuario.

3 Entorno de seguridad.

18 Los mecanismos y garantías de seguridad del OE son válidas para ataques directos sobre el interface de comunicaciones del dispositivo, sin relación con el ordenador donde se utiliza, o con datos extraídos del mismo. Tal escenario, por ejemplo, se dará cuando se sustrae un OE a su usuario legítimo.

3.1 Hipótesis.

3.1.1 Plataforma de uso

A.PCUSO El ordenador donde se utiliza el OE es fiable, y no contiene o es manejado por elementos hostiles de interceptación de activos de cifrado o de autenticación.

3.2 Amenazas a los activos del producto.

3.2.1 Ataques externos

T.CONF Un atacante, con capacidad baja (low attack potential), realiza, en una plataforma hostil y sin el conocimiento previo de datos obtenidos en una plataforma de uso, como claves de cifrado o de autenticación, todo tipo de observaciones y ataques sobre el interfase de comunicaciones del OE, al objeto de comprometer los activos del "Crypto Token USB".

19 Para los ataques anteriores, el atacante puede disponer de toda la información, drivers o aplicaciones que acompañan al OE, siempre hasta un grado de detalle y dificultad de obtención propia de su capacidad de ataque baja.

3.3 Políticas de seguridad.

3.3.1 Ataques físicos

P.TAMPER El OE no se diseñará con capacidad de reacción y protección de sus activos ante escenarios de ataque físico. Sin embargo, se incluirán los mecanismos físicos necesarios que permitan detectar tal tipo de ataques.

3.3.2 Configuración

P.ROLES El OE soportará los siguientes roles:

a) Administrador

b) Usuario

P.ADMIN El Administrador del OE podrá realizar las siguientes operaciones:

a) Asignar y cambiar las claves de autenticación PIN y PUK propios y del usuario;

b) Asignar, borrar, importar y exportar cambiar claves de cifrado y de almacenamiento de ficheros;

P.USUARIOC El usuario del OE podrá realizar las siguientes operaciones en las que intervienen las claves y los mecanismos criptográficos:

a) Asignar y cambiar sus claves de autenticación PIN y PUK;

b) Asignar, borrar, importar y exportar cambiar claves de cifrado y de almacenamiento de ficheros;

c) Cifrar y descrifrar ficheros, tanto con claves predefinidas como con claves suministradas para cada operación.

d) Realizar un reset del OE.

P.USUARIOSF El usuario del OE podrá utilizar la memoria no volátil del OE como un sistema de ficheros, con los siguientes servicios:

a) Lectura, escritura y borrado de ficheros y directorios.

b) Formateo del sistema de ficheros.

c) Obtención del almacenamiento disponible.

d) Asignar la fecha y hora de un fichero o directorio.

4 Objetivos de seguridad.

4.1 Objetivos de seguridad aplicables al producto.

O.CONF El OE garantiza la confidencialidad de los activos del mismo para todo tipo de ataques que no requieran la alteración física del "Crypto Token USB".

O.TAMPER El OE garantiza que cualquier intento de violentarlo físicamente pueda ser detectado posteriormente por los usuarios o administrador del "Crypto Token USB".

O.ROLES El OE implementa los servicios necesarios para su operación conforme a los roles y capacidades establecidos como política de uso.

4.2 Objetivos de seguridad aplicables al entorno.

O.ENV El entorno operacional del ordenador donde se utiliza el OE garantizará que no contiene o es manejado por elementos hostiles de interceptación de activos de cifrado o de autenticación, ni utilizado como mecanismo de ataque.

5 Requisitos de seguridad.

5.1 Requisitos de seguridad aplicables al producto.

5.1.1 Requisitos funcionales.

5.1.1.1 Requisitos funcionales para la autenticación de usuarios y control de acceso

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **GET_WORK_MODE**
- **GET_STATUS_PIN**
- **GET_NUM_CHECK_UPIN**
- **GET_NUM_CHECK_UPUK**
- **GET_NUM_CHECK_APIN**
- **GET_NUM_CHECK_APUK**

(Nota: El OE únicamente distingue dos identidades, coincidentes con los roles definidos en FMT_SMR.1 Security roles. La identificación es implícita a una autenticación correcta. Este componente se incluye en la declaración de seguridad por ajuste al modelo de dependencias de ISO/IEC 15408-2.) 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

- **GET_WORK_MODE**
- **GET_STATUS_PIN**
- **GET_NUM_CHECK_UPIN**
- **GET_NUM_CHECK_UPUK**
- **GET_NUM_CHECK_APIN**

- **GET_NUM_CHECK_APUK**

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.**

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when 3 PIN, 10 PUK unsuccessful authentication attempts occur related to autenticación de Usuario y Administrador .**

FIA_AFL.1.2 **When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall Si se sobrepasan los 3 intentos de autenticación por PIN, se bloquea la autenticación por PIN y se exige mediante PUK. Al introducir un PUK correcto, se solicitará la introduciión de un nuevo PIN. Si se sobrepasan los 10 intentos de autenticación por PUK, el OE bloquea los servicios de autenticación y se activa la puesta en estado de fábrica del "Crypto Token USB".**

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 **The TSF shall maintain the roles Administrador y Usuario.**

FMT_SMR.1.2 **The TSF shall be able to associate users with roles.**

FDP_ACC.2/Control de acceso OE Complete access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 **The TSF shall enforce the "Control de acceso OE" on procesos de invocación de commandos, activos del OE 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 in the TSC and any object within the TSC are covered by an access control SFP.**

FDP_ACF.1/Control de acceso OE 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 "Control de acceso OE" to objects based on the following:**

a) Lista de objetos: los activos del OE.

b) Sujeto: proceso de invocación de un comando del OE.

c) Atributos: identidad del usuario (valores: usuario, administrador), implícita por una autenticación satisfactoria.

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:**

a) Operaciones permitidas al Administrador:

1) Aplicación de Usuario

a) W_SET_USER_PIN

b) W_SET_USER_PUK

c) W_SET_ADMIN_PIN

d) W_SET_ADMIN_PUK

e) W_SET_STORAGE_KEY

f) W_SET_ENCRYPT_KEY

g) U_GET_INFO_KEY

h) U_DELETE_KEY

i) W_EXPORT_KEY

j) W_IMPORT_KEY

k) W_GET_ID_NUMBER

l) W_GET_VERSION

m) EXIT_APLIC

n) W_GET_F_APLIC

o) C_READ_APW

p) CANCEL_OPERATION

b) Operaciones permitidas al Usuario:

1) Aplicación de Usuario

a) W_SET_USER_PIN

b) W_SET_USER_PUK

c) W_SET_STORAGE_KEY

d) W_SET_ENCRYPT_KEY

e) **U_GET_INFO_KEY**

f) **U_DELETE_KEY**

g) **W_EXPORT_KEY**

h) **W_IMPORT_KEY**

i) **W_GET_ID_NUMBER**

j) **W_GET_VERSION**

k) **C_READ_APW**

l) **C_WRITE**

m) **C_READ**

n) **W_CLOSE**

o) **C_OPEN_W**

p) **C_OPEN_R**

q) **W_DELETE**

r) **W_MKDIR**

s) **W_RMDIR**

t) **W_CHDIR**

u) **W_GETCWDIR**

v) **W_FORMAT**

w) **W_GETFREESPACE**

x) **W_SET_DATE_TIME**

y) **W_FINDFIRST**

z) **W_FINDNEXT**

aa) **W_DESTROY**

bb) **CANCEL_OPERATION**

cc) **EXIT_APLIC**

dd) **W_GET_F_APLIC**

ee) **W_ENCRYPT_FILE**

ff) W_DECRYPT_FILE

gg) W_ENCRYPT_FILE_M

hh) W_DECRYPT_FILE_M

ii) GET_OPEN_FILE

jj) RENAME

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ninguna.**

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the cualquier operación no autorizada por las reglas anteriores.**

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 "Control de acceso OE" to provide Atributos fijos, Administrador y Usuario, a partir de su autenticación correcta, default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the Ninguno to specify alternative initial values to override the default values when an object or information is created.**

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 "Control de acceso OE" to restrict the ability to modificar the security attributes Atributos de Administrador o Usuario, a través del correspondiente cambio de claves de autenticación. to Administrador.**

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 **The TSF shall be capable of performing the following security management functions: Las asignadas al Administrador en FDP_ACF.1.2.**

5.1.1.2 Requisitos funcionales para las capacidades criptográficas del OE.

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.2 Complete access control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 **The TSF shall enforce the [assignment: "Control de acceso OE"] when importing user data, controlled under the SFP, from outside of the TSC.**

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

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: none].**

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.2 Complete access control]

FDP_ETC.1.1 **The TSF shall enforce the [assignment: "Control de acceso OE"] when exporting user data, controlled under the SFP(s), outside of the TSC.**

FDP_ETC.1.2 **The TSF shall export the user data without the user data's associated security attributes**

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes]

FCS_CKM.4.1 **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: modificación del índice de claves activas that meets the following: [assignment: ninguno].**

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment: cifrar, descifrar] in accordance with a specified cryptographic algorithm [assignment: AES] and cryptographic key sizes [assignment: 256 bits] that meet the following: [assignment:FIPS PUB 197].**

5.1.1.3 Requisitos funcionales para la implementación de O.Tamper

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 **The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.**

FPT_PHP.1.2 **The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.**

5.1.2 Requisitos de garantía de seguridad.

20 La evaluación se realizará conforme al nivel de garantía definido por:

a) EAL3

ACM_CAP.3 Authorisation controls

Dependencies: ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labelled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.3.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.8C The CM plan shall describe how the CM system is used.

ACM_CAP.3.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.11C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_SCP.1 TOE CM coverage

Dependencies: ACM_CAP.3 Authorisation controls

Developer action elements:

ACM_SCP.1.1D **The developer shall provide a list of configuration items for the TOE.**

Content and presentation of evidence elements:

ACM_SCP.1.1C **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.**

ADO_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation of evidence elements:

ADO_DEL.1.1C **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.**

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D **The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.**

Content and presentation of evidence elements:

ADO_IGS.1.1C **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.**

ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.1.1D **The developer shall provide a functional specification.**

Content and presentation of evidence elements:

ADV_FSP.1.1C **The functional specification shall describe the TSF and its external interfaces using an informal style.**

ADV_FSP.1.2C **The functional specification shall be internally consistent.**

ADV_FSP.1.3C **The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.**

ADV_FSP.1.4C **The functional specification shall completely represent the TSF.**

ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D **The developer shall provide the high-level design of the TSF.**

Content and presentation of evidence elements:

ADV_HLD.2.1C **The presentation of the high-level design shall be informal.**

ADV_HLD.2.2C **The high-level design shall be internally consistent.**

ADV_HLD.2.3C **The high-level design shall describe the structure of the TSF in terms of subsystems.**

ADV_HLD.2.4C **The high-level design shall describe the security functionality provided by each subsystem of the TSF.**

ADV_HLD.2.5C **The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.**

ADV_HLD.2.6C **The high-level design shall identify all interfaces to the subsystems of the TSF.**

ADV_HLD.2.7C **The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.**

ADV_HLD.2.8C **The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.**

ADV_HLD.2.9C **The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.**

ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements:

ADV_RCR.1.1D **The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.**

Content and presentation of evidence elements:

ADV_RCR.1.1C **For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.**

AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D **The developer shall provide administrator guidance addressed to system administrative personnel.**

Content and presentation of evidence elements:

AGD_ADM.1.1C **The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.**

AGD_ADM.1.2C **The administrator guidance shall describe how to administer the TOE in a secure manner.**

AGD_ADM.1.3C **The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.**

AGD_ADM.1.4C **The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.**

AGD_ADM.1.5C **The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.**

AGD_ADM.1.6C **The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

AGD_ADM.1.7C **The administrator guidance shall be consistent with all other documentation supplied for evaluation.**

AGD_ADM.1.8C **The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.**

AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D **The developer shall provide user guidance.**

Content and presentation of evidence elements:

AGD_USR.1.1C **The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.**

AGD_USR.1.2C **The user guidance shall describe the use of user-accessible security functions provided by the TOE.**

AGD_USR.1.3C **The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.**

AGD_USR.1.4C **The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.**

AGD_USR.1.5C **The user guidance shall be consistent with all other documentation supplied for evaluation.**

AGD_USR.1.6C **The user guidance shall describe all security requirements for the IT environment that are relevant to the user.**

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D **The developer shall produce development security documentation.**

Content and presentation of evidence elements:

ALC_DVS.1.1C **The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.**

ALC_DVS.1.2C **The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.**

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D **The developer shall provide an analysis of the test coverage.**

Content and presentation of evidence elements:

ATE_COV.2.1C **The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.**

ATE_COV.2.2C **The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.**

ATE_DPT.1 Testing: high-level design

Dependencies: ADV_HLD.2 Security enforcing high-level design
ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D **The developer shall provide the analysis of the depth of testing.**

Content and presentation of evidence elements:

ATE_DPT.1.1C **The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.**

ATE_FUN.1 Functional testing

Dependencies: No dependencies.

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, test procedure descriptions, expected test results and actual test results.**

ATE_FUN.1.2C **The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.**

ATE_FUN.1.3C **The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.**

ATE_FUN.1.4C **The expected test results shall show the anticipated outputs from a successful execution of the tests.**

ATE_FUN.1.5C **The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.**

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
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_MSU.1 Examination of guidance

Dependencies: ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.1.1D **The developer shall provide guidance documentation.**

Content and presentation of evidence elements:

AVA_MSU.1.1C **The guidance documentation 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.**

AVA_MSU.1.2C **The guidance documentation shall be complete, clear, consistent and reasonable.**

AVA_MSU.1.3C **The guidance documentation shall list all assumptions about the intended environment.**

AVA_MSU.1.4C **The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).**

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design

Developer action elements:

AVA_SOF.1.1D **The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.**

Content and presentation of evidence elements:

AVA_SOF.1.1C **For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.**

AVA_SOF.1.2C **For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.**

AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.1.1D **The developer shall perform a vulnerability analysis.**

AVA_VLA.1.2D **The developer shall provide vulnerability analysis documentation.**

Content and presentation of evidence elements:

AVA_VLA.1.1C **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.**

AVA_VLA.1.2C **The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.**

AVA_VLA.1.3C **The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.**

6 Requisitos de seguridad para el entorno

6.1 Requisitos no IT

NIT_TPC.1 Trusted PC

NIT_TPC.1.1 El entorno operacional del ordenador donde se utiliza el OE garantizará que no contiene o es manejado por elementos hostiles de interceptación de activos de cifrado o de autenticación, ni utilizado como mecanismo de ataque mediante los siguientes procedimientos:

b) Control de la integridad del PC de uso, de manera que el usuario conoce el contenido del PC de uso;

c) Conocimiento de la funcionalidad del PC de uso, de manera que el usuario conoce la ausencia de elementos hostiles en el PC de uso.

7 Síntesis de la especificación del producto

7.1 Especificación funcional

21 El interfase del OE es de tipo USB, en sus niveles físico y de comunicaciones a nivel de enlace.

22 A nivel de aplicación, el OE define su propio interfase, que define sus capacidades y sobre el que se esperan los ataques a los activos del "Crypto Token USB".

23 El interfase de aplicación se define mediante los correspondientes comandos, documentados en el "Manual de Comandos Crypto Token USB". Se agrupan y detallan a continuación tales comandos en funciones de seguridad del OE. Para cada función de seguridad se indican los comandos por los que se activa, estando el detalle del propósito y método de uso, efectos, excepciones y mensajes de error de los mismos, cuando son aplicables, en el "Manual de Comandos Crypto Token USB". La función F5. Función de protección física no tiene comandos asociados, al implementarse por diseño e inclusión de contramedidas físicas pasivas.

7.1.1 F1. Función de gestión de claves y usuarios

24 Las claves de autenticación PIN/PUK se asignan y modifican mediante los siguientes comandos, con los que se entiende se crean y gestionan también los roles del OE, FMT_SMR.1 Security roles, FMT_MSA.1 Management of security attributes, FMT_MSA.3 Static attribute initialisation y FMT_SMF.1 Specification of Management Functions:

a) W_SET_USER_PIN

b) W_SET_ADMIN_PIN

c) W_SET_USER_PUK

d) W_SET_ADMIN_PUK

7.1.2 F2. Función de Autenticación de Usuarios

25 La autenticación de Administrador y Usuario se realiza mediante la correcta presentación del correspondiente PIN. Si se sobrepasan los 3 intentos de autenticación por PIN, se bloquea la autenticación por PIN y se exige mediante PUK. Al introducir un PUK correcto, se solicitará la introducción de un nuevo PIN. Si se sobrepasan los 10 intentos de autenticación por PUK, el "Crypto Token USB" bloquea los servicios de autenticación y se activa la puesta en estado de fábrica.

a) U_SEND_PIN

b) U_SEND_PUK

c) A_SEND_PIN

d) A_SEND_PUK

26 Esta función satisface los requisitos funcionales relativos a la identificación y autenticación, FIA_UID.1 Timing of identification, FIA_UAU.1 Timing of authentication, FIA_AFL.1 Authentication failure handling.

27 La identificación y autenticación de usuarios FIA_UID.1 Timing of identification, FIA_UAU.1 Timing of authentication, FIA_AFL.1 Authentication failure handling, se implementa mediante una mecanismo (PIN o PUK) de naturaleza probabilística o permutacional.

7.1.3 F3. Función de control de acceso

28 Una vez correctamente autenticado, al usuario se le asigna una identidad de los roles definidos en FMT_SMR.1 Security roles. El control de acceso se activa cada vez que se invoca un comando del “Crypto Token USB", siendo la relación de comandos permitidos por identidad la siguiente:

a) Operaciones permitidas al Administrador:

1) Aplicación de Usuario

a) W_SET_USER_PIN

b) W_SET_USER_PUK

c) W_SET_ADMIN_PIN

d) W_SET_ADMIN_PUK

e) W_SET_STORAGE_KEY

f) W_SET_ENCRYPT_KEY

g) U_GET_INFO_KEY

h) U_DELETE_KEY

i) W_EXPORT_KEY

j) W_IMPORT_KEY

k) W_GET_ID_NUMBER

l) W_GET_VERSION

m) EXIT_APLIC

n) W_GET_F_APLIC

o) C_READ_APW

p) CANCEL_OPERATION

b) Operaciones permitidas al Usuario:

1) Aplicación de Usuario

a) W_SET_USER_PIN

b) W_SET_USER_PUK

c) W_SET_STORAGE_KEY

d) W_SET_ENCRYPT_KEY

e) U_GET_INFO_KEY

f) U_DELETE_KEY

g) W_EXPORT_KEY

h) W_IMPORT_KEY

i) W_GET_ID_NUMBER

j) W_GET_VERSION

k) C_READ_APW

l) C_WRITE

m) C_READ

n) W_CLOSE

o) C_OPEN_W

p) C_OPEN_R

q) W_DELETE

r) W_MKDIR

s) W_RMDIR

t) W_CHDIR

u) W_GETCWDIR

v) W_FORMAT

w) W_GETFREESPACE

x) W_SET_DATE_TIME

y) W_FINDFIRST

z) W_FINDNEXT

aa) W_DESTROY

bb) CANCEL_OPERATION

cc) EXIT_APLIC

dd) W_GET_F_APLIC

ee) W_ENCRYPT_FILE

ff) W_DECRYPT_FILE

gg) W_ENCRYPT_FILE_M

hh) W_DECRYPT_FILE_M

ii) GET_OPEN_FILE

jj) RENAME

29 La política y funciones de control de acceso, FDP_ACC.2 Complete access control y FDP_ACF.1 Security attribute based access control, se manifiestan mediante la correspondiente denegación o autorización de acceso a los activos del OE según lo indicado anteriormente.

7.1.4 F5. Función de protección física

30 La capacidad de detección de los ataques físicos que se exigen mediante FPT_PHP.1 Passive detection of physical attack se implementan mediante diversos mecanismos y técnicas de diseño, que se indican en el Documento "Diseño de Alto Nivel Crypto Token USB".

7.1.5 F6. Función de cifrado

31 Las capacidades criptográficas del token están implementadas con los siguientes comandos:

32 Cifrado y descifrado de archivos no almacenados en la memoria del token, requerido por FCS_COP.1 Cryptographic operation;

1) W_ENCRYPT_FILE

2) W_ENCRYPT_FILE_M

3) W_DECRYPT_FILE

4) W_DECRYPT_FILE_M

5) C_WRITE

6) C_READ

33 Importación de claves, FDP_ITC.1 Import of user data without security attributes;

1) W_IMPORT_KEY

2) W_SET_STORAGE_KEY

3) W_SET_ENCRYPT_KEY

34 Exportación de claves, FDP_ETC.1 Export of user data without security attributes;

1) W_EXPORT_KEY

35 Borrado de claves, FCS_CKM.4 Cryptographic key destruction;

1) U_DELETE_KEY

8 Garantía de seguridad

36 Los requisitos de garantía de seguridad se justifican mediante la presentación a la evaluación de los distintos documentos que acreditan el cumplimiento de los correspondientes requisitos.

37 Nota: las versiones finales se ajustarán al término de la evaluación.

Tabla 1 Documentación y requisitos de garantía de seguridad.

Componente	Documento
ACM_CAP.3 Authorisation controls	Plan de Gestión de Configuración del Crypto Token USB.
ACM_SCP.1 TOE CM coverage	Lista de Configuración
ADO_DEL.1 Delivery procedures	Procedimiento de entregas Crypto Token USB
ADO_IGS.1 Installation, generation, and start-up procedures	Manual de Comandos Crypto Token USB Configuración del Crypto Token USB
ADV_FSP.1 Informal functional specification	Apartado 7 de esta Declaración de Seguridad y Manual de comandos Crypto Token USB
ADV_HLD.2 Security enforcing high-level design	Diseño de Alto Nivel Crypto Token USB
ADV_RCR.1 Informal correspondence demonstration	Declaración de seguridad, apartado 7 Manual de Comandos Diseño de Alto NIvel
AGD_ADM.1 Administrator guidance	Manual de Comandos Crypto Token USB
AGD_USR.1 User guidance	Manual de Comandos Crypto Token USB
ALC_DVS.1 Identification of security measures	Manual de Protección para el desarrollo del "Crypto Token USB"
ATE_COV.2 Analysis of coverage	Test funcional Crypto Token USB
ATE_DPT.1 Testing: high-level design	Test funcional Crypto Token USB
ATE_FUN.1 Functional testing	Test funcional Crypto Token USB
AVA_MSU.1 Examination of guidance	Análisis de Vulnerabilidades.
AVA_SOF.1 Strength of TOE security function evaluation	Análisis de Vulnerabilidades.
AVA_VLA.1 Developer vulnerability analysis	Análisis de Vulnerabilidades.
ATE_IND.2 Independent testing - sample	Entrega del OE y entorno de pruebas.

9 Cumplimiento de “Perfiles de Protección”.

38 Esta declaración de seguridad no supone el cumplimiento de ningún perfil de protección.

10 Justificaciones.

10.1 Suficiencia de los objetivos de seguridad.

39 **O.TAMPER** implementa directamente la política de seguridad **P.TAMPER**. La justificación de que el objetivo implementa la política es trivial.

40 **O.ROLES** es una translación directa de implementación de las políticas de roles y capacidades asociadas, **P.ROLES**, **P.ADMIN**, **P.USUARIOC** y **P.USUARIOSF**. La redacción de **O.ROLES** se refiere directamente a las políticas que establecen los roles y sus capacidades, y por tanto resulta suficiente para su cumplimiento.

41 Frente al ataque **T.CONF**, el OE se defenderá garantizando la confidencialidad de los activos del mismo para todo tipo de ataques que no requieran la alteración física del "Crypto Token USB", que resulta ser **O.CONF**.

42 Finalmente, se traslada el cumplimiento de la hipótesis de uso **A.PCUSO** al entorno operacional del ordenador donde se utilice el OE, **O.ENV**.

10.2 Adecuación de los requisitos de seguridad.

43 Los roles indicados por **O.ROLES** se exigen en FMT_SMR.1 Security roles, y la adecuación a las capacidades asociadas se implementan con la política de control de acceso, requerida en FDP_ACC.2 Complete access control y en FDP_ACF.1 Security attribute based access control. Para su correcta implementación, se requiere por dependencias la exigencia de FMT_MSA.3 Static attribute initialisation, FMT_MSA.1 Management of security attributes y FMT_SMF.1 Specification of Management Functions, que permiten la gestión de los roles que discrimina la política de control de acceso, y que se definen en FMT_SMR.1 Security roles.

44 Para la satisfacción del objetivo **O.CONF**, se establece una doble estrategia, requiriendo en primer lugar al OE el control del acceso a los activos del mismo, que impida el compromiso de su confidencialidad ante usuarios no autorizados. Como medida adicional, se requiere que el OE utilice mecanismos criptográficos que garanticen la confidencialidad de los archivos almacenados en su sistema de ficheros, o datos de usuario en terminología de la norma Common Criteria.

45 La política de control de acceso se define en FDP_ACC.2 Complete access control y en FDP_ACF.1 Security attribute based access control. Para su correcta implementación, se requiere por dependencias la exigencia de FMT_MSA.3 Static attribute initialisation, FMT_MSA.1 Management of security attributes y FMT_SMF.1 Specification of Management Functions, que permiten la gestión de los roles que discrimina la política de control de acceso, y que se definen en FMT_SMR.1 Security roles.

46 Por último, para la correcta implementación de los requisitos funcionales de control de acceso que permiten el cumplimiento del objetivo de

confidencialidad, **O.CONF**, la identificación y autenticación de los usuarios autorizados se requiere por FIA_UAU.1 Timing of authentication y FIA_UID.1 Timing of identification, cualificados con FIA_AFL.1 Authentication failure handling.

47 Como se ha indicado, la confidencialidad de los datos de usuario **O.CONF**, se protege adicionalmente con los mecanismos de cifrado del "Crypto Token USB", exigido en los requisitos funcionales FCS_COP.1 Cryptographic operation de cifrado/descrifrado, FDP_ITC.1 Import of user data without security attributes para la importación de claves, FDP_ETC.1 Export of user data without security attributes, para la exportación de claves, y FCS_CKM.4 Cryptographic key destruction para su destrucción.

48 **O.TAMPER** se garantiza con la exigencia de FPT_PHP.1 Passive detection of physical attack., que se implementa con el diseño físico del OE, incluyendo una capa de resina que permite la detección de la apertura del OE.

49 La totalidad de objetivos de seguridad exigible al OE se satisface con la selección de requisitos funcionales indicados. Dichos requisitos funcionales forman un conjunto coherente y consistente, como se deriva del hecho de que todas las dependencias indicadas en la parte 2 de CC se encuentran satisfechas.

50 El mecanismo de PIN tiene una fortaleza de función igual o mayor a básica, lo que resulta coherente con el nivel de garantía de seguridad a exigir al OE, EAL3, y las características de capacidad de ataque baja de los atacantes esperados.

51 La fortaleza de los mecanismos de seguridad basados en algoritmos criptográficos está fuera de las garantías ofrecidas por esta declaración de seguridad, al no ser objeto de la evaluación de las normas CC/CEM.

52 Finalmente, se traslada el cumplimiento de los objetivos de seguridad del entorno operacional del ordenador donde se utilice el OE, **O.ENV**, al requisito **NIT_TPC.1.**

10.3 Justificación de la síntesis funcional.

10.3.1 Requisitos funcionales de seguridad.

53 Se indica en el apartado 7 Síntesis de la especificación del producto la relación de funciones de seguridad implementados por el OE, a saber

- F1. Función de gestión de claves y usuarios
- F2. Función de Autenticación de Usuarios
- F3. Función de control de acceso
- F5. Función de protección física
- F6, Función de cifrado

54 Dichas funciones dan cumplimiento a la totalidad de requisitos funcionales de seguridad, tal y como se detalla en el mencionado apartado 7. La

implementación de las funciones de seguridad se invoca mediante el ejercicio de los correspondientes interfaces funcionales, que resultan ser los comandos del OE (funciones F1 a F3 y F6) y su diseño físico para la F5.

55 De manera semejante a las dependencias de los requisitos funcionales de seguridad, F3 requiere de F1 y F2 para su correcto funcionamiento. F5 protege al TOE de ataques físicos de bajo potencial de ataque que pudiera comprometer la confidencialidad de los activos relevantes. F6 añade una protección adicional al sistema de ficheros del OE, al almacenar los ficheros cifrados, y exporta los servicios de cifrado/descifrado off-line de ficheros.

56 El mecanismo de PIN tiene una fortaleza de función igual o mayor a básica, en aplicación de la metodología de análisis del CEM, para un tamaño de PIN de 4 a 10 dígitos.

10.3.2 Medidas de garantía de seguridad.

57 Las medidas de garantía de seguridad satisfacen los requisitos del nivel de evaluación exigido, EAL3, tal como se deduce del análisis de su contenido y presentación.

58 La selección del nivel de evaluación, EAL3, se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen dictadas por el PPT.

10.3.3 Interpretaciones aplicadas

59 RI 145 FCS component dependencies on FMT_MSA.2