Declaración de Seguridad

para

Módulo de Firma Electrónica de Documentos

(Versión 2.19)

de

RCI Banque España

Versión 2.0

Septiembre 2014

Contenido

Control de Cambios

Versión	Fecha	Autor	Modificaciones
0.9	25/05/2012	RCI Banque	Primera Edición
1.0	04/06/2012	RCI Banque	Cambios en sección 1, 6 y 7
1.1	05/10/2012	RCI Banque	Cambios derivados de las ORs de Epoche
1.2	25/10/2012	RCI Banque	Actualización para la eliminación de DNIe
1.3	12/12/2012	RCI Banque	Cambios derivados de las ORs de Epoche
1.4	05/06/2013	RCI Banque	Cambios derivados de las ORs de Epoche
1.5	20/11/2013	RCI Banque	Actualización acorde a cambios del TOE
2.0	30/09/2014	RCI Banque	Actualización para *assurance continuity*

1 Introducción

1.1 Términos y Definiciones

1 **Documento**: información estructurada, contenida en un fichero en formato PDF, que se va a transmitir al TOE para su firma; un documento puede ser un contrato de financiación. Se utilizarán indistintamente ambos términos, documento o contrato.

2 **Intervinientes**: todas las personas que firman el documento. En el caso del contrato de financiación, se trata del titular o titulares del contrato y los avalistas.

3 **Cliente**: es el puesto desde donde se realiza la operación de firma. En él se ejecutan los applets que forman parte del TOE. Si está en un concesionario, también se ejecuta en él la parte cliente del puesto de venta @baco.

4 **Módulo de firma**: módulo java donde se gestiona todo el proceso de firma, tanto de los intervinientes como del sistema y que incorpora una base de datos temporal. Se trata del producto Módulo de Firma Electrónica de Documentos, objeto de la evaluación (TOE).

5 **Plataforma de firma**: es el producto ASF de TB Solutions encargado de gestionar la validez del certificado de empresa, la obtención del sello de tiempo, realizar el cifrado de los documentos y la longevidad de la firma. También es el sistema que va a custodiar los documentos firmados ("original"), junto con las evidencias de refirmado de dichos documentos.

6 **@baco**: También llamado puesto de venta, es el sistema encargado de la generación de los documentos PDF involucrados en procesos completos de firma, así como de los descriptores XML de dichos procesos. Interactúa con el Módulo de firma ya que le proporciona PDFs a éste, y también es el encargado de almacenar documentos firmados parcialmente. Tiene una arquitectura cliente-servidor, donde su parte cliente corre en el puesto de venta de los concesionarios para realizar contratos de financiación con RCI Banque.

7 **Archivo digital:** Se trata de un gestor de documentos que almacena una copia de los documentos que han pasado un proceso completo de firma. Proporciona opciones de búsqueda, y se comunica con ASF (de donde recupera los documentos firmados) a través del Web Service "Consulta Docs Securizados" publicado por el TOE.

8 **Proceso de firma:** Período de tiempo en que la información de los documentos a ser firmados, así como sus firmas, y su estado, están almacenados dentro del TOE.

9 **Proceso completo de firma:** Comprende todo el procesamiento desde que @baco genera los documentos iniciales, hasta que estos son firmados por todos sus

intervinientes mediante el Módulo de firma, y finalmente firmados digitalmente por ASF, y almacenados en él. Un proceso completo de firma estará formado de uno o varios procesos de firma, y la información será almacenada en @baco en los períodos de tiempo existentes entre procesos de firma.

10 **Descriptor de proceso completo de firma:** Es un fichero XML descriptivo del proceso completo de firma en el que figura la información del estado del proceso. Esta información comprende la totalidad de los documentos involucrados en el proceso, incluidos los propios PDFs completos, así como el estado de las firmas de los intervinientes para cada documento. Este descriptor es generado en @baco, y trasladado al TOE para ser utilizado y actualizado en cada proceso de firma.

11 **Documento firmado parcialmente (documento incompleto):** Es un documento involucrado en un proceso completo de firma que no ha sido firmado por todos los intervinientes.

12 **Documento completo:** Es un documento que ha finalizado el proceso completo de firma, es decir, aquel que ya ha sido firmado por todos los intervinientes, y al que se le ha incluido el sello de tiempo y la firma digital del sistema en ASF.

13 **Administrador de sistemas centrales:** Personal de Renault o RCI Banque que administran el software base de los servidores instalados en el CPD: servidores web y de aplicaciones y gestor de bases de datos. Este personal es distinto al personal que opera en los puestos cliente.

1.2 Referencias del TOE y de la Declaración de Seguridad

1.2.1 Referencia de la Declaración de Seguridad

Título	Declaración de Seguridad para Módulo de Firma Electrónica de Documentos - Versión 2.19 de RCI Banque España
Versión	2.0
Autor	RCI Banque España
Fecha de publicación	30/09/2014

1.2.2 Referencia del TOE

Título	Módulo de Firma Electrónica de Documentos
Versión	2.19
Desarrollador	RCI Banque España
Fecha de publicación	30/09/2014

1.3 Resumen del TOE

1.3.1 Tipo de TOE

14 El TOE es un módulo diseñado para llevar a cabo la gestión y firma de documentos en formato PDF generados por la Alianza Renault-Nissan, tales como contratos de financiación con RCI Banque realizados en concesionarios.

1.3.2 Uso del TOE

15 Se trata de un módulo que permite la firma de contratos de financiación, prestaciones y servicios, u otros tipos de documentos utilizados en la actividad de RCI y empresas de la Alianza Renault-Nissan.

16 El TOE hace uso de un dispositivo de captura de firmas (tableta WACOM 520U) para capturar las firmas de los intervinientes. Esta captura de firmas se realiza con el fin de llevar a cabo un posterior uso de las mismas para adjuntarlas al correspondiente documento PDF.

17 El TOE realiza la gestión de la comunicación entre las partes Cliente y el componente servidor tanto para enviar documentos a firmar, como para recuperar documentos previamente firmados. El procedimiento de firma se gestiona en el componente servidor, e incluye tanto el firmado de los intervinientes sobre el documento a firmar, como la inclusión de un sello de tiempo proveniente de una TSA, y la firma digital de dicho documento, sus firmas y el sello de tiempo, por parte de la plataforma de firmas ASF.

18 La plataforma de firmas tiene como objetivo confirmar la validez del certificado electrónico (no revocación) con el que se va a firmar el documento, la consulta a la TSA para recoger el sello de tiempo y la custodia final de los documentos firmados.

19 El TOE permite que la firma de documentos se realice en diferentes instantes, de forma que se puedan ir incorporando nuevas firmas a lo largo del tiempo hasta el cierre del proceso completo de firma, que culmina con la adición del sello de tiempo y la firma del emisor del contrato por parte de ASF.

20 En el proceso de firma, se pueden pasar varios documentos a firmar, aunque cada uno será firmado por separado.

1.3.3 Características de Seguridad del TOE

21 Las características de seguridad de que consta el TOE son las siguientes:

a. El TOE genera auditoría para los eventos relacionados con los procesos completos de firma.

b. El TOE gestiona las comunicaciones entre las partes cliente y servidor del mismo. Estas comunicaciones hacen uso del protocolo SSL con certificados firmados por la CA del grupo Renault.

c. El TOE elimina todos los datos relativos a documentos almacenados durante los procesos de firma una vez éstos han finalizado.

d. El TOE elimina todos los datos relativos a firmas de intervinientes de los puestos cliente una vez el proceso de firma ha concluido.

e. El TOE controla el orden del proceso completo de firma de modo que únicamente permite finalizarlo cuando todos los intervinientes han firmado los documentos involucrados en el mismo.

f. El TOE realiza las siguiente funciones de gestión:

   i. El TOE permite firmar documentos incompletos en los puestos clientes por parte de los intervinientes a través de la tableta de firma.

   ii. El TOE permite cancelar un proceso de firma.

   iii. El TOE permite finalizar un proceso completo de firma.

   iv. El TOE permite posponer un proceso de firma.

1.3.4 Software y Hardware requerido por el TOE

22 El entorno operacional utilizado por el TOE para operar consta de los siguientes elementos:

- Para los puestos Cliente:

  a. Sistema Operativo Windows XP, Windows 7, 8 y 8.1

  b. Navegadores: Internet Explorer v7 o superior o Mozilla Firefox v9 o superior.

  c. Plugin Flash v11 o superior.

  d. Tableta digitalizadora WACOM 520-U y drivers.

  e. JVM versión 6 o superior.

  f. Microsoft Visual C++ 2005 o superior

- Para el servidor

  a. Sistema operativo: Solaris 10.

  b. Servidor web Apache 2.0.59 o superior.

  c. Servidor de aplicaciones J2EE WebSphere application server CE v.2.1.0.1.

  d. Java JRE v.1.6.20 o superior.

  e. Plataforma ASF de TB Solutions v.51.17 o superior.

  f. Puesto de venta RCI (@baco) v.1.04.267 o superior

  g. Archivo digital

  h. Camerfirma (Conexión SSL a sus servidores)

  i. LDAP SUN One DS 5.2P4

1.4 Descripción del TOE

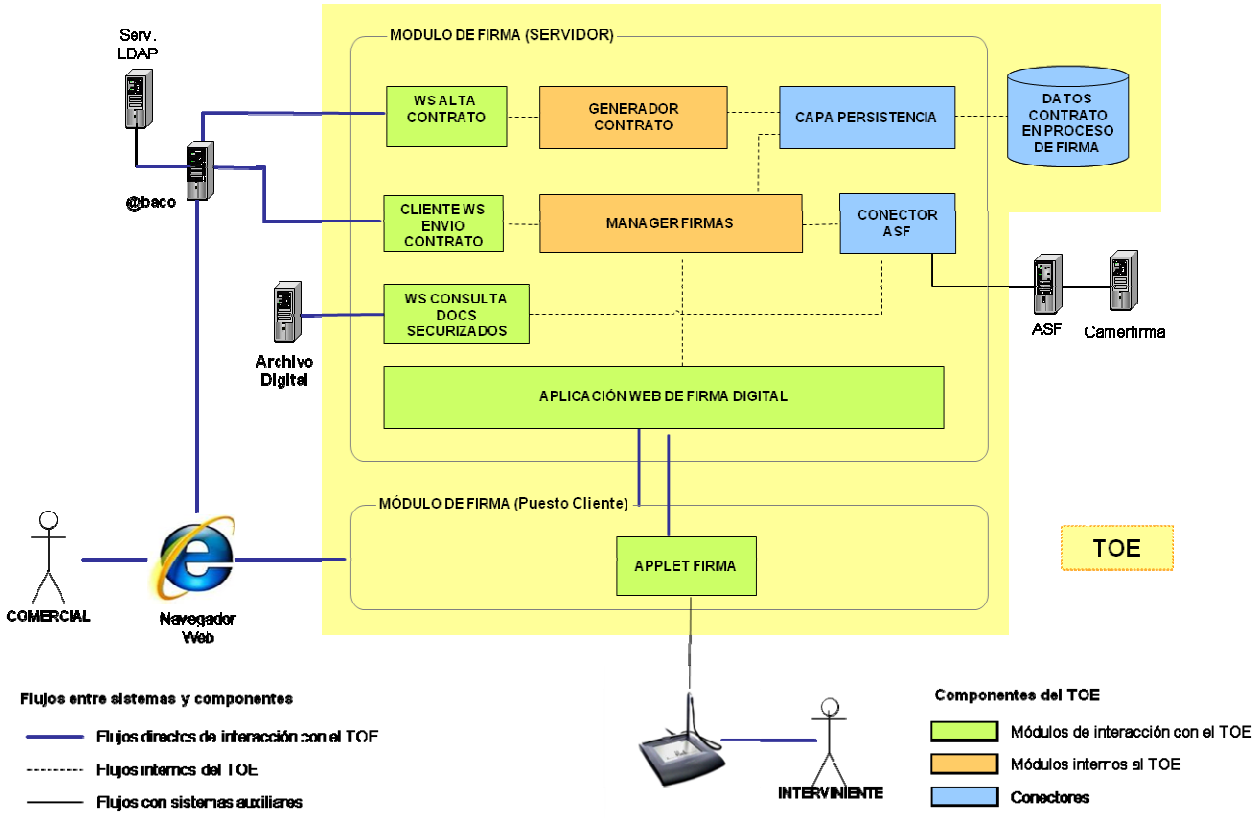
1.4.1 Ámbito físico del TOE

23 Los componentes ejecutables de que consta el TOE son los siguientes:

Elemento	Descripción
ContratoDigitalWeb.war	War que contiene la aplicación Módulo de Firma Electrónica de Documentos.
tabletas.jar	Fichero applet para la gestión de la firma con la tableta.
Guías y manuales	Conjunto de manuales de instalación y operación para Módulo de Firma Electrónica de Documentos.

1.4.2 Ámbito Lógico del TOE

24 La siguiente figura muestra los componentes de que consta el TOE desde un punto de vista lógico, así como la interrelación existente entre ellos:



25 Tal y como se puede apreciar en la figura, el TOE tiene una arquitectura cliente-servidor, en la que la parte cliente se encarga de tomar las firmas de los intervinientes haciendo uso de un **Applet** para la interacción con la tableta digitalizadora. El comercial del grupo Renault es el encargado de dirigir el proceso de firma a través de esta parte cliente, ya que dispone de las siguientes operaciones:

- ✓ Consultar datos de documentos completos.
- ✓ Visualizar documentos parcialmente firmados.

- ✓ Lanzar la rutina de obtención de firma de intervinientes desde la tableta de firma.
- ✓ Cancelar un proceso de firma.
- ✓ Finalizar un proceso de firma en caso de que todos los intervinientes hayan firmado.

26 La parte servidora publica funcionalidad del TOE a través de Web Services (en adelante WS) para la comunicación con entidades externas (Archivo Digital, @baco y ASF). Para la comunicación con la parte cliente del TOE, se hace uso de la **Aplicación Web de Firma Digital**, la cual a su vez se comunica con el **Manager de Firmas**, que es el "core" del Módulo de Firma.

27 El LDAP que aparece en la figura tiene como objetivo la autenticación y control de acceso del comercial a @baco. Por su parte, Camerfirma se utiliza para validar la autenticidad del certificado de empresa con que se firman los documentos y suministra el sello de tiempo.

28 Los WS publicados por el TOE son los siguientes:

- ✓ WS Alta Contrato: Proporciona un mecanismo a través del cual @baco introduce al TOE documentos incompletos (ya sean sin ninguna firma de intervinientes o con alguna), para su inserción en un proceso de firma, en forma de documento XML autocontenido. Una vez que el dicho XML es recibido a través del WS, el módulo **Generador Contrato** valida el formato XML introducido, y posteriormente se traslada a la **Capa Persistencia** donde se traduce a sentencias SQL para introducir la información del XML en la base de datos interna **Datos Contrato en Proceso de Firma**.
- ✓ Cliente WS Envío Contrato: Se utiliza como camino de vuelta de un alta de contrato, y a través de él se proporciona la URL devuelta por el Módulo de Firma para acceder al proceso de firma relativo a esos documentos.
- ✓ WS Consulta Docs Securizados: Provee un servicio de consulta que será utilizado por el Archivo Digital para descargar documentos completos desde ASF, a través del **Conector ASF**, que es la única vía de comunicación de que dispone ASF para con el resto de sistemas.

29 Si se recibe una petición de cancelación de proceso de firma, o una petición para posponerlo, el proceso de firma correspondiente y todos sus datos asociados será eliminado de la base de datos interna. En caso de recibirse una petición de terminación de proceso de firma (porque todos los intervinientes hayan firmado los documentos), todos los datos asociados a dicho proceso de firma serán eliminados de la base de datos interna, y se enviarán los documentos a ASF a través del **Conector ASF** para su sellado de tiempo y su firma digital.

30 Cada vez que un interviniente introduce una firma, ésta es enviada desde la parte cliente del TOE a la parte servidor del mismo, procesada en el **Manager de Firmas**, y

enviada a la **Capa Persistencia** donde se inserta la firma en cuestión en la base de datos interna.

2 Declaraciones de Conformidad

2.1 Conformidad respecto a la norma Common Criteria

31 Esta Declaración de Seguridad cumple con lo indicado en la norma Common Criteria versión 3.1, Parte 2 release 4 extendida, y Parte 3 release 4, para un nivel de evaluación EAL1 aumentado con los componentes ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2.

2.2 Conformidad respecto a Perfiles de Protección

32 Esta Declaración de Seguridad no declara cumplimiento de ningún Perfil de Protección.

3 Definición del Problema de Seguridad

3.1 Activos protegidos por el TOE

33 Los activos que protege el TOE son los siguientes:

Documentos durante el proceso de firma	Integridad y confidencialidad de los documentos a ser firmados, o firmados parcialmente, durante el proceso de firma.
Descriptor de firmas durante el proceso de firma	Integridad y confidencialidad de los descriptores de firmas durante el proceso de firma.
Datos de firma durante el proceso de firma	Integridad y confidencialidad de las firmas de los intervinientes durante el proceso de firma.
Secuencia del proceso de firma	Integridad de la secuencia en que se ejecuta el proceso completo de firma.
Autenticidad de documentos a firmar	Autenticidad de los documentos que intervienen en un proceso de firmas (se consideran auténticos aquellos documentos generados por @baco).

3.2 Agentes de las Amenazas

34 Los agentes contemplados como potenciales atacantes son los siguientes:

Usuario Autenticado	Es un usuario que dispone de un certificado de autenticación con el entorno operacional del TOE. Puede ser personal interno de RCI o personal de concesionarios del grupo Renault.
Usuario sin autenticar	Cualquier usuario conectado a Internet.

3.3 Amenazas

T.Acceso	Un usuario sin autenticar logra acceso a la red donde está desplegado el TOE y obtiene información de documentos, firmas y descriptores de firmas.
T.ModificaSecuencia	Cualquier agente modifica la secuencia de operaciones y hace que un documento incompleto sea firmado digitalmente por ASF, y pasado a documento completo.
T.FirmaNoAutorizada	Cualquier agente inserta una firma en un documento en proceso de firma, sin que dicha firma provenga directamente de un interviniente con el procedimiento habitual.
T.DocumentoFalso	Cualquier agente envía al TOE un documento falso a ser

	firmado, y el TOE procesa dicho documento como válido y realiza un proceso completo de firma.
T.ModificaDocumento	Cualquier agente modifica un documento, sus firmas o el descriptor de firmas durante el proceso completo de firma.

3.4 Políticas Organizativas de Seguridad

35 Las políticas organizativas de seguridad definidas son las siguientes:

OSP.Auditoría	El TOE deberá generar auditoría para las acciones que intervienen en los procesos completos de firma.
OSP.ProcesoFirma	Los documentos firmados por todos los intervinientes se deberán enviar a una entidad externa donde se sellarán con una marca de tiempo y se firmarán digitalmente.
OSP.Gestión	El TOE deberá implementar funcionalidad de gestión relacionada con los procesos completos de firma.

3.5 Hipótesis

36 Las hipótesis para el entorno operacional contempladas son las siguientes:

A.Configuración	Tanto los puestos clientes como los servidores centrales donde se ejecuta el TOE (servidores Web, de aplicaciones, LDAP y base de datos), y los otros sistemas con los que interactúa (@baco, Plataforma ASF, Archivo Digital) están bien configurados, y no son una fuente de ataque.
A.Físico	Todo el sistema global, a excepción de los puestos clientes y los dispositivos de captura de firma, están en un CPD securizado.
A.Personal	Los administradores de los sistemas centrales, tanto de RCI como de Renault, son de confianza.
A.Autenticación	El entorno operacional del TOE es el encargado de autenticar al usuario del puesto cliente con que se opera.
A.Integridad	La integridad de los documentos y sus firmas es mantenida por el entorno operacional.
A.PKI	La custodia de la PKI utilizada para la generación de certificados firmados por la CA del grupo Renault está gestionada por personal confiable, y sólo se generarán certificados si su uso final es conocido y aceptado.
A.DMZ	La parte servidor del TOE y su entorno está desplegado en una red DMZ segura en la que todas las comunicaciones con Internet son manejadas por un reverse proxy y las comunicaciones con la Intranet se autorizan a nivel IP:Puerto. Se utilizan servidores intermedios para las comunicaciones de tal manera que éstas nunca son directas. Toda comunicación entre elementos dentro de la DMZ se considera segura. Tanto la configuración de la red como la asignación y utilización de los pares IP:puerto en los nodos conectados a la misma es responsabilidad del grupo de seguridad de Renault y no constituye una fuente de ataque.

A.Generación	El entorno operacional del TOE es el encargado de generar los documentos a firmar y asegurar su envío de forma única al TOE para cada proceso completo de firma.

4 Objetivos de Seguridad

4.1 Objetivos de Seguridad del TOE

O.Comunicación	La comunicación entre la parte cliente y servidora del TOE se realiza haciendo uso de SSL con certificados firmados por la CA del grupo Renault.
O.Borrado	El TOE deberá borrar los datos de documentos y firmas utilizados durante el proceso de firma, una vez dicho proceso finalice.
O.ProcesoFirma	El TOE asegurará que los documentos serán firmados por todos los intervinientes, y tras esto invocará a una entidad externa que los sellará con una marca de tiempo y los firmará digitalmente.
O.Auditoría	El TOE generará auditoría para las acciones que intervienen en los procesos completos de firma.
O.Gestión	El TOE implementará funcionalidad de gestión relacionada con los procesos completos de firma.

4.2 Objetivos de Seguridad del Entorno Operacional

OE.FirmaDigital	El entorno operacional proporcionará una marca de tiempo de una fuente confiable y un mecanismo para realizar firmas digitales a los documentos firmados por todos sus intervinientes.
OE.Integridad	El entorno operacional garantizará la integridad de los documentos y sus firmas.
OE.Autenticación	El entorno operacional será el encargado de autenticar a los usuarios de los puestos clientes.
OE.Personal	Los administradores de los sistemas centrales tanto de RCI como de Renault son de confianza.
OE. Configuración	Los puestos cliente y los servidores centrales donde se ejecuta el TOE están bien configurados.
OE.Físico	Todo el sistema global, a excepción de los puestos clientes y los dispositivos de captura de firma, están soportados por un entorno seguro.
OE.PKI	La custodia de la PKI utilizada para la generación de certificados firmados por la CA del grupo Renault estará gestionada por personal confiable, y sólo se generarán certificados si su uso final es conocido y aceptado.
OE.DMZ	La parte servidor del TOE y su entorno se desplegará en una red DMZ segura en la que todas las comunicaciones con Internet serán manejadas por un reverse proxy y las comunicaciones con la Intranet se autorizarán a nivel

	IP:Puerto. Se utilizarán servidores intermedios para las comunicaciones de tal manera que éstas nunca serán directas. Tanto la configuración de la red como la asignación y utilización de los pares IP:puerto en los nodos conectados a la misma es responsabilidad del grupo de seguridad de Renault y no constituye una fuente de ataque.
OE.Generación	La generación y el del envío de los documentos a firmar será realizada por el entorno y sólo se realizará dicho envío una única vez para cada proceso completo de firma.

4.3 Justificación de los Objetivos de Seguridad

4.3.1 Cobertura

37 La siguiente tabla muestra el modo en que los objetivos del TOE y del entorno operacional colaboran para solucionar el problema de seguridad definido.

	O.Comunicación	O.Borrado	O.ProcesoFirma	O.Auditoría	O.Gestión	OE.FirmaDigital	OE.Integridad	OE.Autenticación	OE.Personal	OE.Configuración	OE.Físico	OE.PKI	OE.DMZ	OE.Generación
T.Acceso		X								X		X	X	
T.ModificaSecuencia			X											
T.FirmaNoAutorizada	X	X								X				
T.DocumentoFalso	X								X			X		
T.ModificaDocumento	X						X		X			X		
OSP.Auditoría				X										
OSP.ProcesoFirma			X			X								
OSP.Gestión					X									
A.Configuración										X				
A.Físico											X			
A.Personal									X					
A.Autenticación								X						
A.Integridad							X							
A.PKI												X		
A.DMZ													X	
A.Generación														X

4.3.2 Suficiencia

38 Justificación de suficiencia para las amenazas:

T.Acceso	Cualquier información relativa a un proceso de firma se elimina del TOE una vez el proceso de firma ha finalizado (O.Borrado). Los servidores y puestos cliente están bien configurados y evitan el acceso a los recursos a personal no autorizado (OE.Configuración). Además, la gestión y custodia de la PKI utilizada para la generación de certificados firmados por la CA del grupo Renault está gestionada por personal confiable, y únicamente aquel

	personal que requiera de certificados para la comunicación dispondrán de ellos (OE.PKI). El acceso a los componentes del entorno y la parte servidora del TOE que están desplegados en la red DMZ no es accesible desde el exterior (OE.DMZ).
T.ModificaSecuencia	El TOE implementa funcionalidad encargada de garantizar que únicamente los documentos firmados por todos sus intervinientes serán enviados a ASF para su sellado de tiempo y su firma digital. (O.ProcesoFirma).
T.FirmaNoAutorizada	No es posible disponer de una firma que pueda ser aplicada a un documento dentro de un proceso de firma sin que esta firma provenga de algún dispositivo de firma aceptado (tableta digitalizadora), ya que el TOE implementa un borrado de todos los datos involucrados en el proceso de firma, por lo que las firmas utilizadas dejan de estar disponibles en el TOE (O.Borrado). El entorno operacional está bien configurado de modo que no es posible que las firmas de los intervinientes sean capturadas durante el proceso completo de firma para un uso posterior (OE.Configuración). Además, no es posible insertar una firma en un proceso de firma si no se dispone de una conexión SSL con un certificado firmado por la CA del grupo Renault hacia la parte servidora del TOE (O.Comunicación).
T.DocumentoFalso	El entorno operacional garantiza que los responsables de la administración de los sistemas centrales son confiables, y que la custodia de la PKI también descansa en personal confiable (OE.Personal y OE.PKI). Esto hace que no sea posible conectar equipos que se comuniquen con el TOE y envíen a este documentos falsos a ser firmados. El TOE por su parte garantiza que la comunicación con cualquier entidad externa se llevará a cabo a través de un canal securizado que hace uso de certificados firmados por la CA del grupo Renault (O.Comunicación).
T.ModificaDocumento	El entorno operacional garantiza que los responsables de la administración de los sistemas centrales son confiables, y que la custodia de la PKI también descansa en personal confiable (OE.Personal y OE.PKI). Esto hace que no sea posible acceder a la información que el TOE almacena usando conexiones que no utilicen certificados firmados por la CA de Renault, ya que el TOE únicamente acepta conexiones SSL que utilicen certificados firmados por la CA del grupo Renault (O.Comunicación). Además, el entorno operacional garantiza la integridad de la totalidad de los datos involucrados en procesos completos de firma, por lo que su modificación no es posible. (OE.Integridad).

39 Justificación de suficiencia para los objetivos del entorno:

OSP.Auditoría	El TOE genera auditoría. (O.Auditoría).
OSP.ProcesoFirma	El TOE implementa funcionalidad para garantizar que

	únicamente los documentos que estén firmados por todos los intervinientes serán enviados a ASF para su sellado de tiempo y su firma digital. (O.ProcesoFirma y OE.FirmaDigital).
OSP.Gestión	El TOE provee funcionalidad de gestión de los procesos completos de firma. (O.Gestión).

40 Justificación de suficiencia para las hipótesis:

A.Configuración	Esta hipótesis está directamente cubierta con (OE.Configuración).
A.Físico	Esta hipótesis está directamente cubierta con (OE.Físico).
A.Personal	Esta hipótesis está directamente cubierta con (OE.Personal).
A.Autenticación	Esta hipótesis está directamente cubierta con (OE.Autenticación).
A.Integridad	Esta hipótesis está directamente cubierta con (OE.Integridad).
A.PKI	Esta hipótesis está directamente cubierta con (OE.PKI).
A.DMZ	Esta hipótesis está directamente cubierta con (OE.DMZ).
A.Generación	Esta hipótesis está directamente cubierta con (OE.Generación).

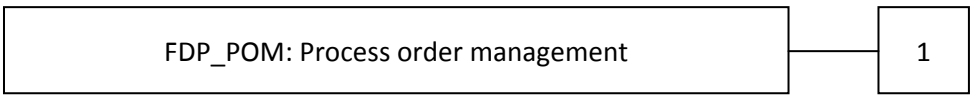
5 Definición de Componentes Extendidos

5.1 Process order management (FDP_POM)

5.1.1 Family behaviour

41 This extended family defines the management of the order that a process must follow before its end. A complete process can be formed by some steps, and restrictions on these steps regarding the order they must be executed. Process order management (FDP_POM) specifies the process steps and their ordering restrictions.

5.1.2 Component levelling



42 FDP_POM.1 Define the process containing restrictions on its steps, and the order these steps must follow to satisfy the restrictions.

Management: FDP_POM.1

43 The following activities should be considered for the management functions in FMT:

a) Actions that derive in changes of the current process status, such as the process termination or the process status update.

Audit: FDP_POM.1

44 The following actions should be auditable if FAU_GEN Security audit data generation is in the PP/ST:

a) Minimal: Successful requests to perform an operation on a process managed by the TOE.

b) Basic: All requests to perform an operation on a process managed by the TOE.

c) Detailed: The specific steps that each process managed by the TOE reach.

FDP_POM.1 Process order management

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FDP_POM.1.1 The TSF shall ensure that the steps involved in the process [assignment: *name of the process*] are executed following the order [assignment: *sorted list including the steps involved in the process and its order*].

5.2 Intra-TOE Trusted Information (FDP_ITI)

5.2.1 Family behaviour

45 This extended family defines the management of the user data communication between a server and a client belonging to the TOE. Such Intra-TOE communication maintains confidentiality, integrity and mutual authentication of both parts involved.

5.2.2 Component levelling

46 FDP_ITI.1 Requires that the TSF provide a trusted communication between two different parts of the TOE.

Management: FDP_ITI.1

47 There are no management activities foreseen.

Audit: FDP_ITI.1

48 There are no auditable events foreseen.

FDP_ITI.1 Intra-TOE Trusted Information

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_ITI.1.1 The TSF shall provide a trusted user data communication management between [assignment: *parts involved in the communication*] that provides assured identification of its end points and protection of the data exchanged from modification or disclosure.

6 Requisitos de Seguridad

6.1 Requisitos funcionales de Seguridad del TOE

6.1.1 Class FAU: Security audit

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [**selection:** **minimum**] level of audit; and

c) [**assignment:** **the following Audited Events**

- **Creación del proceso de firma (preparación del TOE para iniciar el proceso de firma, con el almacenamiento de datos en la base de datos interna, asignando un identificador)**
- **Gestión del proceso de firma (registro de la captura de firmas de intervinientes y la integración de dichas firmas,)**
- **Fin del proceso de firma (registrar la finalización del proceso de firma. Permite identificar el momento en que se borran de la base de datos todas las trazas del proceso).**

].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment:** **ninguna**].

Nota de aplicación: Existe personal de RCI Banque encargado de la gestión del almacenamiento utilizado por los registros de auditoría generados por el TOE. Cuando la cantidad de almacenamiento utilizado por los mismos está cercano al máximo configurado, dicho personal lleva a cabo una copia de seguridad de los registros de auditoría en un almacenamiento externo y se libera espacio en el almacenamiento original.

6.1.2 Class FDP: User data protection

FDP_POM.1 Process order management

FDP_POM.1.1 The TSF shall ensure that the steps involved in the process [**assignment: proceso completo de firma**] are executed following the order [**assignment:**

(1) Firma de los documentos involucrados en el proceso completo de firma por parte de todos los intervinientes.

(2) Envío de los documentos firmados por todos los intervinientes a la plataforma ASF.

].

FDP_ITI.1 Intra-TOE Trusted Information

FDP_ITI.1.1 The TSF shall provide a trusted user data communication management between [**assignment**: **el Applet de la parte cliente y la parte servidora del TOE**] that provides assured identification of its end points and protection of the data exchanged from modification or disclosure.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**selection: deallocation of the resource from**] the following objects: [**assignment: los siguientes objetos:**

- **Documentos involucrados en cualquier proceso completo de firma**
- **Descriptores de los procesos completos de firma**
- **Firmas de intervinientes involucradas en cualquier proceso completo de firma**

].

Nota de aplicación: Los datos a ser borrados están almacenados en una Base de Datos Oracle, y se eliminarán de ella cuando se alcance una de las siguientes condiciones:

- Se termina un proceso de firma: Todos los intervinientes involucrados en el proceso completo de firma han firmado los documentos involucrados en el mismo, y éstos se mandan a ASF para su firma digital y sellado de tiempo.
- Se cancela un proceso de firma mediante los botones proporcionados por la interfaz.
- Se pospone un proceso completo de firma: Alguno pero no todos los intervinientes en un proceso de firma han firmado los documentos involucrados en el mismo, y se pospone el resto de firmas para un momento futuro.
- Un contrato permanece inactivo durante un periodo de tiempo configurado en el servidor.

6.1.3 Class FMT: Security management

FMT_SMF.1 Specification of Management Functions

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

- **Insertar firma de intervinientes en documentos incompletos a través del lector de la tarjeta digitalizadora.**
- **Cancelar proceso de firma.**
- **Finalizar proceso completo de firma.**
- **Posponer proceso de firma.**

].

6.1.4 Justificación de los Requisitos de Seguridad del TOE

6.1.4.1 Cobertura

	O.Comunicación	O.Borrado	O.ProcesoFirma	O.Auditoría	O.Gestión
FAU_GEN.1				X	
FDP_POM.1			X		
FDP_ITI.1	X				
FDP_RIP.1		X			
FMT_SMF.1					X

6.1.4.2 Suficiencia

O.Comunicación	Este objetivo se implementa con el requisito FDP_ITI.1 ya que es el encargados de proporcionar un canal de comunicación que mantiene confidencialidad, integridad y autenticación de los extremos entre la parte cliente y la parte servidora del TOE.
O.Borrado	El requisito FDP_RIP.1 es quien implementa la funcionalidad asociada a este objetivo, ya que se encarga de borrar toda la información de los procesos completos de firma de la base de datos interna del TOE cuando se termina, se cancela o se pospone un proceso completo de firma.
O.ProcesoFirma	Este objetivo se ve satisfecho a través del requisito FDP_POM.1 el cual impone unas restricciones de orden al proceso completo de firma que obligan a que los documentos sean firmados por todos los intervinientes antes de que dichos documentos sean enviados a ASF.

O.Auditoría	El TOE genera auditoría siguiendo las pautas marcadas en el requisito FAU_GEN.1, por lo que este objetivo se ve satisfecho.
O.Gestión	El TOE proporciona funcionalidad de gestión y visualización del proceso completo de firma y sus datos asociados a través de FMT_SMF.1.

6.1.4.3 Justificación de Dependencias

	Dependencia	Satisfecha/Justificación
FAU_GEN.1	FPT_STM.1	El entorno operacional es el encargado de proporcionar el sellado de tiempo para los registros de auditoría.
FDP_POM.1	FMT_SMF.1	Satisfecha
FDP_ITI.1	Ninguna	NA
FDP_RIP.1	Ninguna	NA
FMT_SMF.1	Ninguna	NA

6.2 Requisitos de Garantía

49 El desarrollo y evaluación del TOE se realizará conforme al siguiente nivel de garantía:

- EAL1 con los aumentos ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2.

ASE_CCL.1 Conformance claims

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

ASE_INT.1 ST introduction

Developer action elements:

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

Content and presentation elements:

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

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

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

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

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

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

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

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

ASE_OBJ.2 Security objectives

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

ASE_REQ.2 Derived security requirements

Developer action elements:

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

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

Content and presentation elements:

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

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

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

ASE_REQ.2.4C All operations shall be performed correctly.

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

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

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

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

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

ASE_SPD.1 Security problem definition

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

ASE_TSS.1 TOE summary specification

Developer action elements:

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

Content and presentation elements:

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

ADV_FSP.1 Basic functional specification

Developer action elements:

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

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

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

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

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

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

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

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

ALC_CMC.1 Labeling of the TOE

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

ATE_IND.1 Independent testing - conformance

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

6.2.1 Justificación de los Requisitos de Garantía

50 La elección del nivel de garantía EAL1 con los aumentos ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2 se realiza por considerar que se ajusta al nivel de garantía que el cliente requiere teniendo en cuenta las características del entorno sobre el que opera el TOE.

7 Especificación resumida del TOE

7.1 FAU_GEN.1 Audit data generation

51 El producto genera una trazabilidad de todas las operaciones realizadas para cubrir, fundamentalmente, el proceso de firma de documentos desde cada puesto cliente (todas las firmas realizadas o si el proceso se canceló, la firma de empresa con sellado de tiempo, etc.), y otras operaciones adicionales, tales como la recuperación del documento custodiado en la Plataforma ASF. Todas estas operaciones se escriben a modo de log en el fichero C:\WebSphere\logs\RCILocal.log.

7.2 FDP_POM.1 Process order management

52 El proceso principal que el producto debe asegurar es la firma de los documentos.

1. Tratamiento de la solicitud de firma de documentos, incluidos en un mensaje (metadatos) enviada desde un cliente. En nuestro caso, desde @baco.
2. Muestra los datos resumen de los documentos a firmar, junto con la identificación de los intervinientes; y todo ello incluido en el mensaje.
3. Para cada interviniente, se activará el dispositivo de captura de firma (tableta) para que éste pueda realizar la firma.
4. Incorporación de la firma de cada interviniente en todos los documentos a firmar, previa visualización y confirmación.
5. Capturada la firma de todos los intervinientes, el proceso concluirá pasando cada documento a la Plataforma ASF para la integración del certificado del apoderado y del sello de tiempo.
6. Los documentos cifrados por la Plataforma ASF y recuperados por el TOE son devueltos al cliente para continuar con su proceso.
7. Si todos los intervinientes no están presentes en el acto, el proceso de firma puede interrumpirse, pasando el control al cliente, indicando que el proceso de firma no se ha completado. En cualquier otro momento, y desde el cliente, se puede lanzar la reanudación del proceso, comenzando desde el punto inicial.
8. El proceso puede ser interrumpido voluntariamente por el usuario, cancelando el proceso, cediendo el control al cliente.

53 El TOE interacciona vía una serie de interfaces (WS o flujos https) con otros productos o aplicaciones, para llevar a cabo el proceso de firma de documentos : a) con unas

aplicaciones clientes (@baco y Archivo Digital), donde los usuarios se han debido autenticar previamente, para lanzar los procesos y recoger la respuesta; b) con unos sistemas auxiliares (la Plataforma ASF y los dispositivos de firma –tableta-) para procesar toda la información y realizar el proceso de firma de documentos, propiamente dicho.

54 Asimismo, el TOE pone a disposición una aplicación Web, a partir de la cual el comercial va a dirigir los distintos pasos para capturar las firmas de los clientes, integrarlas dentro del documento final y generar un documento final único y seguro.

7.3 FDP_ITI.1 Intra-TOE Trusted Information

55 La comunicación entre el Applet que corre en la parte cliente del TOE y la parte servidora del mismo (situado en la red DMZ) transfiere información sensible, y por tanto, debe de ser protegida ante posibles ataques. Para ello, se hace uso del protocolo SSL con certificados firmados por la CA de Renault. El uso de este protocolo implica un cifrado de la información, un control de integridad de la misma, y además, una autenticación de las partes involucradas en ella.

7.4 FDP_RIP.1 Subset residual information protection

56 El producto almacena en una base de datos temporal la información (mensaje, incluido los pdfs de los documentos a firmar) necesaria para hacer la firma de los documentos. Esta información se elimina completamente: bien, al finalizar todo el proceso de firma; bien, cuando se abandona el proceso durante una firma parcial de intervinientes o si se cancela todo el proceso.

7.5 FMT_SMF.1 Specification of Management Functions

57 El producto realiza las siguientes operaciones de gestión:

- Operaciones de captura de la firma de los distintos intervinientes mediante la tableta de digitalización de firma. Desde la aplicación Web del TOE vía varios botones (Firmar, Reintentar, Confirmar) se controla los dispositivos externos de captura de firma; una vez realizada la firma, el TOE recoge el control con la información de la firma del interviniente.

- Operación de finalización del proceso completo de firma, donde todos los documentos firmados por los intervinientes será cifrados con la firma del certificado del apoderado de empresa más un sello de tiempo.

- Operación de finalización parcial del proceso, donde no todos los intervinientes han firmado. Los documentos estarán parcialmente firmado. La información del estado del proceso de firma se vuelve al cliente para que éste pueda relanzarlo en otro momento.

- Operación de cancelación del proceso, donde se pasa el control al cliente, borrando todas las evidencias de los procesos realizados en el producto. La aplicación Web del TOE dispone de un botón en la interfaz de usuario para cancelar completamente el

proceso. Al cancelar el proceso se elimina la persistencia de datos y documentos del contrato en la base de datos temporal.