ADVANTIS CRYPTO 3.1
DECLARACIÓN DE SEGURIDAD
VERSIÓN PÚBLICA

Versión: 1.2

18/08/2008

Referencia TI345

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN 1
1.1 Identificación 1
1.1.1 Identificación de la Declaración de Seguridad 1
1.1.2 Identificación del Objeto a Evaluar 1
1.2 Resumen 1
1.3 Ajuste a la norma “Common Criteria” ISO/IEC 15408 2
2. DESCRIPCIÓN DEL PRODUCTO A EVALUAR 3
2.1 Ciclo de vida del TOE 5
3. ENTORNO DE SEGURIDAD 7
3.1 Activos, usuarios y atacantes 7
3.2 Hipótesis. 7
3.3 Amenazas a los activos del producto. 7
3.4 Políticas de seguridad 7
4. OBJETIVOS DE SEGURIDAD 8
4.1 Objetivos de seguridad aplicables al producto. 8
4.2 Objetivos de seguridad aplicables al entorno. 8
5. REQUISITOS DE SEGURIDAD 9
5.1 Requisitos funcionales de seguridad aplicables al producto 9
5.1.1 Soporte Criptográfico (FCS) 9
5.1.1.1 Generación de claves criptográficas (FCS_CKM.1) 9
5.1.1.2 Destrucción de claves criptográficas (FCS_CKM.4) 9
5.1.1.3 Operación criptográfica (FCS_COP.1) 9
5.1.2 Protección de datos de usuario (FDP) 10
5.1.2.1 Subconjunto de control de acceso (FDP_ACC.1) 10
5.1.2.2 Control de acceso basado en atributos de seguridad (FDP_ACF.1) 10
5.1.2.3 Exportación de datos de usuario sin atributos de seguridad (FDP_ETC.1) 10
5.1.2.4 Importación de datos de usuario sin atributos de seguridad (FDP_ITC.1) 10
5.1.2.5 Protección de la información residual (FDP_RIP.1) 10

5.1.2.6 Acción y supervisión de la integridad de los datos almacenados (FDP_SDI.2) 10
5.1.2.7 Integridad en el intercambio de datos (FDP_UIT.1) 10
5.1.3 Identificación y autenticación (FIA) 11
5.1.3.1 Manejo de fallos de autenticación (FIA_AFL.1) 11
5.1.3.2 Definición de atributos de usuario (FIA_ATD.1) 11
5.1.3.3 Secuencia de autenticación (FIA_UAU.1) 11
5.1.3.4 Secuencia de identificación (FIA_UID.1) 11
5.1.4 Gestión de la seguridad (FMT) 11
5.1.4.1 Gestión del comportamiento de las funciones de seguridad (FMT_MOF.1) 11
5.1.4.2 Gestión de los atributos de seguridad (FMT_MSA.1) 11
5.1.4.3 Atributos de seguridad seguros (FMT_MSA.2) 12
5.1.4.4 Inicialización de atributos estáticos (FMT_MSA.3) 12
5.1.4.5 Gestión de datos de TSF (FMT_MTD.1) 12
5.1.4.6 Especificación de las Funciones de Gestión (FMT_SMF.1) 12
5.1.4.7 Roles de seguridad (FMT_SMR.1) 13
5.1.5 Protección de la TSF (FPT) 13
5.1.5.1 Pruebas de la máquina abstracta (FPT_AMT.1) 13
5.1.5.2 Emisiones del TOE (FPT_EMSEC.1) 13
5.1.5.3 Fallo con preservación del estado seguro (FPT_FLS.1) 14
5.1.5.4 Detección pasiva de ataques físicos (FPT_PHP.1) 14
5.1.5.5 Resistencia al ataque físico (FPT_PHP.3) 14
5.1.5.6 Pruebas de TSF (FPT_TST.1) 14
5.1.6 Ruta/canales seguros (FTP) 14
5.1.6.1 Canales seguros Inter-TSF (FTP_ITC.1) 14
5.1.6.2 Ruta segura (FTP_TRP.1) 15
5.2 Requisitos de Garantía 16
5.2.1 Automatización parcial de CM (ACM_AUT.1) 16
5.2.2 Soporte de generación y procedimientos de aceptación (ACM_CAP.4) 16
5.2.3 Cobertura de CM de seguimiento de problemas (ACM_SCP.2) 17
5.2.4 Detección de modificaciones (ADO_DEL.2) 18
5.2.5 Instalación, generación, y procedimientos de arranque (ADO_IGS.1). 18
5.2.6 Interfaces externas totalmente definidos (ADV_FSP.2) 20

5.2.7 Diseño de alto nivel para la imposición de seguridad (ADV_HLD.2) 20
5.2.8 Subconjunto de implementación del TSF (ADV_IMP.1) 21
5.2.9 Diseño de bajo nivel descriptivo (ADV_LLD.1) 22
5.2.10 Demostración informal de la correspondencia (ADV_RCR.1) 23
5.2.11 Modelo informal de política de seguridad del TOE (ADV_SPM.1) 23
5.2.12 Guía del administrador (AGD_ADM.1) 24
5.2.13 Guía de Usuario (AGD_USR.1) 25
5.2.14 Identificación de las medidas de seguridad (ALC_DVS.1) 25
5.2.15 Modelo del ciclo de vida definido por el desarrollador (ALC_LCD.1) 26
5.2.16 Herramientas de desarrollo bien definidas (ALC_TAT.1) 26
5.2.17 Análisis de la cobertura (ATE_COV.2) 27
5.2.18 Pruebas: diseño de alto nivel (ATE_DPT.1) 27
5.2.19 Pruebas funcionales (ATE_FUN.1) 28
5.2.20 Pruebas independientes – ejemplo (ATE_IND.2) 28
5.2.21 Análisis y pruebas sobre los estados inseguros (AVA_MSU.3) 29
5.2.22 Evaluación de la fortaleza de las funciones de seguridad del TOE (AVA_SOF.1) 30
5.2.23 Alta resistencia (AVA_VLA.4) 30
5.3 Requisitos funcionales de seguridad aplicables al entorno 31
5.3.1 Requisitos de seguridad aplicables al entorno de las TI. 31
5.3.1.1 Aplicación de generación de certificados 31
5.3.1.1.1 FCS_CKM.2 Distribución de claves criptográficas 31
5.3.1.1.2 FCS_CKM.3 Acceso de clave criptográfica 32
5.3.1.1.3 Integridad en el intercambio de datos (FDP_UIT.1) 32
5.3.1.1.4 Canal seguro inter-TSF (FTP_ITC.1) 32
5.3.1.2 Aplicación de creación de firma 32
5.3.1.2.1 FCS_COP.1 Operación criptográfica 32
5.3.1.2.2 Integridad en el intercambio de datos (FDP_UIT.1) 32
5.3.1.2.3 Canal seguro inter-TSF (FTP_ITC.1) 32
5.3.1.2.4 Ruta segura (FTP_TRP.1) 33
5.4 Requisitos de seguridad aplicables al entorno ajeno a las IT 33

6. SÍNTESIS DE LA ESPECIFICACIÓN DEL PRODUCTO 34

6.1 Especificación funcional 34

6.1.1 Fortaleza de mecanismos 40
6.1.1.1 Fortaleza de los mecanismos de PIN y PUK 40
6.1.1.2 Mecanismo de canal seguro 42
6.2 Garantía de seguridad 43

7. CUMPLIMIENTO DE PERFILES DE PROTECCIÓN 46
7.1 Perfil de Protección CWA14169 46
7.1.1 Referencia 46
7.1.2 Adaptación y operaciones fijadas 46

8. JUSTIFICACIONES 47
8.1 Suficiencia de los objetivos de seguridad 47
8.2 Adecuación de los requisitos de seguridad 47
8.3 Justificación de la síntesis funcional 47
8.3.1 Combinación de los comandos de la tarjeta 47
8.3.2 Trazabilidad de la especificación funcional 47
8.3.3 Justificación de la cobertura de los requerimientos de seguridad 49
8.3.4 Fortaleza de las funciones 50
8.3.5 Medidas de garantía de seguridad. 50
8.4 Justificación del cumplimiento de Perfiles de Protección 51
8.5 Justificación del nivel de garantía de evaluación EAL4+ 52

9. ACRÓNIMOS 53

10. REFERENCIAS 55

ÍNDICE DE TABLAS

Tabla 1.- Ciclo de vida del TOE 5
Tabla 2.- Relación SF's - interfaces 39
Tabla 3.- Documentación y requisitos de garantía de seguridad 45
Tabla 4.- Trazabilidad de la especificación funcional 48
Tabla 5.- Justificación de la cobertura de los requerimientos de seguridad 50

ÍNDICE DE FIGURAS

Figura 1.- Ciclo de vida conforme a CWA 14169 6

Hoja de Información General

CONTROL DOCUMENTAL

PROYECTO:	ADVANTIS CRYPTO
TÍTULO:	ADVANTIS CRYPTO 3.1 DECLARACIÓN DE SEGURIDAD VERSIÓN PÚBLICA
CÓDIGO DE REFERENCIA:	TI345
VERSIÓN:	1.2
FECHA DE EDICIÓN:	18/08/2008
FICHERO:	TI345 - Advantis Crypto 3.1 - Declaracion de Seguridad_Publica_v1_2.doc
HERRAMIENTAS DE EDICIÓN:	Microsoft Office Word
AUTORES:	Servicios para Medios de Pago, S.A.
COMPAÑÍA:	SERMEPA

Control de Versiones

Versión	Fecha	Afecta	Breve descripción del cambio
1.0	30/07/2008	Todo el documento.	Declaración de Seguridad - Versión pública.
1.1	11/08/2008	Apartado 8.3.3	Modificación de la tabla.
1.2	18/08/2008	Todo el documento.	Se sustituye la calificación del documento "confidencial" por "público" en los pies de página.

1. INTRODUCCIÓN

1.1 Identificación

1.1.1 Identificación de la Declaración de Seguridad

Título: Declaración de seguridad

Versión: 1.0

Revisión: 2

Autor: Servicios para medios de pago, S.A.

Fecha de publicación: 30/07/2008

1.1.2 Identificación del Objeto a Evaluar

Fabricante: Servicios para medios de pago, S.A.

Nombre del producto: Advantis Crypto

Versión: 3.1

1.2 Resumen

Esta declaración de seguridad establece las bases para la evaluación Common Criteria de aplicación de Firma Digital que se ajusta al Perfil de Protección Secure Signature-Creation Device Type 3 Protection Profile, versión 1.05 (SSCD PP) [1] incluida en la tarjeta inteligente “Advantis Crypto”.

La tarjeta Advantis Crypto es una tarjeta inteligente con capacidad criptográfica.

La aplicación de Firma cumple con los siguientes estándares establecidos para tarjetas inteligentes:

a) ISO/IEC 7816-4 [2];

b) ISO/IEC 7816-5 [3];

c) ISO/IEC 7816-8 [4];

d) PKCS#1: RSA Encryption Standard, Versión 1.5, Noviembre, 1993 [6];

e) PKCS#15: Cryptographic Token Information Standard, Versión 1.0, Abril 1999 [7]

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

Esta declaración de seguridad cumple con los requisitos de la norma CC versión 2.3, partes 2 y 3, y define un nivel de garantía de evaluación EAL4, aumentado por los componentes **Análisis y pruebas sobre los estados inseguros (AVA_MSU.3)** y **Alta resistencia (AVA_VLA.4)**. El nivel mínimo de SOF que proporciona el TOE es **high**.

La selección del nivel de evaluación se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen fijadas por **CWA 14169:2004. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05 (Perfil de Protección - Dispositivo Seguro de Creación de Firma)** y que determina un producto altamente resistente a diferentes ataques.

2. DESCRIPCIÓN DEL PRODUCTO A EVALUAR

La tarjeta Advantis Crypto es una tarjeta inteligente con capacidad criptográfica.

Es una tarjeta multi-aplicación capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad. Dispone de una estructura jerárquica de ficheros y datos tipo árbol. Las distintas aplicaciones que implementa son:

a) Aplicación VISA/EMV

b) Aplicación propietaria monedero Advantis

c) Aplicación monedero CEPS

d) Aplicación WIM

e) Aplicación propietaria Firma Digital

f) Aplicación Firma Digital CWA14169

La tarjeta Advantis Crypto es por tanto un dispositivo seguro de creación de firma electrónica, y como tal cumple con los requisitos de seguridad aplicables, recogidos en [1]. **Esta Declaración de Seguridad se centra en las exigencias de seguridad necesarias para la firma electrónica CWA14196** (a partir de ahora simplemente firma digital o firma electrónica), **y no abarca otras aplicaciones o configuraciones de la tarjeta, que no forman parte del TOE. Éste se limita a la aplicación de firma digital**.

El sistema operativo o máscara Advantis Crypto constituye el código que el fabricante del componente incluye en el mismo.

El sistema operativo define el funcionamiento de la tarjeta en los siguientes ámbitos:

1. **Gestión de memoria**: el sistema operativo predetermina y gestiona la disposición lógica y física de memoria EEPROM. Con ello, ofrece a los emisores de aplicaciones estructuras definidas de memoria a las que se pueden añadir las condiciones de acceso necesarias en función de la política de seguridad de sus aplicaciones. El sistema operativo gestiona la memoria a través de estructuras TLV, que deben codificarse de acuerdo con las reglas de codificación de estructuras BER-TLV, con etiquetas y longitudes de 1 ó 2 bytes únicamente.

2. **Seguridad**: el sistema operativo incluye diversos procedimientos criptográficos y las claves secretas asociadas. De esta forma, es posible realizar operaciones protegidas de lectura, escritura y actualización en la memoria de la tarjeta, así como autenticaciones tanto externas como internas. Además, gestiona la verificación de los códigos secretos y certificados utilizados por la aplicación exterior para obtener acceso a la tarjeta.

3. **Interfaz de comunicaciones (APDU)**: el sistema operativo dispone de un conjunto definido de comandos y gestiona un protocolo de comunicación estándar, T = 0 (ISO 7816-3)

4. **Ciclo de vida de la tarjeta**: el sistema operativo gestiona totalmente las diferentes fases en el ciclo de vida de la tarjeta.

El circuito integrado de Infineon AG Technologies sobre el que se implementa el sistema operativo **Advantis Crypto** es el **SLE66CX80PE**.

Ha superado la evaluación CC alcanzando el nivel de garantía EAL5 +, satisfaciendo los requisitos expresados en el Perfil de Protección BSI-PP-0002-2001.

Consta, entre otros, de los siguientes componentes;

- Microprocesador (CPU)
- Unidad de Gestión de la Memoria (MMU)
- Diferentes clases de memoria
- Seguridad lógica
- Timer
- Interfaz de entrada/salida controlado por interrupciones
- Generador de número aleatorio (RNG)
- Módulo CRC (checksum)
- Unidad criptográfica (ACE)

Incluye también la criptolibrería RSA2048 cryptolibrary y los componentes firmware RMS y STS.

2.1 Ciclo de vida del TOE

Esta declaración de seguridad define como TOE una tarjeta inteligente apta para su uso por usuarios finales, lo que en terminología CC-JIL incluye desde las fases 1 - desarrollo del software embebido - hasta la fase 7 - uso final.

La correspondencia de estas fases con lo indicado en [1] se muestra en la tabla siguiente:

CC-JIL	Perfil de Protección CWA 14169
Fase 1: desarrollo de software embebido	Diseño
Fase 2: desarrollo del circuito integrado	
Fase 3: fabricación del circuito integrado y pruebas	Fabricación
Fase 4: empaquetado y pruebas del circuito integrado	
Fase 5: finalización del producto	
Fase 6: personalización	Personalización
Fase 7: uso del producto	Uso
	Destrucción

Tabla 1.- Ciclo de vida del TOE

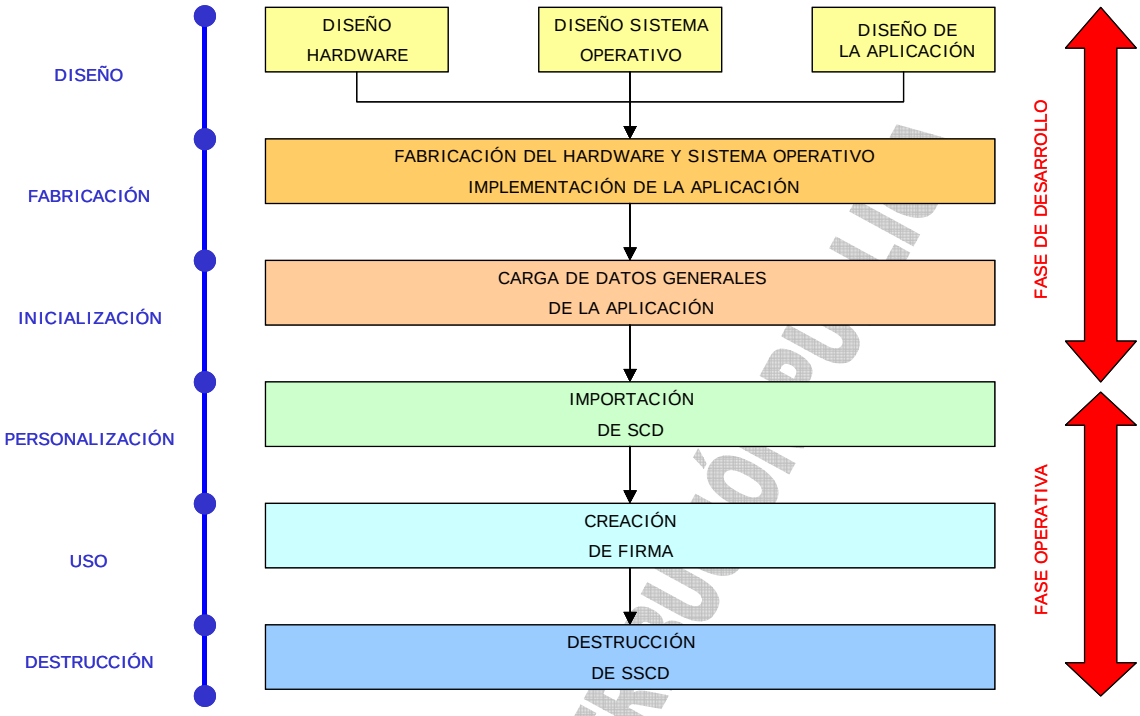

Figura 1.- Ciclo de vida conforme a CWA 14169

3. ENTORNO DE SEGURIDAD

3.1 Activos, usuarios y atacantes

Véase [1].

3.2 Hipótesis.

Véase [1].

3.3 Amenazas a los activos del producto.

Véase [1].

3.4 Políticas de seguridad.

Véase [1].

4. OBJETIVOS DE SEGURIDAD

4.1 Objetivos de seguridad aplicables al producto.

Véase [1].

4.2 Objetivos de seguridad aplicables al entorno.

Véase [1].

5. REQUISITOS DE SEGURIDAD

5.1 Requisitos funcionales de seguridad aplicables al producto

5.1.1 Soporte Criptográfico (FCS)

5.1.1.1 Generación de claves criptográficas (FCS_CKM.1)

FCS_CKM.1.1 La TSF debe generar las claves criptográficas de acuerdo con el algoritmo de generación de claves criptográficas especificado [**rsagen1**][1] ([10]) y con un tamaño de claves criptográficas especificado [**de 768 a 1984 bits**] que cumpla lo siguiente: [**requisitos de generación de número aleatorio trueran**] ([10])

5.1.1.2 Destrucción de claves criptográficas (FCS_CKM.4)

FCS_CKM.4.1 La TSF debe destruir las claves criptográficas en caso de regeneración de un nuevo SCD, de acuerdo con un método de destrucción de claves criptográficas especificado [**sobrescribir las claves con el valor 0**] que cumpla lo siguiente: [**ningún requisito especial**].

5.1.1.3 Operación criptográfica (FCS_COP.1)

FCS_COP.1.1/CORRESP La TSF debe realizar **verificación de la correspondencia SCD/SVD** de acuerdo con un algoritmo criptográfico especificado [**RSA**], con los tamaños de claves criptográficas [**de 768 a 1984 bits**] que cumplan lo siguiente: [**PKCS#1**] ([6])

FCS_COP.1.1/SIGNING La TSF debe realizar **la generación de firma digital** de acuerdo con un algoritmo criptográfico especificado [**RSA**] y con los tamaños de claves criptográficas [**de 768 a 1984 bits**] que cumplan lo siguiente: [**PKCS#1, función hash; sha1, método de padding; emsa-pkcs1-v.5**]([10],[6])

[1] Las operaciones de asignación se representan en color azul, las de sustitución en rojo y las de refinamiento en verde.

5.1.2 Protección de datos de usuario (FDP)

5.1.2.1 Subconjunto de control de acceso (FDP_ACC.1)

Véase [1].

5.1.2.2 Control de acceso basado en atributos de seguridad (FDP_ACF.1)

Véase [1].

5.1.2.3 Exportación de datos de usuario sin atributos de seguridad (FDP_ETC.1)

Véase [1].

5.1.2.4 Importación de datos de usuario sin atributos de seguridad (FDP_ITC.1)

Véase [1].

5.1.2.5 Protección de la información residual (FDP_RIP.1)

Véase [1].

5.1.2.6 Acción y supervisión de la integridad de los datos almacenados (FDP_SDI.2)

Véase [1].

5.1.2.7 Integridad en el intercambio de datos (FDP_UIT.1)

Véase [1].

5.1.3 Identificación y autenticación (FIA)

5.1.3.1 Manejo de fallos de autenticación (FIA_AFL.1)

FIA_AFL.1.1 La TSF debe detectar cuándo ocurren [**tres**] intentos de autenticación infructuosos con relación a **intentos consecutivos de autenticación fallidos**.

FIA_AFL.1.2 Véase [1].

5.1.3.2 Definición de atributos de usuario (FIA_ATD.1)

Véase [1].

5.1.3.3 Secuencia de autenticación (FIA_UAU.1)

Véase [1].

5.1.3.4 Secuencia de identificación (FIA_UID.1)

Véase [1].

5.1.4 Gestión de la seguridad (FMT)

5.1.4.1 Gestión del comportamiento de las funciones de seguridad (FMT_MOF.1)

Véase [1].

5.1.4.2 Gestión de los atributos de seguridad (FMT_MSA.1)

FMT_MSA.1.1/Administrador El TSF debe aplicar la **SFP de inicialización** para restringir la capacidad de [**modificar**] [**ninguna otra operación**] los atributos de seguridad **gestión de SCD/SVD** al **administrador**.

FMT_MSA.1.2/Signatario Véase [1].

5.1.4.3 Atributos de seguridad seguros (FMT_MSA.2)

Véase [1].

5.1.4.4 Inicialización de atributos estáticos (FMT_MSA.3)

Véase [1].

5.1.4.5 Gestión de datos de TSF (FMT_MTD.1)

FMT_MTD.1.1 La TSF debe restringir la capacidad de [**modificar**] [**ninguna otra operación**] los **RAD** al **signatario**.

5.1.4.6 Especificación de las Funciones de Gestión (FMT_SMF.1)

FMT_SMF.1.1/PREPERSO El TSF debe ser capaz de llevar a cabo las siguientes funciones de gestión de la seguridad: [

a) **Actualización de claves**;

b) **Actualización de datos**;]

FMT_SMF.1.1/PERSO El TSF debe ser capaz de llevar a cabo las siguientes funciones de gestión de la seguridad: [

a) **Actualización de claves**;

b) **Actualización de datos**;

c) **Creación de fichero maestro**;

d) **Creación de aplicación de firma** según PER.]

FMT_SMF.1.1/ADMINUSER El TSF debe ser capaz de llevar a cabo las siguientes funciones de gestión de la seguridad: [

a) **Actualización Binaria**;

b) **Autenticación Mutua**;

c) **Bloqueo/Desbloqueo de aplicación**

d) **Borrado binario**

e) **Cambio / Desbloqueo de PIN**;

f) **Establecer Entorno de Seguridad**;

g) **Generación de clave**;

h) **Lectura Binaria**;

i) **Petición de número aleatorio**;

j) **Realizar Operación de Seguridad**;

k) **Selección fichero (sobre fichero de aplicación)**;

l) **Selección fichero (sobre fichero binario)**;

m) **Verificación de PIN**;]

5.1.4.7 Roles de seguridad (FMT_SMR.1)

Véase [1].

5.1.5 Protección de la TSF (FPT)

5.1.5.1 Pruebas de la máquina abstracta (FPT_AMT.1)

FPT_AMT.1.1 La TSF debe ejecutar una colección de pruebas [**durante el arranque inicial**] para demostrar el correcto funcionamiento de las hipótesis de seguridad dadas por la máquina abstracta subyacente a la TSF.
[**La aleatoriedad de los números aleatorios generados por el chip se chequea cada vez que se genera un nuevo par SCD/SVD**]

5.1.5.2 Emisiones del TOE (FPT_EMSEC.1)[2]

FPT_EMSEC.1.1 El TOE no debe emitir [**ningún tipo de campo electromagnético**] por encima de [**valores que permitan deducir claves secretas**] permitiendo el acceso a **RAD** y **SCD**.

FTP_EMSEC.1.2 El TSF asegura que [**cualquier usuario**] sea incapaz de usar las siguientes interfaces [**cualquier interfaz**] para obtener acceso a **RAD** y **SCD**.

[2] Requisito funcional extendido a la parte 2 de las especificaciones Common Criteria [9]a

5.1.5.3 Fallo con preservación del estado seguro (FPT_FLS.1)

FPT_FLS.1.1 El TSF debe preservar un estado seguro cuando los siguientes tipos de fallos ocurren [**ataques al protocolo de comunicaciones, alteraciones de la alimentación VCC**]

5.1.5.4 Detección pasiva de ataques físicos (FPT_PHP.1)

Véase [1].

5.1.5.5 Resistencia al ataque físico (FPT_PHP.3)

FPT_PHP.3.1 EL TSF debe resistir [**cambios del entorno operacional, ataques físicos**] a [**la señal de reloj, VCC, capas de circuito integrado, RNG y shield**] ([11]) respondiendo de forma automática de manera que la TSP no sea transgredida.

5.1.5.6 Pruebas de TSF (FPT_TST.1)

FPT_TST.1.1 El TSF debe realizar una serie de auto-tests [**en el arranque inicial,** [**en ningún otro caso**]] para demostrar la correcta operatividad del TSF.

FPT_TST.1.2 Véase [1].

FPT_TST.1.3 Véase [1].

5.1.6 Ruta/canales seguros (FTP)

5.1.6.1 Canales seguros Inter-TSF (FTP_ITC.1)

FTP_ITC.1.1/SVD TRANSFER Véase [1].

FTP_ITC.1.2/SVD TRANSFER El TSF permitirá a [**un producto IT remoto seguro**] iniciar la comunicación por medio del canal seguro.

FTP_ITC.1.3/SVD TRANSFER Véase [1].

FTP_ITC.1.1/DTBS IMPORT Véase [1].

FTP_ITC.1.2/DTBS IMPORT Véase [1].

FTP_ITC.1.3/DTBS IMPORT Véase [1].

5.1.6.2 Ruta segura (FTP_TRP.1)

FTP_TRP.1.1 / TOE El TSF proporcionará una ruta de comunicación entre el mismo y los usuarios locales lógicamente distinto de otras rutas de comunicación y que provea identificación garantizada de sus puntos finales y protección contra modificación y difusión de los datos comunicados.

FTP_TRP.1.2 / TOE El TSF deberá permitir [**al TSF**] iniciar la comunicación por la ruta segura.

FTP_TRP.1.3 / TOE El TSF deberá requerirle uso de la ruta segura para autenticación [**autenticación inicial de usuario**][**ningún otro caso**]

5.2 Requisitos de Garantía

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

a) EAL4

b) AVA_VLA.4

c) AVA_MSU.3

5.2.1 Automatización parcial de CM (ACM_AUT.1)

Dependencias: ACM_CAP.3 Controles de Autorización.

Elementos de acción del desarrollador:

ACM_AUT.1.1D El desarrollador debe usar un sistema de CM.

ACM_AUT.1.2D El desarrollador debe proporcionar un plan de CM.

Contenido y presentación de elementos de evidencia:

ACM_AUT.1.1C El sistema de CM debe proporcionar medios automatizados, los cuales permiten llevar a cabo sobre la representación de la implementación del TOE los cambios autorizados.

ACM_AUT.1.2C El sistema de CM debe proporcionar medios automatizados para la generación del TOE.

ACM_AUT.1.3C El plan de CM debe describir las herramientas automatizadas se usan en el sistema de CM.

ACM_AUT.1.4C El plan de CM debe describir como las herramientas automatizadas se usan en el sistema de CM.

5.2.2 Soporte de generación y procedimientos de aceptación (ACM_CAP.4)

Dependencias: ALC_DVS.1 Identificación de medidas de seguridad

Elementos de acción del desarrollador:

ACM_CAP.4.1D El desarrollador debe proporcionar una referencia para el TOE.

ACM_CAP.4.2D El desarrollador debe usar un sistema de CM.

ACM_CAP.4.3D El desarrollador debe proporcionar documentación de CM.

Contenido y presentación de elementos de evidencia:

ACM_CAP.4.1C La referencia para el TOE debe ser única para cada versión del TOE.

ACM_CAP.4.2C El TOE debe estar etiquetado con su referencia.

ACM_CAP.4.3C La documentación del CM debe incluir una lista de configuración, un plan de CM y un plan de aceptación.

ACM_CAP.4.4C La lista de configuración debe identificar de forma unívoca todos los elementos de configuración que constituyen al TOE.

ACM_CAP.5.4C La lista de configuración debe describir los elementos de configuración que constituyen el TOE.

ACM_CAP.4.6C La documentación de CM debe describir el método usado para identificar de forma unívoca todos los elementos de configuración que constituyen al TOE.

ACM_CAP.4.7C El sistema de CM debe identificar de forma unívoca todos los elementos de configuración que constituyen el TOE.

ACM_CAP.4.8C El plan de CM debe describir como se usa el sistema de CM.

ACM_CAP.4.9C Debe ser evidente que el sistema de CM es operativo de acuerdo con el plan de CM.

ACM_CAP.4.10C La documentación de CM debe proporcionar evidencias de que todos los elementos de configuración han sido y son mantenidos de forma efectiva por el sistema de CM.

ACM_CAP.4.11C El sistema de CM debe proporcionar medios tales que los elementos de configuración sólo sufren los cambios autorizados.

ACM_CAP.4.12C El sistema de CM debe soportar la generación del TOE.

ACM_CAP.4.13C El plan de aceptación debe describir los procedimientos usados para aceptar como parte del TOE elementos de configuración modificados a creados nuevos.

5.2.3 Cobertura de CM de seguimiento de problemas (ACM_SCP.2)

Dependencias: ACM_CAP.3 Controles de Autorización

Elementos de acción del desarrollador:

ACM_SCP.2.1D El desarrollador debe proporcionar una lista elementos de configuración para el TOE.

ACM_SCP.2.1C La lista de elementos de configuración debe incluir lo siguiente: representación de la implementación, flujos de seguridad y evidencia de evaluación requerida por los componentes de garantía en la Declaración de Seguridad.

5.2.4 Detección de modificaciones (ADO_DEL.2)

Dependencias: ACM_CAP.3 Controles de Autorización.

Elementos de acción del desarrollador:

ADO_DEL.2.1D El desarrollador debe documentar procedimientos para la entrega del TOE o partes del mismo para el usuario.

ADO_DEL.2.2D El desarrollador debe usar los procedimientos de entrega.

Contenido y presentación de elementos de evidencia:

ADO_DEL.2.1C La documentación de entrega debe describir todos los procedimientos que son necesarios para mantener la seguridad durante la distribución de versiones del TOE al usuario.

ADO_DEL.2.2C La documentación de entrega debe describir como los distintos procedimientos y medidas técnicas proporcionadas para la detección de modificaciones, o cualquier discrepancia entre la copia maestra del desarrollador y la versión recibida por el usuario.

ADO_DEL.2.3C La documentación de entrega debe describir los distintos procedimientos permiten la detección de intentos de realizar un enmascarado como el desarrollador, incluso en los casos en los que éste no ha enviado nada al usuario.

5.2.5 Instalación, generación, y procedimientos de arranque (ADO_IGS.1)

Dependencias: AGD_ADM.1 Controles de Autorización.

Elementos de acción del desarrollador:

ADO_IGS.1.1D El desarrollador debe documentar los procedimientos necesarios para la instalación, generación y arranque seguros del TOE.

Contenido y presentación de elementos de evidencia:

ADO_IGS.1.1C La documentación de instalación, generación y arranque debe describir todos los pasos necesarios para la instalación, generación y arranque seguros del TOE.

5.2.6 Interfaces externas totalmente definidos (ADV_FSP.2)

Dependencias: AGD_ADM.1 Controles de Autorización.

Elementos de acción del desarrollador:

ADV_FSP.2.1D El desarrollador debe proporcionar especificaciones funcionales.

Contenido y presentación de elementos de evidencia:

ADV_FSP.2.1C Las especificaciones funcionales deberán proporcionar el TSF y sus interfaces externas usando un estilo informal.

ADV_FSP.2.2C Las especificaciones funcionales deben ser internamente coherentes.

ADV_FSP.2.3C Las especificaciones funcionales deben describir el propósito y método de uso de todas las interfaces externas del TSF, proporcionando detalles completos de todos los efectos, excepciones y mensajes de error.

ADV_FSP.2.4C Las especificaciones funcionales representarán de forma completa el TSF.

ADV_FSP.2.5C Las especificaciones funcionales deben incluir justificación de que el TSF está totalmente representado.

5.2.7 Diseño de alto nivel para la imposición de seguridad (ADV_HLD.2)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales.

ADV_RCR.1 Demostración de correspondencia informal.

Elementos de acción del desarrollador:

ADV_HLD.2.1D El desarrollador debe proporcionar el diseño de alto nivel del TSF.

Contenido y presentación de elementos de evidencia:

ADV_HLD.2.1C La presentación del diseño de alto nivel debe ser informal.

ADV_HLD.2.2C El diseño de alto nivel debe ser internamente consistente.

ADV_HLD.2.3C El diseño de alto nivel debe describir la estructura del TSF en términos de subsistemas.

ADV_HLD.2.4C El diseño de alto nivel debe describir las funcionalidades de seguridad proporcionada por cada uno de los subsistemas del TSF.

ADV_HLD.2.5C El diseño de alto nivel debe identificar cualquier hardware, firmware y/o software subyacente requeridos por el TSF con una presentación de las funciones proporcionadas por los mecanismos de soporte de la protección implementados por esos hardware, firmware y/o software.

ADV_HDL.2.6C El diseño de alto nivel debe identificar todas las interfaces de subsistema del TSF.

ADV_HLD.2.7C El diseño de alto nivel debe identificar que interfaces de los subsistemas son externamente visibles.

ADV_HLD.2.8C El diseño de alto nivel debe describir el propósito y método de uso de todas las interfaces de los subsistemas del TSF, proporcionando detalles de los efectos, excepciones y mensajes de error, según sea apropiado.

ADV_HLD.2.9C El diseño de alto nivel debe describir la separación del TOE en imposiciones de la TSP y otros subsistemas.

5.2.8 Subconjunto de implementación del TSF (ADV_IMP.1)

Dependencias: ADV_LLD.1 Diseño descriptivo de bajo nivel.

ADV_RCR.1 Demostración de correspondencia informal.

ALC_TAT.1 Herramientas de desarrollo correctamente definidas

Elementos de acción del desarrollador:

ADV_IMP.1.1D El desarrollador debe proporcionar una representación de la implementación para un subconjunto seleccionado del TSF.

Contenido y presentación de elementos de evidencia:

ADV_IMP.1C La representación de la implementación debe definir sin ambigüedades el TSF con un nivel de detalle tal que el TSF puede ser generado sin más decisiones sobre el diseño.

ADV_IMP.2C La representación de la implementación debe ser internamente consistente.

5.2.9 Diseño de bajo nivel descriptivo (ADV_LLD.1)

Dependencias: ADV_HLD.2 Imposiciones de seguridad del diseño de alto nivel.

ADV_RCR.1 Demostración de correspondencia informal.

Elementos de acción del desarrollador:

ADV_LLD.1.1D El desarrollador debe proporcionar el diseño de bajo nivel del TSF.

Contenido y presentación de elementos de evidencia:

ADV_LLD.1.1C La presentación del diseño de bajo nivel debe ser informal.

ADV_LLD.1.2C El diseño de bajo nivel debe ser internamente consistente.

ADV_LLD.1.3C El diseño de bajo nivel debe describir el diseño de bajo nivel en términos de módulos.

ADV_LLD.1.4C El diseño de bajo nivel debe describir el propósito de cada módulo.

ADV_LLD.1.5C El diseño de bajo nivel debe definir las interrelaciones entre los módulos en términos de funcionalidades de seguridad proporcionadas en otros módulos.

ADV_LLD.1.6C El diseño de bajo nivel debe describir como se proporciona cada función impuesta por la TSP.

ADV_LLD.1.7C El diseño de bajo nivel debe identificar todas las interfaces de los módulos del TSF.

ADV_LLD.1.8C El diseño de bajo nivel debe identificar que interfaces de los módulos de TSF son visibles externamente.

ADV_LLD.1.9C El diseño de bajo nivel debe describir el propósito y método de uso de todas las interfaces de módulo del TSF, proporcionando detalles de los efectos, excepciones y mensajes de error de forma apropiada.

ADV_LLD.1.10C El diseño de bajo nivel debe describir la separación del TOE en impuesto por TSP y otros módulos.

5.2.10 Demostración informal de la correspondencia (ADV_RCR.1)

Dependencias: sin dependencias.

Elementos de acción del desarrollador:

ADV_RCR.1.1D El desarrollador debe proporcionar un análisis de correspondencia entre todos los pares adyacentes de representaciones del TSF proporcionadas.

Contenido y presentación de elementos de evidencia:

ADV_RCR.1.1C Para cada de los pares adyacentes de representaciones del TSF proporcionadas, el análisis debe demostrar que todas las funciones de seguridad de la representación más abstracta del TSF esta correcta y completamente refinada en la representación del TSF menos abstracta.

5.2.11 Modelo informal de política de seguridad del TOE (ADV_SPM.1)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales

Elementos de acción del desarrollador:

ADV_SPM.1.1D El desarrollador debe proporcionar un modelo de TSP.

ADV_SPM.1.2D El desarrollador debe demostrar correspondencia entre las especificaciones funcionales y el modelo TSP.

Contenido y presentación de elementos de evidencia:

ADV_SPM.1.1C El modelo de TSP debe ser informal.

ADV_SPM.1.2C El modelo de TSP debe describir las normas y características de la TSP que pueden mostrarse por medio de modelos.

ADV_SPM.1.3C El modelo de TSP debe incluir una justificación razonada que demuestre que es consistente y completa con respecto a todas las políticas de la TSP que pueden mostrarse por medio de modelos.

ADV_SPM.1.4C La demostración de la correspondencia entre el modelo de TSP y las especificaciones funcionales debe mostrar que todas las funciones de seguridad de las especificaciones funcionales son completas y consistentes con respecto al modelo TSP.

5.2.12 Guía del administrador (AGD_ADM.1)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales

Elementos de acción del desarrollador:

AGD_ADM.1.1D El desarrollador debe proporcionar una guía para el administrador dirigida al personal de administración del sistema.

Contenido y presentación de elementos de evidencia:

AGD_ADM.1.1C La guía de administración debe describir las funciones del administrador y las interfaces disponibles para el administrador del TOE.

AGD_ADM.1.2C La guía del administrador debe describir como administrar el TOE de forma segura.

AGD_ADM.1.3C La guía del administrador debe contener avisos acerca de funciones y privilegios que deben ser controlados en un entorno seguro de procesamiento.

AGD_ADM.1.4C La guía del administrador debe describir todos los supuestos relativos al comportamiento del usuario relevantes para la operación segura con el TOE.

AGD_ADM.1.5C La guía del administrador debe describir todos los parámetros de seguridad bajo el control del administrador, indicando los valores seguros apropiados.

AGD_ADM.1.6C La guía del administrador debe describir cada tipo de evento relevante en cuanto a la seguridad relativo a las funciones administrativas que necesitan ser ejecutadas, incluyendo cambios en las características de seguridad bajo el control del TSF.

AGD_ADM.1.7C La guía del administrador debe ser consistente con toda la otra documentación remitida para su evaluación.

AGD_ADM.1.8C La guía del administrador debe describir todos los requisitos de seguridad para el entorno de IT relevantes para el administrador.

5.2.13 Guía de Usuario (AGD_USR.1)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales

Elementos de acción del desarrollador:

AGD_USR.1.1D El desarrollador debe proporcionar una guía de usuario.

Contenido y presentación de elementos de evidencia:

AGD_USR.1.1C La guía de usuario debe describir las funciones e interfaces disponibles a los usuarios no administrativos del TOE.

AGD_USR.1.2C La guía de usuario debe describir el uso de las funciones de seguridad proporcionadas por el TOE accesibles al usuario.

AGD_USR.1.3C La guía de usuario debe contener avisos acerca de funciones accesibles al usuario y privilegios que deben ser controlados en un entorno de procesamiento seguro.

AGD_USR.1.4C La guía de usuario debe presentar de forma clara todas las responsabilidades del usuario necesarias para operar de forma segura con el TOE, incluyendo aquellos supuestos relativos al comportamiento del usuario reflejados en la descripción del entorno de seguridad del TOE.

AGD_USR.1.5C La guía de usuario debe ser consistente con el resto de la documentación remitida para su evaluación.

AGD_USR.1.6C La guía de usuario debe describir todos los requisitos del entorno de IT que son relevantes para el usuario.

5.2.14 Identificación de las medidas de seguridad (ALC_DVS.1)

Dependencias: No tiene dependencias

Elementos de acción del desarrollador:

ALC_DVS.1.1D El desarrollador debe producir documentación de seguridad del desarrollo.

Contenido y presentación de elementos de evidencia:

ALC_DVS.1.1C La documentación de seguridad del desarrollo debe describir todas las medidas de seguridad físicas, de procedimiento, de personal, y otras que son necesarias para proteger la confidencialidad e integridad del diseño e implementación del TOE en su entorno de desarrollo.

ALC_DVS.1.2C La documentación de seguridad del desarrollo debe proporcionar evidencias de que las medidas de seguridad se siguen durante el desarrollo y mantenimiento del TOE.

5.2.15 Modelo del ciclo de vida definido por el desarrollador (ALC_LCD.1)

Dependencias: No tiene dependencias

Elementos de acción del desarrollador:

ALC_LCD.1.1D El desarrollador debe establecer un modelo de ciclo de vida para usar en el desarrollo y mantenimiento del TOE.

ALC_LCD.1.2D El desarrollador debe proporcionar documentación de definición del ciclo de vida.

Contenido y presentación de elementos de evidencia:

ALC_LCD.1.1C La definición del ciclo de vida debe describir el modelo usado para desarrollar y mantener el TOE.

ALC_LCD.1.2C El modelo del ciclo de vida debe mantener el control necesario sobre el desarrollo y mantenimiento del TOE.

5.2.16 Herramientas de desarrollo bien definidas (ALC_TAT.1)

Dependencias: ADV_IMP.1 Subconjunto de implementación del TSF.

Elementos de acción del desarrollador:

ALC_TAT.1.1D El desarrollador debe identificar las herramientas de desarrollo usadas para el TOE.

ALC_TAT.1.2D El desarrollador debe documentar las opciones de las herramientas de desarrollo dependientes de la implementación escogidas.

Contenido y presentación de elementos de evidencia:

ALC_TAT.1.1C Todas las herramientas de desarrollo usadas para la implementación deben estar bien definidas.

ALC_TAT.1.2C La documentación de las herramientas de desarrollo debe definir sin ambigüedades el significado de todas las sentencias usadas en la implementación.

ALC_TAT.1.3C La documentación de las herramientas de desarrollo debe definir sin ambigüedades el significado de todas las opciones dependientes de la implementación.

5.2.17 Análisis de la cobertura (ATE_COV.2)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales.

ATE_FUN.1 Pruebas funcionales.

Elementos de acción del desarrollador:

ATE_COV.2.1D El desarrollador debe proporcionar un análisis de la cobertura de las pruebas.

ATE_COV.2.1C El análisis de la cobertura de las pruebas debe demostrar la correspondencia entre las pruebas identificadas en la documentación de pruebas y el TSF como se describe en las especificaciones funcionales.

ATE_COV.2.2C El análisis de la cobertura de las pruebas debe demostrar que la correspondencia entre el TSF como se describe en las especificaciones funcionales y las pruebas identificadas en la documentación de pruebas es completa.

5.2.18 Pruebas: diseño de alto nivel (ATE_DPT.1)

Dependencias: ADV_HLD.1 Descripción de diseño de alto nivel.

ATE_FUN.1 Pruebas funcionales.

Elementos de acción del desarrollador:

ATE_DPT.1.1D El desarrollador debe proporcionar el análisis de la profundidad de las pruebas.

Contenido y presentación de elementos de evidencia:

ATE_DPT.1.1C El análisis de profundidad debe demostrar que las pruebas identificadas en la documentación de pruebas son suficientes para demostrar que el TSF opera en concordancia con el diseño de alto nivel.

5.2.19 Pruebas funcionales (ATE_FUN.1)

Dependencias: No tiene dependencias.

Elementos de acción del desarrollador:

ATE_FUN.1.1D El desarrollador debe realizar pruebas sobre el TSF y documentará los resultados.

ATE_FUN.1.2D El desarrollador debe proporcionar la documentación de las pruebas.

Contenido y presentación de elementos de evidencia:

ATE_FUN.1.1C La documentación de pruebas debe consistir en planes de pruebas, descripción de procedimientos de prueba, resultados esperados y resultados obtenidos en las pruebas.

ATE_FUN.1.2C Los planes de pruebas deben identificar las funciones de seguridad para ser probadas y describir el objetivo de las pruebas a realizar.

ATE_FUN.1.3C La descripción de los procedimientos de prueba debe identificar las pruebas que deben realizarse y describirán los escenarios para probar cada función de seguridad. Estos escenarios incluirán cualquier relación de dependencia de los resultados de otras pruebas.

ATE_FUN.1.4C Los resultados de las pruebas deben mostrar las salidas anticipadas de una ejecución exitosa de las pruebas.

ATE_FUN.1.5C Los resultados de las pruebas de la ejecución realizada de estas por parte del desarrollador deben demostrar que cada función de seguridad probada se comporta como se esperaba.

5.2.20 Pruebas independientes – ejemplo (ATE_IND.2)

Dependencias: ADV_FSP.1 Especificaciones funcionales informales.

AGD_ADM.1 Guía del administrador.

AGD_USR.1 Guía del usuario.

ATE_FUN.1 Pruebas funcionales.

Elementos de acción del desarrollador:

ATE_IND.2.1D El desarrollador proporcionará el TOE para pruebas.

Contenido y presentación de elementos de evidencia:

ATE_IND.2.1C El TOE debe estar adaptado para las pruebas.

ATE_IND.2.2C El desarrollador debe proporcionar un conjunto de recursos equivalente a aquellos que fueron usados en las pruebas funcionales del desarrollador sobre el TSF.

5.2.21 Análisis y pruebas sobre los estados inseguros (AVA_MSU.3)

Dependencias: ADO_IGS.1 Procedimientos de instalación, generación y arranque.

ADV_FSP.1 Especificaciones Funcionales Informales.

AGD_ADM.1 Guía del administrador.

AGD_USR.1 Pruebas funcionales.

Elementos de acción del desarrollador:

AVA_MSU.3.1D El desarrollador debe proporcionar documentación de guía.

AVA_MSU.3.2D El desarrollador debe documentar un análisis de la documentación de guía.

Contenido y presentación de elementos de evidencia:

AVA_MSU.3.1C La documentación de guía debe identificar todos los posibles modos de operación del TOE (incluyendo seguimiento de errores en operaciones o errores operacionales), sus consecuencias e implicaciones para el mantenimiento de la seguridad en las operaciones.

AVA_MSU.3.2C La documentación de guía debe ser completa, clara, consistente y razonada.

AVA_MSU.3.3C La documentación de guía debe listar todos los supuestos acerca del entorno esperado.

AVA_MSU.3.4C La documentación de guía debe listar todos los requisitos para medidas de seguridad externa (incluyendo procedimientos eternos, físicos y controles de personal)

AVA_MSU.3.5C La documentación de análisis debe demostrar que la documentación de guía es completa.

5.2.22 Evaluación de la fortaleza de las funciones de seguridad del TOE (AVA_SOF.1)

Dependencias: ADV_FSP.1 Especificaciones Funcionales Informales.

ADV_HLD.1 Descripción Diseño de Alto Nivel.

Elementos de acción del desarrollador:

AVA_SOF.1.1D El desarrollador debe realizar un análisis de la fortaleza de las funciones de seguridad para cada mecanismo identificado en la ST que afirma tener una fortaleza como función de seguridad del TOE.

Contenido y presentación de elementos de evidencia:

AVA_SOF.1.1C Para cada mecanismo que afirma tener fortaleza como función de seguridad del TOE el análisis de la fortaleza de función de seguridad del TOE debe mostrar que reúne o excede la medida de fortaleza especifica definida en el PP/ST.

AVA_SOF.1.2C Para cada mecanismo con una afirma tener una fortaleza específica como función de seguridad del TOE, el análisis de la fortaleza de las funciones de seguridad del TOE debe mostrar si reúne o supera la medida de fortaleza especifica definida en el PP/ST.

5.2.23 Alta resistencia (AVA_VLA.4)

Dependencias: ADV_FSP.1 Especificaciones Funcionales Informales.

ADV_HLD.2 Descripción Diseño de Alto Nivel.

ADV_IMP.1 Subconjunto de implementación del TSF

ADV_LLD.1 Descripción de diseño de bajo nivel

AGD_ADM.1 Guía de administrador

AGD_USR.1 Guía de usuario

Elementos de acción del desarrollador:

AVA_VLA.4.1D El desarrollador debe realizar un análisis de vulnerabilidades.

AVA_VLA.4.2D El desarrollador debe proporcionar documentación del análisis de vulnerabilidades.

Contenido y presentación de elementos de evidencia:

AVA_VLA.4.1C La documentación del análisis de vulnerabilidades debe describir el análisis de las distribuciones del TOE llevados a cabo par buscar caminos en los que un usuario puede violar la TSP.

AVA_VLA.4.2C La documentación del análisis de vulnerabilidades debe describir la disposición de las vulnerabilidades identificadas.

AVA_VLA.4.3C La documentación del análisis de vulnerabilidades debe demostrar, para todas las vulnerabilidades identificadas, que las vulnerabilidades no pueden ser explotadas en el entorno al que está destinado el TOE.

AVA_VLA.4.4C La documentación del análisis de vulnerabilidades debe justificar que el TOE, con las vulnerabilidades identificadas, es resistente a los ataques de penetración obvios.

AVA_VLA.4.5C La documentación del análisis de vulnerabilidades debe mostrar que la búsqueda de vulnerabilidades es sistemática.

AVA_VLA.4.6C La documentación del análisis de vulnerabilidades debe proporcionar una justificación de que el análisis está completamente dirigido a TOEs dispuestos a su distribución.

5.3 Requisitos funcionales de seguridad aplicables al entorno

5.3.1 Requisitos de seguridad aplicables al entorno de las TI.

5.3.1.1 Aplicación de generación de certificados

5.3.1.1.1 FCS_CKM.2 Distribución de claves criptográficas

FCS_CKM.2.1/CGA La TSF debe distribuir las claves criptográficas de acuerdo con un método de distribución de claves criptográficas especificado ***certificado cualificado*** que cumple lo siguiente [**PKCS#10**][6]

5.3.1.1.2 FCS_CKM.3 Acceso de clave criptográfica

FCS_CKM.3.1/CGA El TSF debe realizar la ***importación de SVD*** de acuerdo con el método de acceso a las claves criptográficas ***importación a través de un canal seguro*** que cumple lo siguiente [**MAC reforzado con padding tipo 2 y cifrado DES ECB**](véase §[5][**según los comandos y API definidos por APP y CMD**]).

5.3.1.1.3 Integridad en el intercambio de datos (FDP_UIT.1)

Véase [1].

5.3.1.1.4 Canal seguro inter-TSF (FTP_ITC.1)

FTP_ITC.1.1/SVD Import El TSF debe proporcionar un canal de comunicación entre el mismo y un producto de IT remoto lógicamente distinto de otros canales de comunicación y proporcionar garantía de identificación en sus puntos finales y protección de los datos del canal de modificación o revelación de datos.

FTP_ITC.1.2/SVD Import EL TSF debe permitir [**al producto IT seguro remoto**] iniciar la comunicación vía canal seguro.

FTP_ITC.1.3/SVD Import EL TSF o el TOE debe iniciar la comunicación vía canal seguro para la ***importación de SVD.***

5.3.1.2 Aplicación de creación de firma

5.3.1.2.1 FCS_COP.1 Operación criptográfica

FCS_COP.1.1/SCA_HASH El TSF debe criptográfico específico realizar el **cálculo del hash de los DTBS** de acuerdo a un algoritmo [**sha1**] y con ***no aplica*** tamaño de claves criptográficas que cumpla lo siguiente [**FIPS PUB 180-2**].

5.3.1.2.2 Integridad en el intercambio de datos (FDP_UIT.1)

Véase [1].

5.3.1.2.3 Canal seguro inter-TSF (FTP_ITC.1)

Véase [1].

5.3.1.2.4 Ruta segura (FTP_TRP.1)

La ruta segura entre el TOE y la SCA será requerida sólo si el interfaz humano para la autenticación de usuario no está proporcionada por el TOE sino por la SCA.

FTP_TRP.1.1/SCA El TSF proporcionará una ruta de comunicación entre el mismo y los usuarios locales lógicamente distinto de otras rutas de comunicación y que provea identificación garantizada de sus puntos finales y protección contra modificación y difusión de los datos comunicados.

FTP_TRP.1.2/SCA El TSF deberá permitir [**al TSF**] iniciar la comunicación por la ruta segura.

FTP_TRP.1.3/SCA El TSF deberá requerirle uso de la ruta segura para autenticación [**autenticación inicial de usuario**][**ningún otro caso**].

5.4 Requisitos de seguridad aplicables al entorno ajeno a las IT

Véase [1], apartado 5.4 “Security Requirements for the Non IT environment”.

6. SÍNTESIS DE LA ESPECIFICACIÓN DEL PRODUCTO

6.1 Especificación funcional

CMD TI317 Manual de Usuario Advantis Crypto V.3.1.

PER TI348, Personalización de la Aplicación de Firma Digital, v.1.2

APP TI349, Manual de Diseño de la Aplicación de Firma, v.2.0

ST SECURITY TARGET

El manual CMD es la especificación técnica y descripción funcional del Sistema Operativo Advantis Crypto, en su versión evaluada. Dicho manual describe el interfaz funcional a nivel de aplicación de la tarjeta.

El documento PER concreta la personalización de la aplicación de firma objeto de la evaluación, personalización que deberá ser implementada estrictamente en todas las configuraciones de la tarjeta Advantis cuya aplicación de firma pretenda utilizar la condición de producto certificado al amparo de esta declaración de seguridad y su posterior evaluación y certificación.

Por último, la funcionalidad y detalles de implementación de la aplicación de firma se detallan en el manual APP, que se basa en los dos anteriores.

Se relacionan en este apartado los requisitos funcionales de la declaración de seguridad con los comandos o funciones que, conforme se detallan en APP, dan cumplimiento a los mismos.

Dicho manual de usuario, APP, es la especificación funcional de los interfaces de la aplicación de firma de la tarjeta Advantis Crypto. Conforme al párrafo 228 de la primera parte de la norma CC, segunda frase, *"Note that the functional information provided as part of the TOE summary specification could be identical in some cases to the information to be provided for the TOE as part of the ADV_FSP requirements"*, no se repetirá en esta sección tal información del manual de usuario, sino que se hacen referencias los apartados aplicables del mismo.

El cumplimiento de los siguientes requisitos funcionales se garantiza por la plataforma de la tarjeta Advantis Crypto, **el chip IC**, como se detalla en su declaración de seguridad: ST:

a) **Detección pasiva de ataques físicos (FPT_PHP.1)**

b) **Resistencia al ataque físico (FPT_PHP.3)**

c) **Protección de la información residual (FDP_RIP.1)**

d) **Emisiones del TOE (FPT_EMSEC.1)**

En el caso de **Protección de la información residual (FDP_RIP.1)** se complementa con el comando

a) **Borrado de fichero binario**

Este comando garantiza la inaccesibilidad a SCD una vez que se cuando deja de utilizarse. Respecto al RAD (PIN y PUK) su acceso cuando se han bloqueado es imposible puesto que se almacenan en la cabecera de los ficheros de aplicación y no en el cuerpo de los ficheros elementales, tal y como se describe en CMD.

Fallo con preservación del estado seguro (FPT_FLS.1) no es implementado directamente por los comandos de la tarjeta, sino que se corresponde con funcionalidad interna del diseño, en particular con los mecanismos de redundancia y shield[3] incluidos en la arquitectura del **chip** por un lado y los **contadores dobles**, **mecanismo de espejo** y **checksum** descritos en CMD.

Pruebas de TSF (FPT_TST.1) tampoco se implementa con comandos de la tarjeta, sino con mecanismos de chequeo interno de las funcionalidades de la tarjeta que se describen en CMD y en la información del diseño de bajo nivel insertada en el propio código en forma de comentarios y cabeceras de funciones y ficheros.

Las capacidades requeridas en **Secuencia de autenticación (FIA_UAU.1)** y **Secuencia de identificación (FIA_UID.1)** requieren de la autenticación del usuario, conforme a los comandos

a) **Cambio/Desbloqueo de PIN (como inicialización de PIN, con presentación de PUK)**

b) **Verificación de PIN.**

El comando Verificación de PIN permite la **Gestión del Atributo SCD/SVD Management**. Dicho atributo puede tener 2 valores para el usuario: **autorizado/no autorizado**. En el momento previo a una Verificación de PIN correcta el valor del atributo es no autorizado. Cuando el usuario ejecuta correctamente el comando y verifica su identidad el valor del atributo es autorizado y puede generar las claves.

Los roles que se exigen en **Roles de seguridad (FMT_SMR.1)** se implementan por el sistema operativo mediante la conjunción de los comandos indicados para cada rol en **Especificación de las Funciones de Gestión (FMT_SMF.1)**, y la secuencia de pre-personalización y personalización requerida para la implementación de PER.

[3] El mecanismo de shield conlleva la implementación de una rutina que haga uso de dicho mecanismo según las indicaciones proporcionadas por el fabricante del chip.

Las capacidades de gestión de la seguridad requeridas por **Gestión de los atributos de seguridad (FMT_MSA.1)/ADMINISTRADOR** se gestionan con

a) Borrado de fichero binario

b) Establecer entorno de seguridad

c) Generación de claves

d) Petición e número aleatorio

e) Realizar operación de seguridad

Y con el mecanismo de **condiciones de acceso de ficheros**. En el caso de **Gestión de los atributos de seguridad (FMT_MSA.1)/SIGNATARIO** el requisito se cumple con el comando

a) Autenticación mutua

El comando Autenticación Mutua permite la **Gestión del Atributo DTBS enviados desde SCA autorizada**. Dicho atributo puede tener 2 valores: **si/no**, según los DTBS sean efectivamente enviados por una SCA autorizada o no. Si la SCA se autentica correctamente al ejecutarse el comando Autenticación Mutua el valor del atributo es **sí**, y por tanto pueden enviarse a la tarjeta los datos que se desea firmar. Si la autenticación falla el valor del atributo es **no**, el canal seguro requerido para la recepción de los datos no se abre.

El atributo **Acción y supervisión de la integridad de los datos almacenados (FDP_SDI.2)** se implementa con los siguientes mecanismos

- En el caso de SCD/SVD tenemos el de **espejo** (en la fase de escritura de los datos), **condiciones de acceso** de los ficheros (en el caso particular de los ficheros que contienen SVD y SCD la condición de acceso de escritura es siempre prohibida) y los propios mecanismos de garantía de la integridad de los datos que implementa el **chip**.

- En el caso de los DTBS que se almacenan temporalmente en RAM mientras se opera con ellos, los propios mecanismos de garantía de la integridad de los datos que implementa el **chip**.

- En el caso del RAD, además de los mecanismos proporcionados por el chip se usa el **checksum** de la cabecera de los ficheros ya que estos datos se guardan en la cabecera de los ficheros de aplicación como se expone en el CMD.

Los atributos **Manejo de fallos de autenticación (FIA_AFL.1), Definición de atributos de usuario (FIA_ATD.1)** y **Gestión de datos de TSF (FMT_MTD.1)** se implementan con los comandos

a) Verificación de PIN;

b) Cambio / Desbloqueo de PIN;

La política de control de acceso, **Control de acceso basado en atributos de seguridad (FDP_ACF.1)**, y las correspondientes funciones **Subconjunto de control de acceso (FDP_ACC.1)**, se activan implícitamente al invocar los comandos sujetos a dicha política, que son los siguientes:

a) Borrado de fichero binario;

b) Establecer entorno de seguridad;

c) Generación de clave;

d) Verificación de PIN;

El atributo de seguridad **Gestión del comportamiento de las funciones de seguridad (FMT_MOF.1)** se controla con el comando

a) Verificación de PIN;

Y el mecanismo de **condiciones de acceso**, que impone la ejecución de dicho comando como paso previo para la ejecución de la Firma Digital.

El atributo de seguridad **Inicialización de atributos estáticos (FMT_MSA.3)** se implementa con los comandos

a) Bloqueo/Desbloqueo de Aplicación

cuya ejecución permite que el SCD esté operativo o no, y con el mecanismo de seguridad de **test internos**.

El comando Bloqueo/Desbloqueo de Aplicación permite la **Gestión del Atributo SCD Operativa**. Dicho atributo puede tener 2 valores para el usuario: **sí/no** según la clave esté operativa o no. Si la aplicación está bloqueada la clave no será operativa, mientras que si está desbloqueada sí lo estará. Los citados comandos permiten el paso de uno a otro estado.

Los atributos **Canales seguros Inter-TSF (FTP_ITC.1)** y **Ruta segura (FTP_TRP.1) se implementan con el comando**

a) Autenticación mutua

El requisito criptográfico **Atributos de seguridad seguros (FMT_MSA.2)**, se satisface con los comandos

a) Autenticación mutua

b) Bloqueo/Desbloqueo de Aplicación

c) Verificación de PIN

Y el mecanismo de **condiciones de acceso.**

Generación de claves criptográficas (FCS_CKM.1) se satisface con el comando

a) Generación de claves

Destrucción de claves criptográficas (FCS_CKM.4) se satisface con el comando

a) Borrado de fichero binario

y **FCS_COP.1 Operación criptográfica**, se implementa mediante los comandos

a) Generación de claves

b) Autenticación mutua

c) Petición de número aleatorio

d) Establecer entorno de seguridad

e) Realizar operación de seguridad

f) Cambio / Desbloqueo de PIN

g) Verificación de PIN

en las variantes indicadas en APP, que igualmente incluyen la implementación de la seguridad de las comunicaciones, **Canales seguros Inter-TSF (FTP_ITC.1)**.

Exportación de datos de usuario sin atributos de seguridad (FDP_ETC.1)Importación de datos de usuario sin atributos de seguridad (FDP_ITC.1) FDP_ETC.1/SVD Transfer y **FDP_UIT.1/SVD Transfer** se cumplen con el comando

a) Generación de claves

Que da como respuesta SVD securizado con el MAC de canal seguro. Por su parte **Integridad en el intercambio de datos (FDP_UIT.1)** se cumple con el comando

a) Realizar operación de seguridad

Que fuerza a que los DTBS sean recibidos cifrados de acuerdo a PKCS#1 y securizados también con el MAC de canal seguro.

Por ultimo **Pruebas de la máquina abstracta (FPT_AMT.1)** también se cumple usando una serie de tests internos del S.O que comprueban los mecanismos de shield, DES, RSA y grado de aleatoriedad de los números aleatorios generados.

Estos mecanismos se presentan de modo somero en CMD, y su descripción detallada se encuentra en la documentación de diseño de bajo nivel.

La siguiente tabla muestra la identificación de cada función de seguridad (SFX), la agrupación de SF's por interfaz y si dicha interfaz es interna o externa.

SF's		Agrupación de SF's	Visibilidad
SF1	Actualización binaria	Interfaz APDU	Externa
SF2	Actualización de clave		
SF3	Actualización de datos		
SF4	Autenticación mutua		
SF5	Bloqueo/Desbloqueo de Aplicación		
SF6	Borrado de fichero binario		
SF7	Cambio/Desbloqueo de PIN		
SF8	Checksum cabecera de ficheros	Interfaz S.O	Interna
SF9	Circuito integrado	Interfaz chip	Externa
SF10	Condiciones de acceso de ficheros	Interfaz S.O	Interna
SF11	Creación de fichero	Interfaz APDU	Externa
SF12	Establecer Entorno de Seguridad		
SF13	Generación de claves		
SF14	Lectura binaria		
SF15	Mecanismo de contadores	Interfaz S.O	Interna
SF16	Mecanismo de espejo		
SF17	Petición de número aleatorio	Interfaz APDU	Externa
SF18	Realizar operación de seguridad		
SF19	Selección de fichero		
SF20	Tests Internos	Interfaz S.O	Interna
SF21	Verificación de PIN	Interfaz APDU	Externa

Tabla 2.- Relación SF's - interfaces

La interfaz APDU se describe en [14], libro 1, apartado 11.1.1 y es común para todas las SF's basadas en comandos de la tarjeta. Las excepciones, mensajes de error y efectos que los caracterizan se describen en CMD.

El interfaz chip reúne los mecanismos facilitados por el circuito integrado. Su descripción se encuentra en [15] En el caso del mecanismo denominado "shield", el

control del mecanismo se efectúa por medio del software del S.O y por tanto su funcionamiento se encuentra descrito en la información de diseño de bajo nivel (incluida en las cabeceras de las unidades de implementación y funciones)

El interfaz S.O reúne los mecanismos implementados por el sistema operativo que no corresponden a un comando concreto. Estos mecanismos se encuentran parcialmente descritos en el CMD, y de forma más detallada en la información de diseño de alto nivel.

6.1.1 Fortaleza de mecanismos

Los requisitos funcionales de la clase **Identificación y autenticación (FIA)** utilizan mecanismos probabilísticos o permutacionales, para los cuales es necesaria la comprobación de su fortaleza.

Nótese que en la tarjeta inteligente, la identificación es implícita a la autenticación, por cuanto se supone un dispositivo de un sólo usuario, y su posesión implica la identidad del usuario.

Los mecanismos de autenticación, son el mecanismo de PIN de 16 bytes (que agrupa las operaciones de cambio, desbloqueo y verificación de PIN) y de autenticación mutua, cuya fortaleza es alta, como resulta de la aplicación de la metodología de análisis de SOF del CEM [13].

Los requisitos funcionales de la clase **Soporte Criptográfico (FCS)** relativos a Establecer entorno de seguridad/Generación de claves también tienen nivel de fortaleza alta, aplicando el algoritmo trueran especificado en [10] Esto mismo aplica para todas las operaciones que se basan en el cálculo de un número aleatorio, como los comandos de Autenticación Mutua y Petición de Número Aleatorio.

6.1.1.1 Fortaleza de los mecanismos de PIN y PUK

Tanto el PIN como el PUK están constituidos por 16 bytes de longitud. Supongamos un caso menos favorable para la seguridad, en el que la aplicación utiliza sólo 8 de esos bytes, rellenando el resto con un padding predeterminado. Esta longitud de clave se ajusta más a las que se usan en la actualidad.

Cada unos de esos bytes puede tomar hasta 64 valores distintos (se limitan los valores a caracteres alfanuméricos: 27 letras minúsculas + 27 letras mayúsculas en teclado español + 10 números) Podemos calcular el número de posibles valores del PIN y el PUK como variaciones con repetición (puesto que los caracteres se pueden repetir pero el orden en que se introducen se tiene en cuenta) de 64 elementos tomados de 8 en 8. Esto nos da un resultado de $64^8 = 2^{48}$ posibles PINs y PUKs. Puesto que tanto uno como otro tienen una limitación en el número de presentaciones de 3, la probabilidad de acertar el dato sin conocerlo es de $3x2^{-48}$. **Este dato hace por sí mismo que no sea abordable tratar de averiguar el PIN o el PUK para atacar a la tarjeta**.

Sin contar con este mecanismo de control, el SOF de estos mecanismos sigue siendo alto. Suponemos ahora que ambas claves se puedan presentar tantas veces como se quiera. Considerando la tabla 3 del apartado A8 de [13] podemos suponer que el mecanismo de PIN y de PUK es plenamente conocido hoy en día y que no requiere ningún tiempo ni formación especial identificarlos, ni tampoco acceso al TOE.

Valor de identificación:

Elapsed Time < 0.5 horas => 0

Expertise Layman => 0

Knowledge of the TOE None => 0

Acces to TOE < 0.5 noras => 0

Equipment None => 0

Total: 0

Respecto a la explotación del mecanismo podemos suponer que se va a tratar de averiguar el PIN/PUK no introduciéndolo a mano, sino usando una serie de ordenadores trabajando en paralelo, con lo cual se necesitaría un equipamiento estándar (2) y un nivel de formación Proficient (2).

Valor de explotación (sin considerar el tiempo):

Expertise Proficient => 2

Knowledge of the TOE None => 0

Equipment Standar => 2

Pero lo que realmente marcaría el SOF es el tiempo de acceso al TOE necesario para poder averiguar las claves. El número de intentos promedio para acertar sería de $2^{48}/2=2^{47}$, el tiempo necesario para ejecutar cada operación de verificación será del orden de los milisegundos. Sería necesario usar aproximadamente 100 ordenadores durante 44 años para averiguar una de las 2 claves. Por tanto los parámetros elapsed time y Acces to TOE tendrían el valor “Not Practical”.

6.1.1.2 Mecanismo de canal seguro

El mecanismo de canal seguro tiene también SOF high. En este caso es aún más evidente. Aún suponiendo que el atacante conociese de antemano la clave que se utiliza para establecer el canal seguro, las claves de sesión se calculan a partir de 2 números aleatorios de 8 bytes generados por la tarjeta y el terminal respectivamente. Esto hace que haya un total de 2^{48} posibles claves de sesión de cifrado y de MAC. La posibilidad de acertar ambas simultáneamente es de 2^{-96}, puesto que cuando se realiza una operación errónea el canal seguro se cierra y se tienen que volver a generar las claves. Como en el caso anterior, **este dato por si sólo hace inabordable intentar averiguar las claves de sesión**. Incluso en el caso de que no hubiese limitación en el número de intentos, el hecho de tener que averiguar 2 claves simultáneamente haría que el número de intentos necesario fuese muy superior al caso del PIN y el PUK.

Además del tiempo, el resto de los parámetros contemplados en tabla 3 del apartado A8 de [13] hacen que se supere el valor que nos marca el SOF high (tabla 4 del mismo apartado)

Valor de identificación:

Elapsed Time < 1 mes => 3

Expertise Proficient => 2

Knowledge of the TOE Sensitive => 5

Acces to TOE < 1 mes => 3

Equipment Specialised => 3

Total: 16

En el caso del valor de explotación tendríamos (sin considerar el tiempo, que como hemos visto es “No Practical”)

Valor de explotación:

Expertise Proficient => 2

Knowledge of the TOE Sensitive => 5

Acces to TOE < 1 mes => 3

Equipment Specialised => 3

Total: 13

Por lo tanto, incluso sin considerar el tiempo, el valor total alcanzado es 29 y por tanto el valor del SOF del mecanismo es high.

6.2 Garantía de seguridad

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.

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

COMPONENTE	DOCUMENTO
Automatización parcial de CM (ACM_AUT.1)	Version Control with Subversion version 10061. TortoiseSVN. A Subversion client for Windows. TI390 - Manual de Usuario del Repositorio.doc TI344 – Manual de Gestión de la Configuración.
Soporte de generación y procedimientos de aceptación (ACM_CAP.4)	Version Control with Subversion version 10061. TortoiseSVN. A Subversion client for Windows. TI344 – Manual de Gestión de la Configuración. TI390 – Manual del Repositorio TI392 - Incidencias Advantis Crypto PE
Cobertura de CM de seguimiento de problemas (ACM_SCP.2)	Version Control with Subversion version 10061. TortoiseSVN. A Subversion client for Windows. TI344 – Manual de Gestión de la Configuración. TI392 – Incidencias Advantis Crypto PE
Detección de modificaciones (ADO_DEL.2)	CC SecureX Extranet Portal User Manual TI346 - Procedimiento de entrega de las tarjetas al usuario final TI404 – Lista de configuración Advantis Crypto v.3 TI405 - Envío de tarjetas de prueba a betatesters.doc TI406 - Recepción de tarjetas en Sermepa.doc
Instalación, generación, y procedimientos de arranque (ADO_IGS.1)	TI200 - Manual de Pre-personalización Advantis y Advantis Crypto TI201 - Manual de Personalización Advantis Crypto TI407 - Medidas generales de seguridad para el usuario de tarjeta Advantis Crypto como dispositivo de firma electrónica.doc
Interfaces externas totalmente definidos (ADV_FSP.2)	TI317 - Manual de Usuario Advantis Crypto V.3.1 TI338 - Interfaces de subsistema en Advantis Crypto V3.1.doc TI345 - Advantis Crypto 3.1 - Declaración de Seguridad TI348 - Personalización de la Aplicación de Firma Digital.doc
Diseño de alto nivel para la imposición de seguridad (ADV_HLD.2)	TI336 - Diseño de Alto Nivel Advantis Crypto V.3.1 TI349 - Manual de Diseño de la Aplicación de Firma.doc
Subconjunto de implementación del TSF (ADV_IMP.1)	Acceso al código fuente.
Diseño de bajo nivel descriptivo (ADV_LLD.1)	La información de diseño de bajo nivel se incluye en el código, en las cabeceras de subsistemas y funciones.

COMPONENTE	DOCUMENTO
Demostración informal de la correspondencia (ADV_RCR.1)	TI338 - Interfaces de subsistema en Advantis Crypto V.3.1 TI340 - Manual de Certificación de la Aplicación Firma Digital CWA14169
Modelo informal de política de seguridad del TOE (ADV_SPM.1)	Según se refleja en esta declaración de seguridad.
Guía del administrador (AGD_ADM.1)	TI200 - Manual de Pre-personalización Advantis y Advantis Crypto TI201 - Manual de Personalización Advantis Crypto TI348 - Personalización de la Aplicación de Firma Digital.doc
Guía de Usuario (AGD_USR.1)	TI317 - Manual de Usuario Advantis Crypto V.3.1
Identificación de las medidas de seguridad (ALC_DVS.1)	TI245 – Requisitos de Seguridad del Entorno de Desarrollo v5.3
Modelo del ciclo de vida definido por el desarrollador (ALC_LCD.1)	TI098 - Medidas de Protección anti-DPA v1.2 TI138 - Metodología de desarrollo de Sistemas Operativos para Tarjeta Inteligente v3.2 TI246 - Análisis de Vulnerabilidades en Sistemas Operativos v1.2
Herramientas de desarrollo bien definidas (ALC_TAT.1)	TI245 - Requisitos de Seguridad del Entorno de Desarrollo v5.3 SLE66CxxxPE Security Programmers Manual 2006-12 ERRATA SHEET SLE66CxxxPE 2006-11 INSTRUCTION SET SLE66CxxxPE 2004-07 SLE66CxxPE /MicroSlim Security Controller Family DATA BOOK, October 2006 CAN - SLE 66CxxxP/PE - Memory Encryption Decryption 11.2004 CAN - SLE 66CxxxP/PE - testing the RNG 11.2004 CAN - SLE 66CxxxP/PE – Security Controller Family -Using RNG a.t. FIPS140 02.2004 CAN - SLE 66CxxxPE DDES Accelerator 07.2005. CAN - Security Controller Family -Memory Managment Unit – Far Memory Access 12.2004 CAN - SLE 66CxxxPE - Optimized usage of NVM above 64k 08.2005 CAN - SLE 66CxxxPE - Security Controller Family - Security Advice 05.2004 CAN - SLE 66CxxxPE - Using MicroSlim NVM Note 05.2005 CAN - Security & Chip Card ICs - Using the Active Shield security feature 12.2004 Security & Chip Card ICs RSA 2048 bit Support SLE 66CXxxxPE. RSA Interface Specification for Library V.1.4. 2005-06 Security & Chip Card ICs RSA 2048 bit Support SLE 66CXxxxPE. RSA Arithmetic V.1.4. 2005-06 SDK CC 03.2005. Components of RM66PII V.2.0 for BondOut E21. SDK CC for SLE 66. Confidential User's Manual. March 2005. Cx51 Compiler. Optimizing C Compiler and Library Reference for Classic and Extended 8051 Microcontrollers. September 2001. TI389 – Entorno de desarrollo de Advantis Crypto 3.1

COMPONENTE	DOCUMENTO
Análisis de la cobertura (ATE_COV.2)	T340 - Manual de Certificación de la Aplicación Firma Digital CWA 14169 Escenarios de las pruebas desarrolladas en Sermepa, así como las trazas de dichas pruebas.
Pruebas: diseño de alto nivel (ATE_DPT.1)	T340 - Manual de Certificación de la Aplicación Firma Digital CWA 14169 Escenarios de las pruebas desarrolladas en Sermepa, así como las trazas de dichas pruebas.
Pruebas funcionales (ATE_FUN.1)	TI340 - Manual de Certificación de la Aplicación Firma Digital CWA14169 Escenarios de las pruebas desarrolladas en Sermepa, así como las trazas de dichas pruebas.
Pruebas independientes – ejemplo (ATE_IND.2)	Documentación entregada por el laboratorio independiente encargado de la realización de las pruebas.
Análisis y pruebas sobre los estados inseguros (AVA_MSU.3)	TI200 - Manual de Pre-personalización Advantis y Advantis Crypto TI201 - Manual de Personalización Advantis Crypto TI317 - Manual de Usuario Advantis Crypto V.3.1. TI246 - Análisis de Vulnerabilidades en Sistemas Operativos.doc TI343 - Análisis de Vulnerabilidades de la Tarjeta Advantis Crypto V.3.1
Evaluación de la fortaleza de las funciones de seguridad del TOE (AVA_SOF.1)	TI246 - Análisis de Vulnerabilidades en Sistemas Operativos.doc TI343 - Análisis de Vulnerabilidades de la Tarjeta Advantis Crypto V.3.1
Alta resistencia (AVA_VLA.4)	TI246 - Análisis de Vulnerabilidades en Sistemas Operativos.doc TI343 - Análisis de Vulnerabilidades de la Tarjeta Advantis Crypto V.3.1

Tabla 3.- Documentación y requisitos de garantía de seguridad.

7. CUMPLIMIENTO DE PERFILES DE PROTECCIÓN

Esta declaración de seguridad supone la segunda fase de la posible cadena de certificaciones de la seguridad de una tarjeta inteligente.

Se apoya en la certificación del chip y satisface los requisitos adicionales requeridos para el cumplimiento de Perfil de Protección [1].

7.1 Perfil de Protección CWA14169

7.1.1 Referencia

Véase [1].

7.1.2 Adaptación y operaciones fijadas

Todas las operaciones del PP están definidas en esta declaración de seguridad.

8. JUSTIFICACIONES

8.1 Suficiencia de los objetivos de seguridad

Véase [1].

8.2 Adecuación de los requisitos de seguridad

Véase [1].

8.3 Justificación de la síntesis funcional

8.3.1 Combinación de los comandos de la tarjeta

La relación de comandos de la tarjeta Advantis Crypto, especificada en CMD, es ortogonal, en el sentido de que la funcionalidad de cada comando, tal como se especifica, es única, y no hay solapamientos de funcionalidad ni efectos laterales o secundarios no documentados.

La relación de requisitos funcionales de seguridad exigidos por esta declaración de seguridad y los comandos y propiedades de la tarjeta Advantis especificados en el apartado **SÍNTESIS DE LA ESPECIFICACIÓN DEL PRODUCTO**, es completa y única, no pudiendo establecerse otra correspondencia, de manera que es la única combinación de comandos que satisface los requisitos funcionales.

8.3.2 Trazabilidad de la especificación funcional

La siguiente tabla resume que funciones de seguridad son necesarias para cubrir los requisitos de seguridad impuestos:

SFRs \ SFs		SF1	SF2	SF3	SF4	SF5	SF6	SF7	SF8	SF9	SF10	SF11	SF12	SF13	SF14	SF15	SF16	SF17	SF18	SF19	SF20	SF21
FTP_PHP.1										X												
FPT_PHP.3										X												
FDP_RIP.1							X			X												
FPT_EMSEC.1										X												
FPT_TST.1										X											X	
FPT_FLS.1									X	X						X	X					
FIA_UAU.1								X														X
FIA_UID.1								X														X
FMT_SMR.1		X	X	X	X		X	X				X	X	X				X		X		
FMT_SMF.1	PREPERSO		X	X																		
	PERSO		X	X								X										
	ADMINUSER	X			X	X	X	X			X		X	X	X			X	X	X		X
FMT_MSA.1	ADMINISTRADOR						X						X	X				X	X			
	SIGNATARIO				X						X											X
FDP_SDI.2									X	X	X								X			
FIA_AFL.1																						X
FIA_ATD.1																						X
FMT_MTD.1								X														
FDP_ACF.1											X		X	X								X
FDP_ACC.1					X			X					X	X	X				X			X
FMT_MOF.1											X											X
FMT_MSA.3						X															X	
FTP_ITC.1					X													X				
FTP_TRP.1					X													X				
FMT_MSA.2				X	X	X					X		X	X				X	X			X
FCS_CKM.1														X								
FCS_CKM.4						X																
FCS_COP.1													X					X				
FDP_ITC.1				X														X				
FDP_ETC.1														X								
FDP_UIT.1	SVD TRANSFER													X								
	TOE DTBS				X														X			
FPT_AMT.1																					X	

Tabla 4.- Trazabilidad de la especificación funcional

8.3.3 Justificación de la cobertura de los requerimientos de seguridad

SFR's		SF's
FTP_PHP.1		SF9
FPT_PHP.3		
FDP_RIP.1		SF6, SF9
FPT_EMSEC.1		SF9
FPT_FLS.1		SF8, SF9, SF15, SF16
FIA_UAU.1		SF7, SF21
FIA_UID.1		
FMT_SMR.1		SF1, SF2, SF3, SF4, SF5, SF6, SF7, SF11, SF12, SF13, SF14, SF17, SF18, SF19, SF21
FMT_SMF.1	**PREPERSO**	SF2, SF3,
	PERSO	SF2, SF3, SF11
	ADMINUSER	SF1, SF4, SF5, SF6, SF7, SF12, SF13, SF14, SF17, SF18, SF19, SF21
FMT_MSA.1	**ADMINISTRADOR**	SF6, SF10, SF12, SF13, SF17, SF18
	SIGNATARIO	SF4, SF10, SF21
FDP_SDI.2		SF8, SF9, SF10, SF18
FIA_AFL.1		SF21
FIA_ATD.1		
FMT_MTD.1		SF7
FDP_ACF.1		SF10, SF12, SF13, SF21
FDP_ACC.1		SF4, SF7, SF12, SF13, SF14, SF18, SF21
FMT_MOF.1		SF10, SF21
FMT_MSA.3		SF5, SF20
FTP_ITC.1		SF4, SF17
FTP_TRP.1		

SFR's		SF's
FMT_MSA.2		SF4, SF5, SF6, SF10, SF12, SF13, SF17, SF18 SF21
FCS_CKM.1		SF13
FCS_CKM.4		SF6
FCS_COP.1		SF12, SF17
FDP_ITC.1		SF4, SF17
FDP_ETC.1		SF13
FDP_UIT.1	**SVD TRANSFER**	
	TOE DTBS	SF4, SF18
FPT_AMT.1		SF20
FPT_TST.1		SF9, SF20

Tabla 5.- Justificación de la cobertura de los requerimientos de seguridad

8.3.4 Fortaleza de las funciones

La fortaleza de función alta, para el mecanismos permutacionales / probabilísticos citados anteriormente (véase §6.1.1) se requiere para asegurar la resistencia del TOE frente a atacantes con alto potencial de ataque.

La fortaleza de los mecanismos criptográficos empleados por la tarjeta, indicados en el apartado 4.2 de APP, son igualmente de fortaleza alta. Dicha fortaleza está fuera del alcance de esta evaluación.

8.3.5 Medidas de garantía de seguridad.

Las medidas de garantía de seguridad satisfacen los requisitos del nivel de evaluación exigido, EAL4+, tal como se deduce del análisis de su contenido y presentación.

8.4 Justificación del cumplimiento de Perfiles de Protección.

El requisito **Especificación de las Funciones de Gestión (FMT_SMF.1)** no está incluido inicialmente en [1]. Este requisito se incorpora a esta declaración de seguridad en cumplimiento de la versión de la norma de evaluación utilizada, CC/CEM 2.3, que lo exige por dependencia de varios componentes de la clase FMT, que sí están demandados por el PP.

La incorporación del requisito **Especificación de las Funciones de Gestión (FMT_SMF.1)** no exige de la modificación de los objetivos de seguridad a satisfacer, por cuanto se trata de una exigencia para el correcto soporte a los demás requisitos de la clase FMT que se requieren en el [1], que son los que directamente satisfacen los objetivos de seguridad demandados en dicho PP.

La divergencia entre las distintas versiones de Common Criteria en las que se basa el PP (2.1) y la que cumple el TOE (2.3) no produce ningún conflicto. Para comprobarlo se analizan las distintas "Final Interpretations" que se encuentran en la página oficial de CC bajo el epígrafe **Interpretations that apply to CC v2.2 and CC v2.1 and which have been included in CC v2.3**

"Role of Sponsor": esta interpretación hace referencia a la distinción entre el papel de desarrollador y el papel de sponsor. En nuestro caso no nos afecta puesto que ambos roles son desarrollados por Sermepa.

"Rules governing binding should be specifiable": esta interpretación se refiere a la familia FIA_USB, que no se incluye en EAL4+, por lo que no nos afecta.

"C&P elements incluye characteristics": esta interpretación explica que los elementos de contenido y presentación no sólo se refieren a las evidencias sobre el TOE o garantía de seguridad sino al propio TOE. Así se ha interpretado al seguir el PP.

"Circular Arguments in the objectives of FUN.2": en la versión 2.1 se incluía entre los propósitos de FUN.2 evitar los argumentos circulares. Esto se ha corregido y aclarado. El propósito de ordenar los tests es evitar que se obtengan resultados distintos por las dependencias entre las distintas pruebas. Así se ha interpretado al seguir el PP.

"COV.3 dependency on FSP.1": esta interpretación no nos afecta porque el componente ATE_COV.3 no se incluye en EAL4+.

"Sequencing of sub-activities": esta interpretación hace referencia al conflicto que se crea cuando hay dependencias circulares entre dos requisitos. Si para dar un evaluar un requisito se deben cumplir todos aquellos de los que depende, si existen dependencias circulares nunca se podrán evaluar. Esto se ha corregido en CC 2.3, y no afecta a la redacción del PP. Además los requisitos que se ven afectados (ASE_INT and ASE_DES) no forman parte del nivel EAL4+.

"FCS_CKM/COP dependency on FDP_ITC.1": FCS_CKM.2/3/4 y FCS_COP.1 dependen todos ellos de FDP_ITC.1. En esta interpretación introduce además dependencia de FDP_ITC.2. Este requisito no se incluye en EAL4+ por lo cual esta interpretación no nos afecta.

"CC Part2 F.12 user notes": esta interpretación se limita a señalar un error tipográfico.

"Inconsistency between FDP_ITC and FDP_ETC": esta interpretación no nos afecta puesto que hace referencia a un fallo editorial/gramatical. En el requisito FDP_ITC, en lugar de SFP en singular debe aparecer SPF(s), dando opción a que se puedra interpretar como singular o plural.

"FDP_ROL statement": esta interpretación se refiere a la familia FDP_ROL, que no se incluye en EAL4+, por lo que no nos afecta.

"Must Test Setup An Cleanup Code Run Unprivileged": esta interpretación soluciona la duda de si se pueden o no ejecutar scripts con determinados privilegios para preparar el TOE o reiniciarlo. En la versión 2.3 de CC se especifica que es posible siempre y cuando se indique. En CC 2.1 la cuestión estaba abierta, con lo cual no tiene repercusión para este caso.

"Applicability of ISO/IEC Standards": esta interpretación no nos afecta ya que se limita a incluir un elemento más a la bibliografía expuesta en el anexo C de la parte 1 de CC relativo a los procedimientos de registro de los PP.

8.5 Justificación del nivel de garantía de evaluación EAL4+

El nivel de garantía EAL 4 se ha escogido porque permite al desarrollador obtener un nivel de seguridad alto sin necesidad de procesos y prácticas altamente especializadas. Se considera como el nivel superior que puede ser aplicado a un producto sin encarecerlo en exceso o aumentar su complejidad demasiado.

Puesto que el producto será distribuido a múltiples usuarios y su funcionamiento escapará al control directo del desarrollador es necesario que la documentación de uso este libre de errores, contradicciones o ambigüedades. Los procedimientos de seguridad de todos los modos de funcionamiento y los estados inseguros ser fácilmente detectables. Esta es la razón por la que EAL4 se aumenta con el componente **AVA_MSU.3**.

El TOE debe ser altamente resistente a ataques de penetración para cumplir con los objetivos de seguridad OT_SCD_secrecy, OT_SIGy_SIgF y OT_Sig_Secure. Esta es la razón por la que EAL 4 se aumenta con el componente **AVA_VLA.4**.

9. ACRÓNIMOS

CAN: Nota de aplicación Confidencial (Confidencial Application Note)

CC: Criterios Comunes (Common Criteria)

CCD: Dato de Creación de Cifrado (Cipher Creation Data)

CEM: Metodología Común para la Evaluación de la Seguridad de la Tecnología de la Información (Common Methodology for Information Technology Security Evaluation)

CGA: Aplicación de Generación de Certificado (Certificate Generation Application)

CM: Gestión de la Configuración (Configuration Management)

DTBS: Datos que se desea Firmar (Data To Be Signed)

EAL: Nivel de Garantía de la Evaluación (Evaluation Assurance Level)

IC: Circuito Integrado (Integrated Circuit)

IT: Tecnología de la Información (Information Technology)

ISO: Organización Internacional para la Estandarización (International Standardization Organization)

JIL: Librería Colectiva de Interpretación (Joint Interpretation Library)

RAD: Datos de Autenticación de Referencia (Reference Authentication Data)

PIN: Número de Identificación Personal (Personal Identification Number)

PUK: Clave de Desbloqueo de PIN (PIN Unblocking Key)

PKCS: Estándar Criptográfico de Clave Pública (Public-Key Cryptographic Standard)

PP: Perfil de Protección (Protection Profile)

RNG: Generador de Números Aleatorios (Random Number Generator)

SCA: Aplicación de Creación de Firma (Signature-Creation Application)

SCD: Datos de Creación de Firmas (Signature-Creation Data), clave privada.

SOF: Fortaleza de Función (Strength of Function)

SSCD: Dispositivo Seguro de Creación de Firmas (Secure Signature-Creation Device)

ST: Declaración de Seguridad (Security Target)

SVD: Datos de Verificación de Firmas (Signature-Verification Data), clave pública.

TOE: Objeto de evaluación (Target of Evaluation)

TSF: TOE Security Functions (Funciones de Seguridad del TOE)

TSP: Política de Seguridad del TOE (TOE Security Policy)

10. REFERENCIAS

[1] CWA 14169:2004. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05 (Perfil de Protección - Dispositivo Seguro de Creación de Firma)

[2] ISO/IEC 7816-4 Identification Cards – Integrated Circuit(s) cards with contacts. Inter-industry commands for interchange.

[3] ISO/IEC 7816-5 Identification Cards – Integrated Circuit(s) cards with contacts. Registration system for applications in IC cards.

[4] ISO/IEC 7816-8 Identification Cards – Integrated Circuit(s) cards with contacts. Security architecture and related inter-industry commands.

[5] ISO/IEC 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[6] RSA Laboratories, PKCS#1: RSA Encryption Standard, an RSA Laboratories Technical Note Version 1.5. Revised November 1, 1993.

[7] RSA Laboratories, PKCS#10: Certification Request Syntax Standard, an RSA Laboratories Technical Note Version 1.7. Revised May 26, 2000.

[8] RSA Laboratories, PKCS#15: Cryptographic Token Information Standard, an RSA Laboratories Technical Note Version 1.0, Revised April 1999.

[9] Common Criteria for Information Technology. Security Evaluation. August 2005, Version 2.3, ISO/IEC 15408:1999.

a. Part 2: Security functional requirements.

b. Part 3: Security assurance requirements.

[10] ETSI TS 102 176-1 v.1.2.1 (2005-07) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

[11] Infineon Technologies AG. Security and Chip card Ics. Evaluation Documentation. SLE66CX162PE / m1531-a24 SLE66CX80PE / m1533-a24. Both with RSA2048 V1.4 Security Target Version 1.1 Date 2005-11-05 Author H.-J. Novinsky, H.-U. Buchmüller.

[12] Manual de Usuario Advantis Crypto V.3.1. Sermepa, 2007

[13] Common Methodology for Information Technology Security Evaluation. Evaluation methodology. August 2005, Version 2.3.

[14] EMV '2000, Especificaciones de Tarjetas de Circuito Integrado para Sistemas de Pago. Versión: 4.1, Mayo, 2004.

[15] Infineon Technologies AG. Security and Chipcard ICs. Evaluation Documentation. SLE66CX162PE / m1531-a24, SLE66CX80PE / m1533-a24 Both with RSA2048 V1.4. Security Target Version 1.1 Date 2005-11-05.