Comunidad de Madrid | CONSEJERÍA DE TRANSPORTES, MOVILIDAD E INFRAESTRUCTURAS

CONSORCIO TRANSPORTES MADRID

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL "SERVICIO DE VIRTUALIZACIÓN DE TARJETAS DE TRANSPORTES BASADO EN EL MODELO DE SISTEMAS OPERATIVOS" DEL CONSORCIO REGIONAL DE TRANSPORTES DE MADRID

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL "SERVICIO DE VIRTUALIZACIÓN DE TARJETAS DE TRANSPORTES BASADO EN EL MODELO DE SISTEMAS OPERATIVOS" DEL CONSORCIO REGIONAL DE TRANSPORTES DE MADRID

ÍNDICE

1. ANTECEDENTES

Desde al año 2018, todo el billetaje de la Comunidad de Madrid, se basa en tarjetas sin contactos, tanto en tarjetas personales (TTP), como en tarjetas anónimas (Multi).

Las tarjetas de transportes del Consorcio Regional de Transportes Públicos Regulares de Madrid -en adelante CRTM- (TTP o Multi) utilizan el chip DesFire cuya propiedad intelectual ostenta en exclusiva la entidad NXP Semiconductors Lo que implica que todos los actores del sistema (fabricantes, operadores de transportes y redes de carga), tienen adaptada la tecnología (hardware y software), siguiendo especificaciones del CRTM, que a su vez, se basa en especificaciones técnicas de bajo nivel, del chip DesFire de NXP.

En consecuencia, la evolución del billetaje de la Comunidad de Madrid debe orientarse a la reutilización de todo lo existente, que otorga dos ventajas: la primera, ahorro de inversión por todos los actores del sistema implicados, y segundo, facilidad de integración al no tener que incorporar nuevos componentes hardware, aunque si es necesario añadir algún elemento de software. Por ello, se concibe como evolución natural del sistema de Billetaje Inteligente del Transporte (BIT) actual, el teléfono móvil, orientado la virtualización de la tarjeta de transportes. Un procedimiento por el cual un teléfono se comportará como una tarjeta física de transporte público, como si fuera una tarjeta TTP o una tarjeta Multi.

2. TÉCNICAS DE VIRTUALIZACIÓN

En el momento de la redacción de este pliego, las estrategias posibles para virtualizar una tarjeta de transportes en un smartphone se pueden clasificar en base al actor que finalmente ejecuta en el teléfono el proceso de introducir la tarjeta virtualizada, de forma que tenemos tres posibles planteamientos:

- A.- El operador de telefonía, utilizando su SIM telefónico, concretamente el SE (elemento seguro) que incorpora su SIM.

- B.- El fabricante del sistema operativo (SO) que es capaz de buscar el lugar más seguro del que dispone el smartphone del usuario; unas veces ofuscando y otras, además guardando parte de la virtualización de la tarjeta en algún SE disponible. **Esta opción: modelo de sistemas operativos, determina el ámbito de este contrato.**

- C.- El fabricante del teléfono, el cual dispone también de uno o varios SE en la circuitería de sus smartphones

3. OBJETO DEL CONTRATO

El objeto de este documento es establecer el alcance y las condiciones de carácter técnico que han de regir la contratación por Procedimiento Abierto de los trabajos necesarios para el "SERVICIO DE VIRTUALIZACIÓN DE TARJETAS DE TRANSPORTE BASADO EN EL MODELO DE SISTEMAS OPERATIVOS". En principio la estructura de la tarjeta, el mapa de memoria, obedece a la tarjeta de transporte del CRTM. Pero en este pliego entendemos el concepto de tarjeta en su sentido más amplio (el equivalente en el mundo de las tarjetas físicas a la licencia del chip) que se puede estructurar según los intereses del CRTM, pudiendo evolucionar su estructura de ficheros de aplicaciones o incluso un monedero, transformando la tarjeta de transportes del CRTM, en una tarjeta de movilidad como servicio o en una tarjeta ciudadana. **La licencia del chip virtual se orienta por dispositivo y no por el número de UIDs virtuales asociado al mismo smartphone**

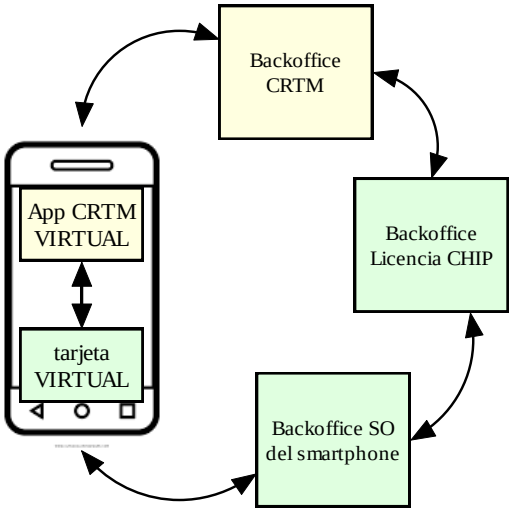
El CRTM indica en este pliego los principales casos de uso.

También es objeto de este documento definir los procedimientos de ejecución y seguimiento de los trabajos contemplados.

El alcance del contrato abarca desde la integración con el BackOffice del CRTM hasta la emulación de tarjeta de transportes del CRTM en el terminal del usuario, por lo que este contrato abarca el proceso informático seguro que garantiza la emulación de las tarjetas de transportes del CRTM en el entorno de los smartphone.

Para una mejor comprensión del alcance. El siguiente esquema indica en color verde, la parte del proyecto de responsabilidad del adjudicatario de este contrato.

Responsabilidad del adjudicatario



Sin embargo, el epígrafe 6.4 de este documento contempla también, si fuera necesario, un refuerzo en las zonas de color amarillo (CRTM)

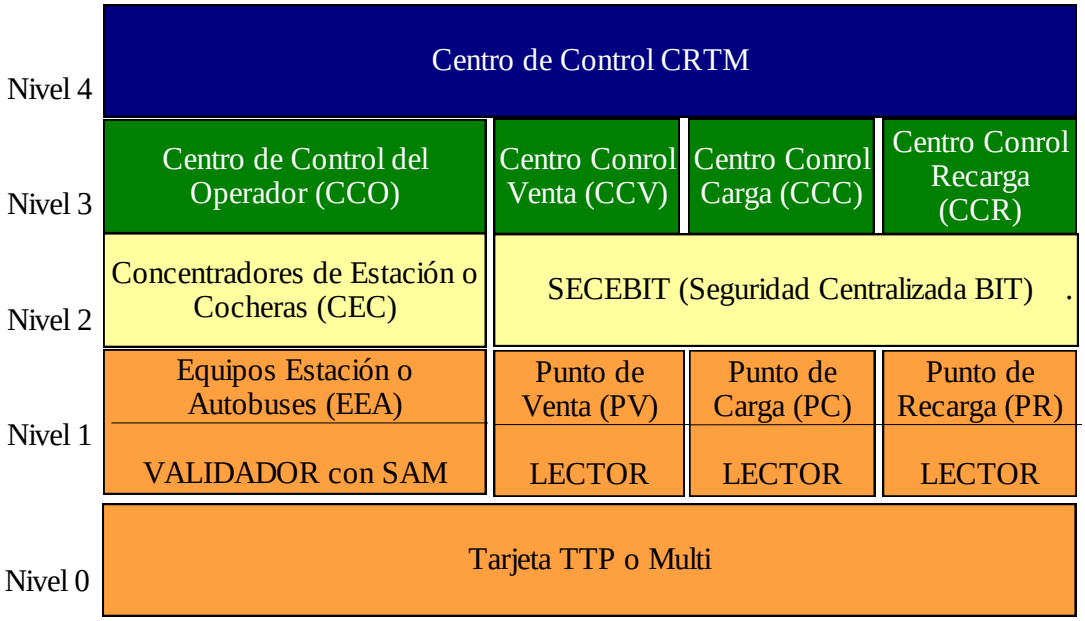
El CRTM tiene previsto que esta solución coexista en el futuro, con otras técnicas de virtualización que puedan aparecer o evolucionen de las ya existentes, y que lógicamente, no queda dentro del ámbito del presente contrato.

4. Descripción general del Sistema BIT

El sistema BIT (Billetaje Inteligente del Transporte) es la evolución del sistema basados en billetes magnéticos hacia sistemas basados en tarjetas sin contacto, ya sean estas últimas, físicas o virtuales. Este aparente simple cambio de soporte, ha supuesto, profundos cambios técnicos y funcionales, en todos los niveles del transporte público de la Comunidad de Madrid.

El sistema BIT, concibe la tarjeta sin contacto como un contenedor de títulos de transporte, cuyo chip contiene toda la información necesaria, que permite operar directamente con dispositivos de validación, carga e inspección. Previamente, las tarjetas han requerido de las fases de pre-personalización y personalización

Para explicar el flujo de información entre el CRTM y cualquier otro actor nos hemos centrado, por simplificar, en operadores de transportes, pero con cualquier otro actor el proceso es similar. El intercambio de información se realiza en ambos sentidos. Cuando se detecta la tarjeta en los validadores hasta que llega a la autoridad de transportes, es decir, al Consorcio Regional de Transportes de Madrid (CRTM).



El usuario entra en el operador de transportes y sitúa la tarjeta sin contactos (ISO 14443-A) sobre la antena del validador, esta es una operación muy rápida, del orden de milisegundos. En este instante se activa el proceso que consiste en la comprobación de que al menos uno de los títulos que residen en la tarjeta sin contacto es válido en dicho instante. Este proceso se realiza enviando tramas de información por radiofrecuencia, (aclaramos que no se envían datos personales, ya que ni siquiera existen en el interior de la tarjeta, de esta forma, el CRTM garantiza el cumplimiento de la RGPD). Independientemente del resultado del envío y/o recepción de tramas por radiofrecuencia, se genera un registro de la operación, al que llamaremos registro de validación o transacción. Este registro de validación, que es firmado digitalmente por el dispositivo de seguridad (SAM), incluye, entre otros datos; el número de serie de la tarjeta, el resultado de validación, la fecha y hora. El proceso descrito forma parte del nivel 0/1.

Cuando el validador o el subconcentrador (concentrador de validadores de una batería o vestíbulo) puede comunicar con el concentrador (nivel 2) le envía todos los registros de validación. Todos los concentradores de estación o cocheras envían sus registros al centro de control del correspondiente operador de transportes (CCO, nivel 3)

Para la transmisión de la información de validación entre el nivel 3 (CCO) y el nivel 4 (CRTM) se elegirá una ventana de tiempo que garantice la velocidad de transmisión de los procesos, normalmente en modo nocturno, aunque pueden darse comunicaciones diurnas. El canal entre el nivel 3 y 4, es seguro, pues se ha utilizado FTP sobre SSH. Por este canal, se transmitirán desde el nivel 3 al nivel 4 toda la información correspondiente a los registros de validación generados en los operadores de transporte a lo largo del día. Por otro lado, el CCO descargará del CRTM la información necesaria para actualizar su sistema. La información que genera el CRTM es de naturaleza muy diversa; tarifas, configuraciones, listas de tarjetas no permitidas, etc...

Cuando el operador, en conexión, comprueba que hay una nueva lista de tarjetas no permitidas procederá a descargarla, una vez recibido en su sistema

verificará la firma electrónica de la lista para autentificarla, e inmediatamente, el operador distribuirá la lista de tarjetas no permitida por su red, es decir, enviando cada fichero desde el nivel 3 al 1, por lo tanto, llegando hasta cada validador del operador. Así, por ejemplo, si el CRTM genera una lista en la que una nueva tarjeta sin contactos ha sido incluida, el operador detectará el cambio y actualizará su lista a nivel 3 para después transmitirla al nivel 2. Cada concentrador de estación (nivel 2) enviará la nueva lista a los distintos subconcentradores, transmitiendo esta información a todos los posibles equipos intermedios hasta que la reciban todos los validadores (nivel 1). De manera que, al día siguiente, cuando la tarjeta afectada intente entrar por cualquier operador de transportes se le denegará el acceso, ya que, el validador comprobará que la tarjeta está en lista no permitida informando de esta situación y bloqueando el paso.

Bloquear el acceso de una tarjeta a cualquier operador de transportes es una operación que prueba la capacidad defensiva del CRTM, mecanismo que se materializa en listas no permitidas de tarjetas. Esto es, una relación de tarjetas no admitidas.

Como se ha dicho, los operadores envían información de validaciones al CRTM, pero también lo hace los fabricantes de tarjetas, la red de ventas y también la red de carga/recarga. Todas estas fuentes de información alimentan a una base de datos (BBDD) donde se registra cada número de serie de cada tarjeta. Es decir, se dispone de una BBDD actualizada donde figuran todas las tarjetas que ha vendido el CRTM. De manera, que cualquier tarjeta que haya accedido a cualquier operador debe figurar en la BBDD del CRTM. En caso de que algún actor pusiera alguna tarjeta en circulación sin autorización del CRTM la tarjeta quedaría bloqueada en menos de 48 horas por el sistema.

Hablar de seguridad en el Sistema BIT implica hablar de la seguridad inherente a la tarjeta sin contactos TTP y/o Multi, de la seguridad en la custodia de las claves y de la seguridad de las comunicaciones e información de transacciones (como ya hemos explicado).

La tarjeta TTP y Multi, se ha implementado sobre DESFire de NXP, este chip incorpora mecanismos de seguridad que se basa en tres pilares, estos son:

- Número de serie único (garantizado por el fabricante)

- Generador de números aleatorios FIPS 140-2
- Algoritmo criptográfico triple DES (3DES) y AES

Como norma general, cada vez que se accede a la TTP o Multi, ya sea para realizar una lectura o una escritura, es necesario un proceso de autentificación. El proceso de autentificación usado por las tarjetas del CRTM es el denominado como AUTENTIFICACIÓN MUTUA EN TRES PASOS que es el de mayor seguridad que soporta el DESFire. En el sistema BIT este modo se mejora con la seguridad añadida de dispositivos de seguridad como son SAM (Security Access Module) y/o HSM (Host Security Module). Estos módulos de seguridad son elementos de custodia de claves, además incorporan comandos especiales de seguridad, con una propiedad tremendamente interesante, que es la de no permitir en ningún caso que las claves salgan del dispositivo, aunque internamente se opere con ellas para obtener la clave de sesión, que si se entrega al lector, para acceder a un determinado fichero en un momento determinado.

Antes de comenzar el proceso de autentificación, hay que realizar algunas tareas previas:

- Cuando una tarjeta TTP o Multi, entra en el campo magnético del lector, se le induce una corriente que activa la tarjeta y responde con su número de serie. El lector recibe este dato y se lo reenvía al dispositivo de seguridad. En este momento todos los dispositivos están preparados para trabajar con la tarjeta.

- El programa del lector necesita leer o escribir en un determinado fichero, pero lo único que conoce es el índice de la clave que utilizará, es decir, solo conoce la posición de las claves únicas que tiene cada tarjeta. El lector le comunica a la tarjeta y al dispositivo de seguridad algo del estilo “vamos a trabajar con la clave 5”. En definitiva, el lector coordina el trabajo, pero no entra en los detalles.

Una vez establecido el índice de la clave con la que se va a trabajar, comentamos el proceso de autentificación que explicamos de forma general. La tarjeta TTP o Multi genera un número aleatorio (mediante FIPS 140-2) y lo cifra con el algoritmo 3DES utilizando el valor de la clave del índice, que conoce la tarjeta TTP o

Multi. Todo esto, cifrado, se envía al programa del lector, este es el primer paso. Pero el lector no conoce clave alguna y no entra en esos detalles (el CRTM no desea que los integradores conozcan las claves) y por esto se lo reenvía al dispositivo de seguridad; a un SAM o a un HSM.

El dispositivo de seguridad, internamente, descifra el dato al que aplica una serie de operaciones para generar un segundo dato y también otro nuevo número aleatorio. Finalmente se cifra la concatenación de ambos números con la clave que indica el índice y el resultado se envía al lector. El lector hace eco de esta información hacia la TTP o Multi. Ahora la tarjeta descifra la información y obtiene ambos números. Si la tarjeta TTP (o Multi) comprueba que uno de ellos, después de deshacer las transformaciones necesarias, es el número original que envió, entonces significa que el otro extremo conoce su clave para trabajar. Este es el segundo paso.

Seguidamente la tarjeta TTP (o Multi) hace una serie de transformaciones al número que genero el dispositivo de seguridad y lo cifra con 3DES, este es el paso 3 y el último. El dato cifrado se envía al lector que a su vez lo reenvía al dispositivo de seguridad. El dispositivo de seguridad comprueba si este número aleatorio es el número que él generó en el paso 1, pero previamente tiene que transformarlo. Si esto es así, queda autentificado el otro extremo también y el dispositivo de seguridad proporciona al lector la clave de sesión.

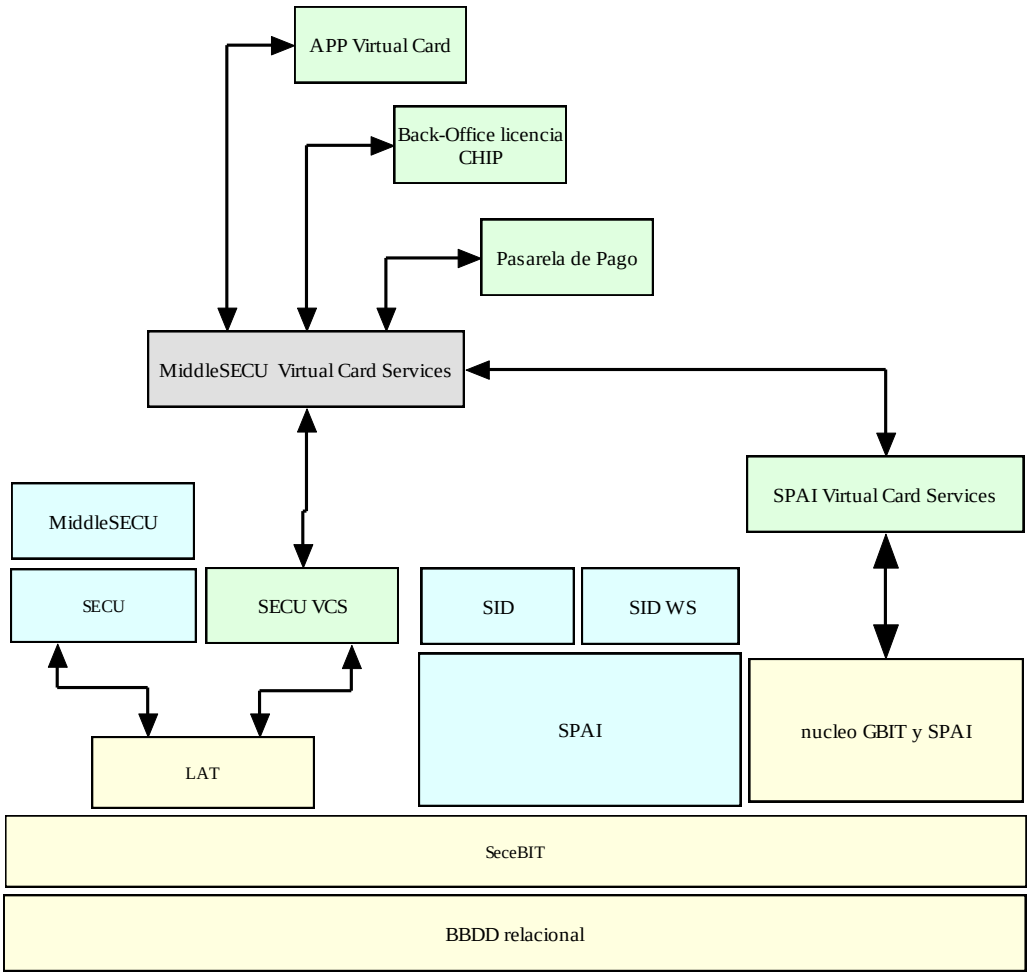
El sistema BIT, es también, un generador de datos. Cada proceso asociado a la vida de las tarjetas del CRTM (prepersonalización, personalización, carga, validación e inspección) genera una o varias transacciones que se envían al SID (Servidor de Intercambio de Datos) y que es procesado mediante el SPAI (Sistema de Procesamiento Automático de Información). El gran volumen de datos recibido se ha formalizado en un enorme modelo de datos en BBDD relacional, que a su vez, en la actualidad, alimenta a GBIT, herramienta que permite resolver cualquier problema a los usuarios de la TTP y Multi, y que se utiliza en la Oficinas de Gestión (OOGG) del CRTM.

El proceso de virtualización debe ser coherente con el sistema BIT actual.

5. Back office técnico del CRTM

En los esquemas de los casos de uso que se detallan más adelante, se entenderá como Back-Office del CRTM la entrada a la capa denominada “MiddleSECU Virtual Card Services”, que abreviadamente identificaremos como MiddleSECU-VCS. Por lo tanto, el adjudicatario de este contrato se integrará con MiddleSECU-VCS

El esquema de los elementos del Back Office del CRTM a alto nivel, en relación con esta licitación, será el siguiente:



La capa que interactúa con la “app virtual card”, será el MiddleSECU-VCS, un servicio middleware que se interpone entre cada uno de los elementos necesarios para lograr la virtualización, esto es, entre la “app virtual card” (app de carga), el SECU-VCS (del CRTM), el SPAI-VCS (que permitirá conectividad con GBIT del CRTM), la pasarela de pagos (contratada por concurso público por el CRTM) y el Back-office licencia del CHIP (este contrato)

El MiddleSECU-VCS gestionará con seguridad y garantías las operaciones de devolución asociadas a problemas al proceso de carga.

El LAT (Lógica Aplicación Transporte) permite realizar toda la lógica de las aplicaciones de prepersonalización, personalización, carga, validación ligera e inspección. Conviene aclarar, que el LAT es independiente de la tecnología de base del chip utilizada en el título de transporte, pues la capa, que se ocupa del nivel del chip, es la parte conocida como SECU (implementa los comandos de seguridad) o SECU-VCS

6. Trabajos a realizar

Los servicios que se solicitan en este contrato deben dimensionarse, por parte del adjudicatario, para garantizar un nivel de servicio de disponibilidad no inferior al 99.9% (casi TIER III).

6.1.- Casos de uso

La virtualización de la tarjeta debe ser un espejo de la tarjeta física, un usuario de la tarjeta virtual pueda hacer lo mismo que los usuarios de las tarjetas físicas, aunque mejorando la experiencia del usuario. En este canal se busca que el usuario desde su terminal móvil pueda realizar cualquier gestión o resolver una incidencia, sin necesidad de desplazarse a una oficina de gestión.

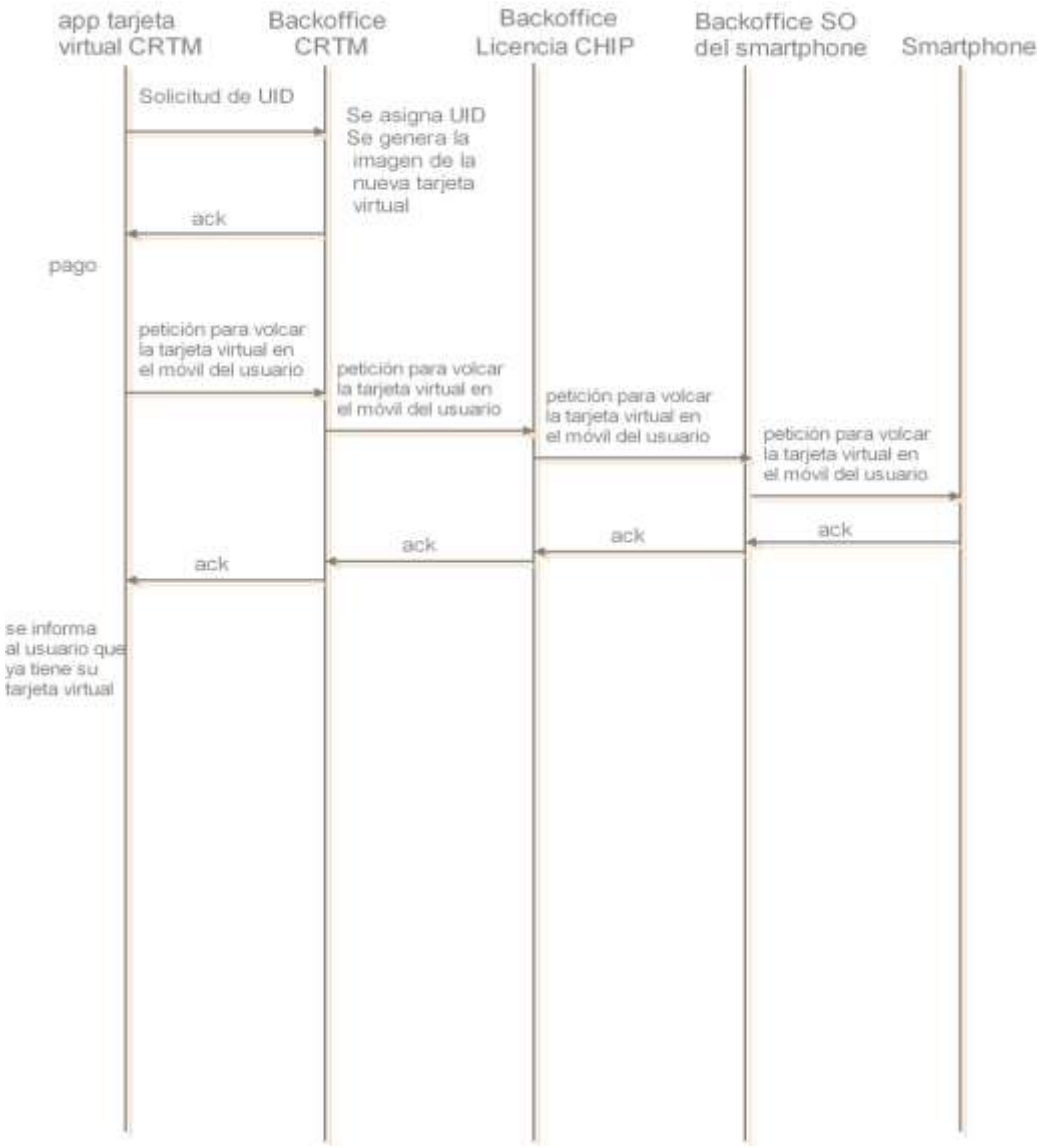
La virtualización basada en HCE (host card emulation), para el caso de Android, modelo (SO); requiere que la **app de carga/recarga de tarjetas virtuales del CRTM,** acceda a la virtualización de forma indirecta. Es decir, la app del CRTM no accederá directamente a la parte del teléfono donde reside la tarjeta virtual, sino que lo hará indirectamente, a través de los diferentes backoffice que forman parte del sistema.

Téngase en cuenta también, que el CRTM ya dispone de un contrato que cubre la PASARELA DE PAGOS.

Los CASOS de USO identificados, son los siguientes:

6.1.1. COMPRA/ ALTA TARJETA VIRTUAL ANONIMA

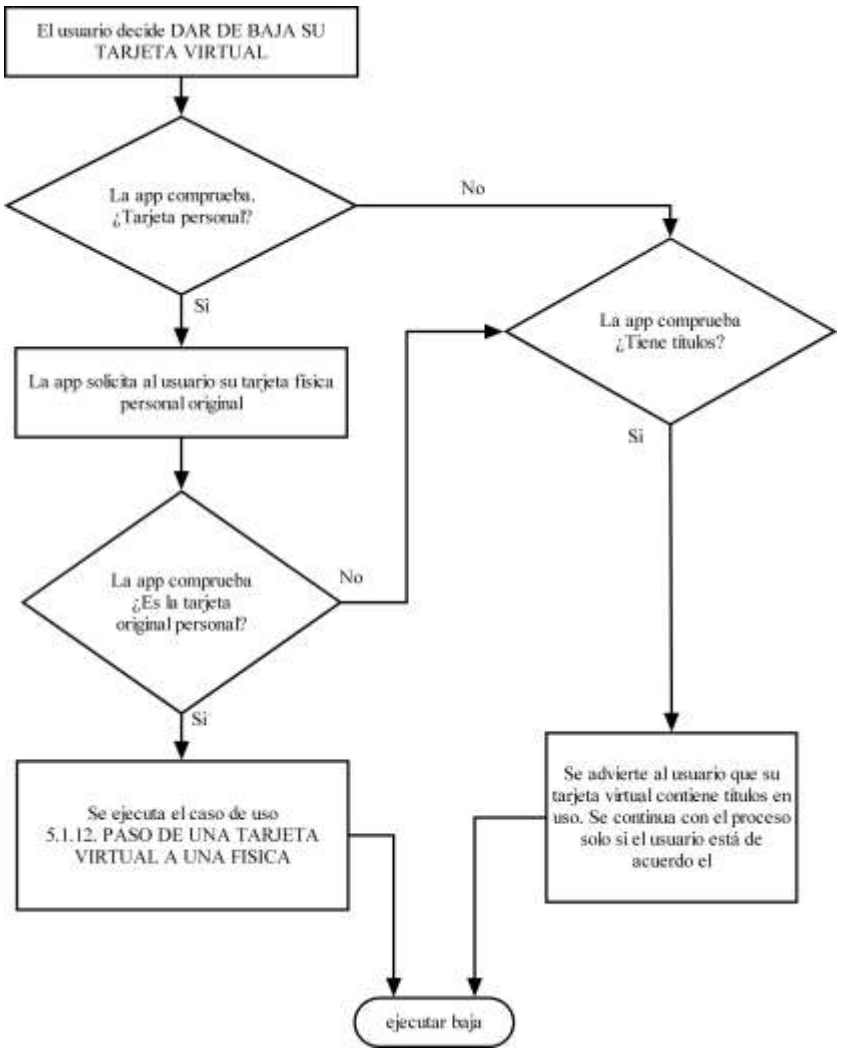
Es el proceso en el que el usuario adquiere la tarjeta virtual. Este sistema puede ser gratuito o con coste para el usuario final. El siguiente esquema, representa el cambio de mensajería entre la app y los diferentes backoffice hasta alcanzar la parte segura emulada en el teléfono



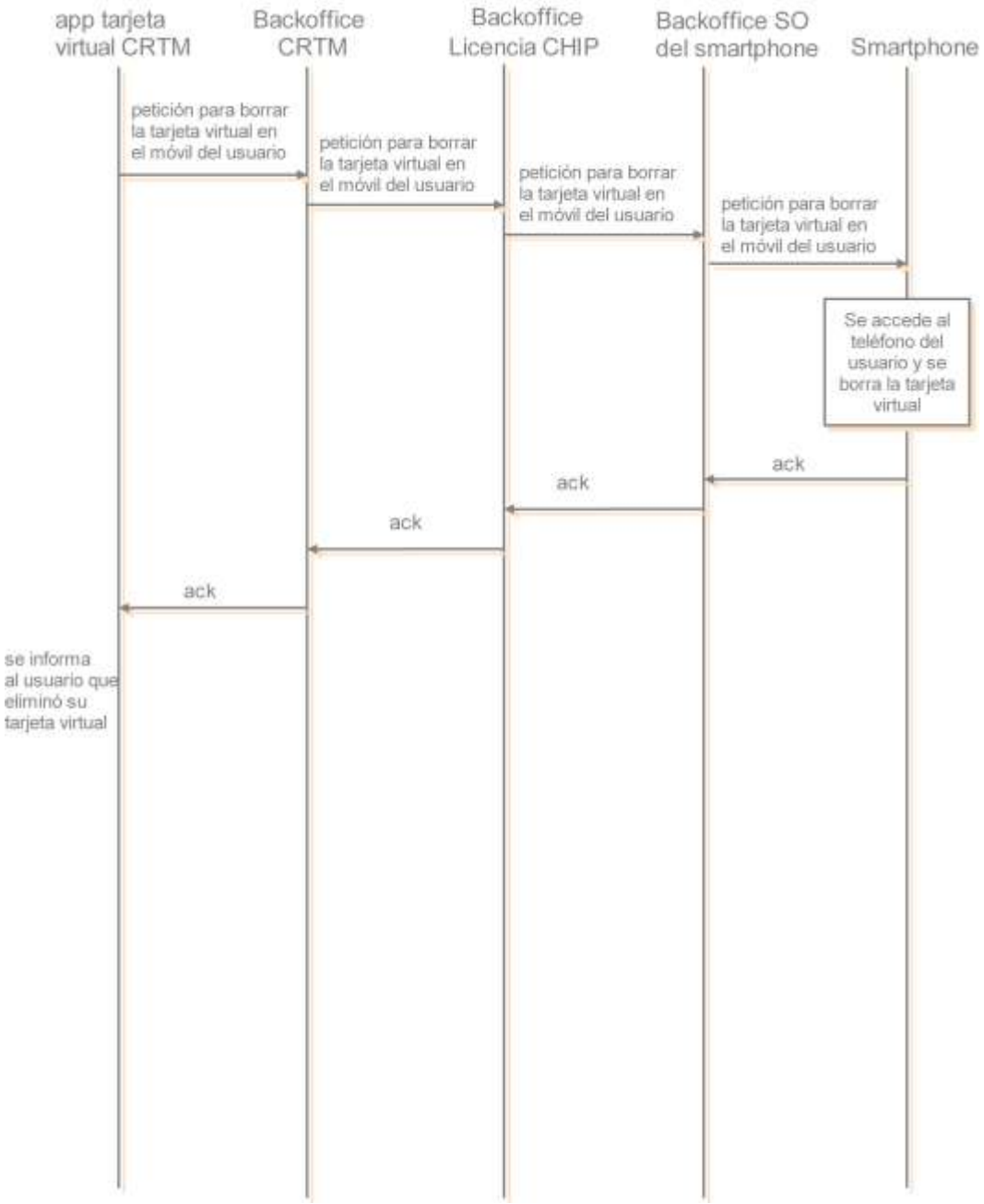
6.1.2. BAJA voluntaria por el usuario TARJETA VIRTUAL anónima o personal

Cuando el usuario lo decida, podrá optar por dar de baja su tarjeta virtual, ya sea anónima o personal.

Para el caso de tarjetas personales, esta funcionalidad normalmente vendrá precedida de la funcionalidad de PASO DE UNA TARJETA VIRTUAL A UNA FISICA, aunque pudiera ser que el usuario renuncie a esta operación. La función que será solicitada por el usuario desde la app. Se representa en el siguiente diagrama:



A nivel de integración entre los diferentes backoffice que intervienen en el proceso, se detalla gráficamente el intercambio de mensajes previstos (para el caso más sencillo), en el cual participa el adjudicatario de este contrato.



6.1.3. COMPRA/ ALTA TARJETA VIRTUAL PERSONAL

Este caso de uso requiere un proceso previo no incluido en este contrato correspondiente a la identidad del usuario.

Se trata, por un lado, de autentificar al usuario, y por otro, de verificar todos los requisitos de descuento que solicite, como por ejemplo, descuento por ser joven, tercera edad, familia numerosa, discapacidad, etc…

Una vez, autentificado el usuario y comprobado los descuentos a los que tiene derecho se ejecutará el proceso definido en 6.1.1, con la salvedad que el mapa de memoria que representa la tarjeta virtual incorporará si los tuviera, los perfiles y colectivos, asociados a descuentos.

Por lo tanto, se soportará en este contrato la posibilidad de poder comprar tarjetas virtuales con diferentes mapas de bytes o estructuras de ficheros

6.1.4. LECTURA DE SALDO

Se entiende por lectura de saldo, la operación que se realiza con la tarjeta de transportes en un terminal adecuado (en este caso el smartphone) para informar al usuario sobre su contenido; títulos cargados, periodos de validez, etc...

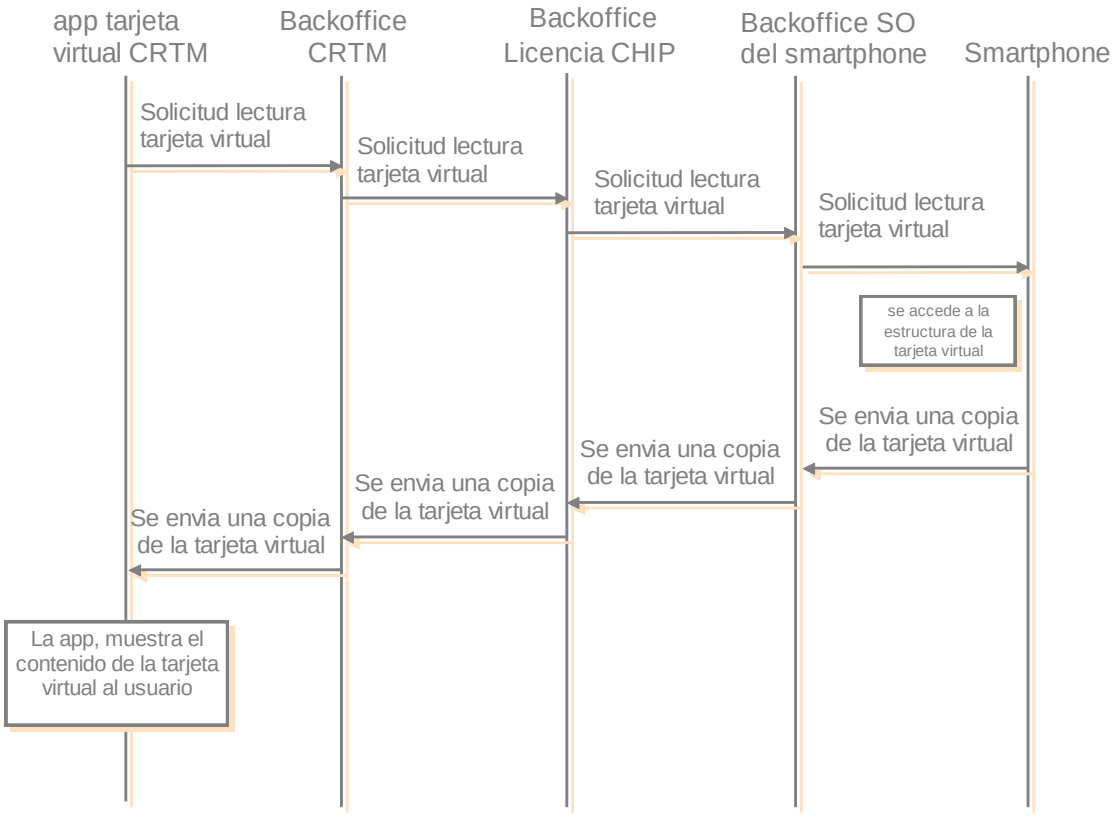
El flujo de la operación de saldo, es el siguiente:

1. El propio terminal lee la información de configuración que tiene almacenada en su memoria.
2. Se comprueba que todos los campos necesarios están definidos. En el caso de resultado negativo, el terminal informa que queda fuera de servicio y la ejecución del programa vuelve a empezar
3. Se ejecuta el comando de lectura de datos de tarjeta sin contacto. Si el terminal no recibe ninguna respuesta, es decir si no hay tarjeta, la ejecución del programa vuelve a empezar.
4. Se leen los datos de la tarjeta.
5. Se comprueba que los datos generales de la tarjeta (como periodo de validez, estado de activación etc.) son correctos. En caso de resultado negativo, se informa el usuario sobre el resultado de procesamiento del contenido de la tarjeta y la ejecución del programa vuelve a empezar.
6. Se presentan el contenido de los títulos de la tarjeta. En realidad, se presentan los parámetros más importantes de cada título: nombre, periodo de validez o viajes disponibles para temporales o multiviajes respectivamente, para carga y recarga. Además, se genera un registro con la información más importante sobre la tarjeta.
7. Después de un determinado periodo de tiempo sin ninguna actividad, el terminal deja de mantener los datos presentados en su pantalla y la ejecución del programa vuelve a empezar

Para que la app, pueda realizar la función descrita con anterioridad, es preciso disponer de un caso de uso para recuperar la estructura de ficheros de una tarjeta virtualizada (RAW), este caso de uso se utilizará previamente como paso inicial a operaciones más complejas como pueden ser:

6.1.4. COMPRA DE TITULO VIRTUAL
6.1.7. PASO DE UNA TARJETA VIRTUAL A UNA FISICA
6.1.8. PASO DE UN MOVIL A OTRO
6.1.12. ASISTENCIA EN REMOTO

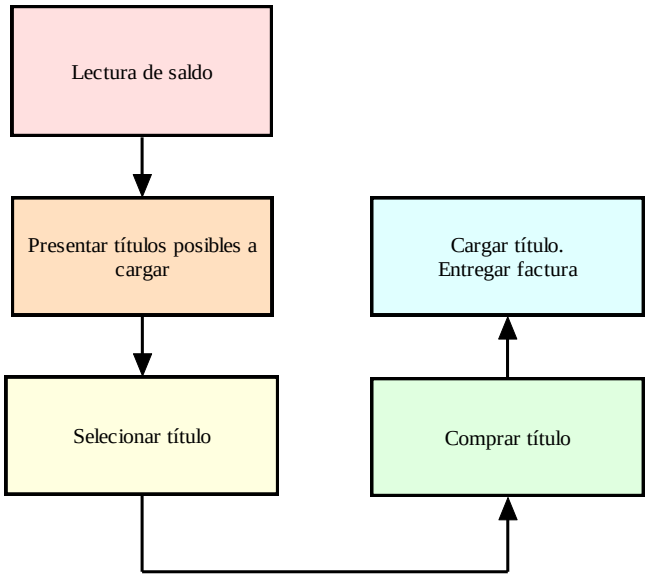
El flujo siguiente muestra un posible intercambio de mensajería, en la situación más sencilla.



6.1.5. COMPRA DE TITULO VIRTUAL

Está función permite al usuario adquirir un título para cualquiera de las tarjetas comerciales del CRTM (personales, anónimas, azul, etc..). Como carga/recarga de título se define la operación que se realiza en un terminal adecuado para introducir un título nuevo en la tarjeta (carga), o ampliar (recarga) la validez de otro anteriormente introducido (que puede, en la actualidad, ser válido o no).

El diagrama de flujo siguiente ilustra el funcionamiento por bloques de la compra de un título a alto nivel



Para ejecutar el primer bloque del esquema (lectura de saldo) se utilizará el caso de uso descrito en 6.1.4.

El siguiente bloque, aunque la lógica no afecta al adjudicatario de este contrato, posiblemente requiera la información resultante. El mencionado bloque permite seleccionar el título que el usuario puede adquirir, en base a las reglas de coexistencia que tiene prevista el sistema actual. La tarjeta personal es la más compleja, pues en ella hay una alta probabilidad de que se almacenen varios títulos simultáneos.

A continuación, se describen las situaciones de convivencia de títulos que no presentan dificultadas de elección para los equipos de validación y que han sido recogidas en los documentos del proyecto BIT con anterioridad. Seguidamente se muestra los criterios de coexistencias:

Coexistencia tipo A: solo para títulos de tipo multiviajes o sencillos tanto en tarjeta TTP como MULTI

Podrán coexistir 1,2, o 3 títulos de tipo sencillo o multiviajes con sus recargas correspondientes siempre que no compartan operadores de validez.

Podrán coexistir 1,2, o 3 títulos de tipo sencillo o multiviajes con sus recargas correspondientes siempre que, si existe coincidencia en los operadores de validez, no exista ningún solapamiento de zonas.

Compartiendo operador y/o zona de validez los títulos Metrobus/sencillos, MetroSur/sencillos, MetroNorte/sencillos, MetroEste/sencillos y TFM/sencillos podrán coexistir entre sí y con bonobuses disjuntos y con 10 viajes MLO/sencillos.
El billete combinado ferroviario no podrá convivir con ningún otro billete ferroviario incluyendo el Metrobus y el 10 viajes MLO/sencillos. Si podrá hacerlo con bonobuses disjuntos.

Nota: existe un título de carácter temporal que es posible alojarlo en una tarjeta MULTI y es el título turístico, se regirá por las reglas de coexistencia de temporales junto a multiviajes/sencillos que se describen en el Bloque B. En fase 1, no podrá coexistir con ningún otro tipo de título como se verá más adelante.

TABLA RESUMEN (C/R→ Carga/Recarga ; 10V/sen→ 10 viajes/sencillos)

Tarjeta MULTI					
COEXISTENCIAS	METRONORTE, METROSUR,METROESTE, TFM,METROBUS	BONOBUSES	MLO	COMBINADO FERROVIARIO	TURISTICOS
METRONORTE, METROSUR,METROESTE, TFM,METROBUS	C/R 10V/sen	SI. Si hay 2 bonobuses deben ser disjuntos	SI	NO	NO
BONOBUSES	SI. Si hay 2 bonobuses deben ser disjuntos	C/R 10V. Si hay más de uno deben ser disjuntos	SI. Si hay 2 bonobuses deben ser disjuntos	SI. Si hay 2 bonobuses deben ser disjuntos	NO
MLO	SI	SI. Si hay 2 bonobuses deben ser disjuntos	C/R 10V/sen	NO	NO
COMBINADO FERROVIARIO	NO	SI. Si hay 2 bonobuses deben ser disjuntos	NO	C/R 10V/sen	NO
TURISTICOS	NO	NO	NO	NO	Carga/recarga Nota: En primera fase no permiten coexistencia con ningún otro título

Coexistencias de tipo B: introduciendo en la ecuación los títulos de tipo abono anuales/ 30 días en tarjetas TTP.

Una tarjeta TTP solo puede albergar un título de tipo abono, 30 días o anual (o turístico si así se decidiese en alguna fase). El título de tipo abono está priorizado en validación frente a los de tipo multiviajes/sencillo.
No es obligatorio tener al menos un título de tipo abono en una TTP ni hay que reservar un contenedor de la tarjeta TTP para ello.

Una TTP puede comportarse a efectos de coexistencia como una MULTI si no tiene título de tipo abono.

Un abono tarifa plana joven, 30 días/anual (valido para todas las zonas incluyendo E1 y E2) puede coexistir con cualquier combinación de títulos 10viajes/sencillos con dos precauciones.

- Si son bonobuses deben ser disjuntos y en este caso cualquier combinación siempre está englobada dentro del abono.
- Si es el título 10 viajes /sencillo combinado ferroviario el otro ya no puede ser ferroviario incluyendo el Metrobus y MLO.

Un abono tarifa plana 3 edad, 30 días/anual (válido hasta la zona C2) puede coexistir con cualquier combinación de títulos 10viajes/sencillos con dos precauciones.

- Si son Bonobuses deben ser disjuntos entre sí, y/o estar englobados totalmente por el abono o ser disjuntos totalmente del abono.
- Si es el título 10 viajes /sencillo combinado ferroviario el otro ya no puede ser ferroviario incluyendo el Metrobus y MLO.

Un abono de la Zona A, 30 días/anual puede coexistir con cualquier combinación de títulos 10viajes/sencillos con dos precauciones.

- Si son bonobuses deben ser disjuntos entre ellos (siempre son disjuntos del abono zona A)
- Si es el título 10 viajes /sencillo combinado ferroviario el otro ya no puede ser ferroviario incluyendo el Metrobus y MLO.

Resto de abonos zonales/interzonales, 30 días/anual pueden coexistir con cualquier combinación de títulos 10viajes/sencillos con dos precauciones.

Si son Bonobuses deben ser disjuntos entre ellos, y/o estar englobados totalmente por el abono o ser disjuntos totalmente del abono. Dicho de otra forma, no puede existir ningún solapamiento de zonas entre los Bonobuses y con los abonos dos opciones o están totalmente englobados dentro del abono o son totalmente disjuntos.

Si es un 10 viajes/sencillo combinado ferroviario no podrá con otro ferroviario, además debe estar totalmente englobado por el abono o ser totalmente disjunto.

Por ejemplo, Abono normal 30 días B3+ sencillo combinado ferroviario+ Bonobus B1-B2

TABLA RESUMEN

Tarjeta TTP								
COEXISTENCIAS	Abonos tarifa plana	Abonos zona A	Resto de Abonos zonales o interzonales	METRONORTE, METROSUR, METROESTE, TFM, METROBUS	BONOBUSES	MLO	COMBINADO FERROVIARIO	TURISTICOS
Abonos tarifa plana	C.R	NO	NO	SI	SI. Si hay dos bonobuses deben ser disjuntos	SI	SI, en caso de no haber otro ferroviario	NO
Abonos zona A	NO	C.R	NO	SI	SI. Si hay dos bonobuses deben ser disjuntos	SI	NO	NO
Resto de Abonos zonales o interzonales	NO	NO	C.R	SI	Si hay más de un bonobus deben ser disjuntos. Abono debe englobarlos totalmente o ser disjunto con el abono totalmente	Abono debe englobar Totalmente o ser disjunto totalmente	Si, en caso de no haber otro ferroviario y el Abono debe englobar Totalmente o ser totalmente disjunto	NO
METRONORTE, METROSUR,METROESTE	SI	SI	SI	C.R 10V/sen	SI. Si hay dos bonobuses deben ser disjuntos	SI	NO	NO
BONOBUSES	SI. Si hay dos bonobuses deben ser disjuntos	SI. Si hay dos bonobuses deben ser disjuntos	Si hay más de un bonobus deben ser disjuntos. Abono debe englobarlos totalmente o ser disjunto con el	SI. Si hay dos bonobuses deben ser disjuntos	C.R 10V Si hay más de uno deben ser disjuntos	SI. Si hay dos bonobuses deben ser disjuntos	SI. Si hay dos bonobuses deben ser disjuntos	NO
MLO	SI	SI	Abono debe englobar Totalmente o ser disjunto totalmente	SI	SI. Si hay 2 bonobuses deben ser disjuntos	C.R 10V/sen	NO	NO
COMBINADO FERROVIARIO	SI	NO	Abono debe englobar Totalmente o ser disjunto totalmente	NO	SI	NO	C.R 10V/sen	NO
TURISTICOS	NO	NO	NO	NO	NO	NO	NO	NO

Nota: respecto al resto de operaciones relacionadas con la carga, en especial, una operación de canje venta o modificación de las zonas tarifarias de un título. La realización de esta operación solo se permitirá si tras la ejecución de la misma no se rompen las reglas de coexistencia que se han definido.

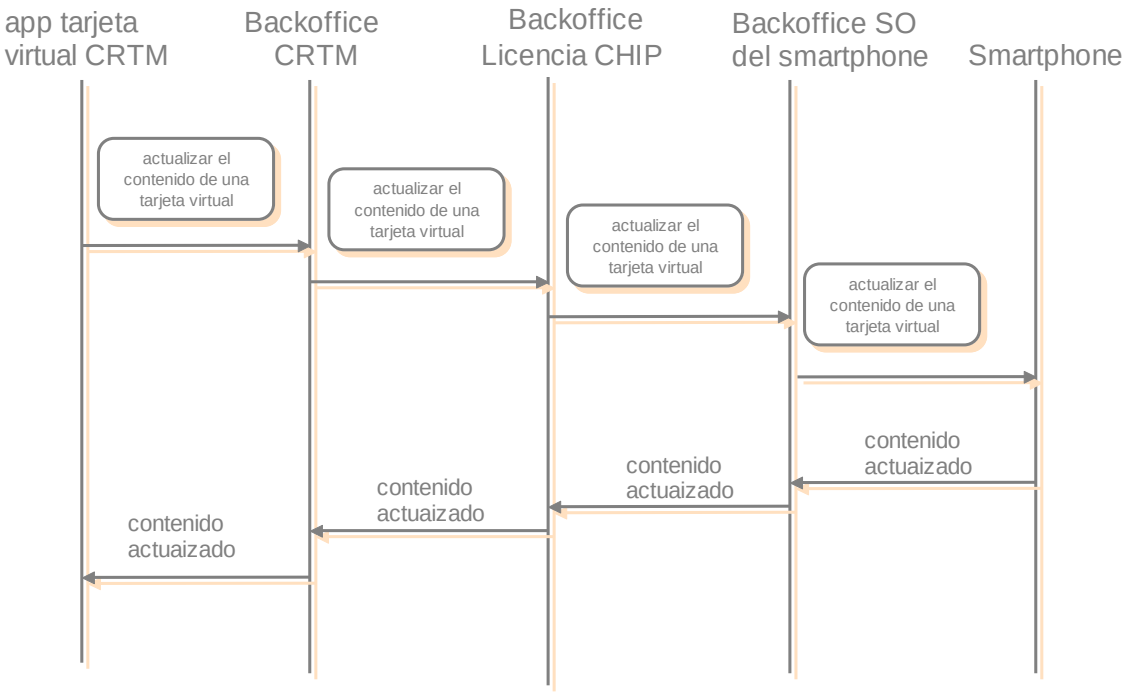
El bloque amarillo (seleccionar título), permitirá seleccionar el título en base a las reglas establecidas en las coexistencias de tipo A y B, como si fuese una tarjeta física.

Sin embargo, en la modalidad de tarjeta virtual, se mejorará, con la posibilidad de cargar un título incompatible (uno o varios) con las coexistencias de tipo A y B. La solución técnica para esto puede ser tener dos UIDs virtuales en el mismo smartphone (**como se ha dicho a lo largo de este contrato se entiende que la licencia se computa por dispositivo y no por el numero de UIDs virtuales que tiene un mismo dispositivo**)

Si el título adquirido es incompatible estará en otra tarjeta virtual, por lo que será obligatorio, por parte del usuario determinar, de entre los títulos incompatibles, cuál de ellos se utilizará por defecto, es decir, cuál de ellos será activo en el momento de la validación. Por ello el usuario podrá seleccionar, en cualquier momento, la tarjeta virtual de transportes que desea utilizar.

El siguiente paso es la compra del título (bloque verde) que la app lo gestionará mediante la PASARELA DE PAGOS DEL CRTM. Si todos los procesos anteriores son correctos, se carga el título de transportes (bloque azul) en la tarjeta virtual, además de facilitar una factura al usuario.

El caso de uso para el adjudicatario de la carga de un título es en realidad, actualizar en el smartphone una representación del contenido de la tarjeta. El siguiente flujo representa la integración desde la app de la carga del CRTM hasta el teléfono móvil del usuario.



6.1.6. COEXISTENCIA DE TÍTULOS INCOMPATIBLES CONDUCIDO POR EL USUARIO

Como se indicaba en el caso anterior el sistema BIT, define los títulos compatibles que pueden coexistir en la misma tarjeta simultáneamente sin presentar problemas de elección en los algoritmos de validación. Quedando excluidos de la posibilidad de cargar en la misma tarjeta de transportes, aquellos títulos, que siendo aceptados en el mismo operador de transportes, coinciden en tipo de título (abono, multiviajes, etc..), y en zona a de validez, pues en estos casos, el algoritmo de validación no puede discernir cual de ambos títulos desea el usuario utilizar. Sin embargo, la app que gestiona la tarjeta virtual, permitirá al usuario gestionar estos casos.

Para ello, el algoritmo de carga dispondrá de la posibilidad de ofrecer títulos cuya coexistencia requiere selección por parte del usuario. Esta información se almacenará en una tarjeta virtual nueva, lo que implica, que al tener el usuario varias

tarjetas virtuales de transporte, será responsabilidad del mismo activar la tarjeta a utilizar antes de acceder al transporte público.

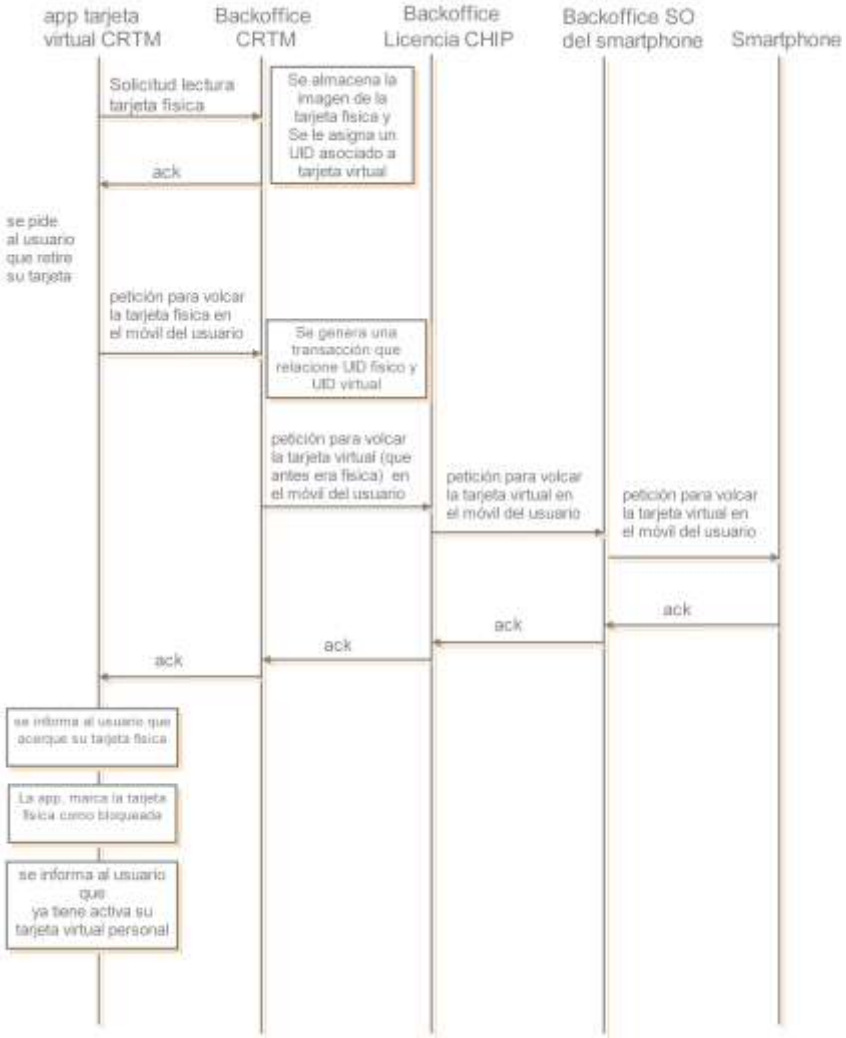
Para soportar esta funcionalidad, el adjudicatario tendrá que desarrollar procedimientos para que un smartphone tenga activa varias UIDs simultáneamente, de forma que el MiddleSECU-VCS podrá enviar mensajes al Back-office licencia del CHIP del tipo siguiente:

a.- Lista de UIDs disponibles para el smartphone X
b.- Añadir nueva UID y mapa de memoria Z, para el smartphone X

6.1.7. PASO DE UNA TARJETA FISICA A UNA VIRTUAL

El universo de tarjetas de transporte público personal, es de aproximadamente 4,5 millones. Este caso de uso tiene aplicación sobre este conjunto de tarjetas.

La funcionalidad de transferir una tarjeta personal de transporte, que previamente el CRTM ya ha revisado, garantiza que el usuario final continuará disfrutando de sus beneficios en el entorno virtual. Este proceso debe garantizar que solo se habilitará una de las tarjetas, la virtual o la física.

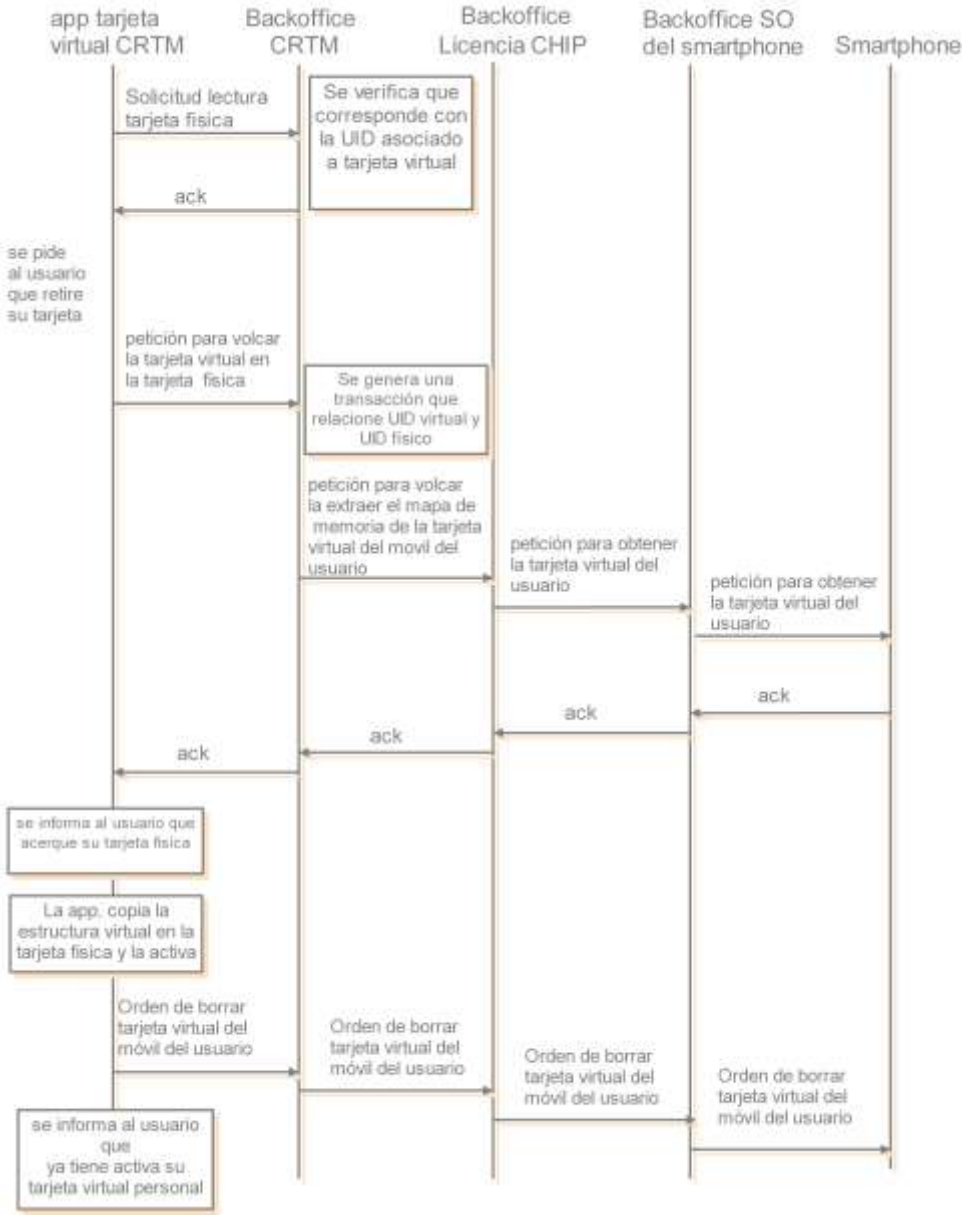


Es importante aclarar, que el proceso de virtualizar la tarjeta requerida de alguna información adicional del usuario final (como por ejemplo, número de teléfono) que permita, en el futuro, ejecutar el caso de uso de PASO DE UN MOVIL A OTRO o el caso de uso de COEXISTENCIA DE TÍTULOS INCOMPATIBLES.

6.1.8. PASO DE UNA TARJETA VIRTUAL A UNA FISICA

Este caso, sólo se soportará para tarjetas personales.

Para que la app pueda lanzar este proceso, previamente debe comprobar que la tarjeta física de la que parte, es la misma que se utilizó en el proceso inverso, es decir en el caso de uso “PASO DE UNA TARJETA FISICA A UNA VIRTUAL”. El MiddleSECU-VCS del CRTM, con quien se conecta la app de carga, realizará para esta comprobación, llamadas a el SPAI-VCS.



6.1.9. PASO DE UN MOVIL A OTRO

Es una realidad, que el usuario en un momento dado decida renovar su smartphone por otro más moderno, lo que implica por parte del usuario afrontar un proceso de migración. En el caso de la tarjeta virtual del CRTM, el adjudicatario de este contrato deberá habilitar el procedimiento para permitir dicha funcionalidad.

Mediante algún procedimiento, que se describirá con detalle en la ejecución del proyecto, la virtualización estará asociada al número de teléfono móvil del usuario, por lo tanto, no es necesario tener operativos ambos móviles para transferir una tarjeta virtual de un teléfono a otro. Sin embargo, será necesario previamente, desde el terminal antiguo, ejecutar en la app del CRTM, una opción que permita almacenar la tarjeta virtual, transitoriamente en el backoffice del CRTM y borrarla del smartphone antiguo del usuario, para posteriormente, recuperar dicha tarjeta virtual en el nuevo smartphone del usuario

6.1.10. PÉRDIDA/ROBO DE UN MOVIL Y OBTENCION DE UNA NUEVA TARJETA VIRTUAL

En la situación, en que el caso de uso de “PASO DE UN MOVIL A OTRO” no se pueda ejecutarse, debido a que el usuario no disponga del smartphone antiguo por un robo o extravío. El proceso generará una incidencia que se podrá resolver de la siguiente manera:

a.- El usuario tendrá que notificar la pérdida al CRTM de su teléfono, indicando la información de su número de teléfono y/o UID virtual.

b.- El CRTM comprobará si es correcto, y en cuyo caso se ejecuta el punto c

c.- El backoffice del CRTM lanzará una orden de borrado de la tarjeta UID virtual

d.- Si “d” no tiene éxito la UID virtual se envía a LNS

e.- Se reconstruirá, en el backoffice del CRTM, el contenido de la UID virtual perdida o robada, y se le asigna una nueva UID, obteniendo una UID’ virtual.

f.- Se envía la nueva UID’ virtual, junto con el contenido de la tarjeta virtual al nuevo móvil del usuario, que recupera su tarjeta virtual tal y como estaba antes de la perdida/robo de su anterior terminal.

6.1.10. Cambio de estructura de la tarjeta

La estructura de la tarjeta del CRTM actual, se compone de una serie de ficheros, organizados por el tipo de contenido:

1. Fichero de datos generales FEdg.
2. Fichero de datos FEdp que almacena información de facturación
3. Fichero de activación y perfiles FEap.
4. Ficheros de datos relacionados con los títulos FEdt.
5. Ficheros históricos de accesos con los títulos FEha.
6. Fichero de registro de transacciones FErt.
7. Fichero de validez de la aplicación y de títulos para inspección FEvl.
8. Fichero de consumo FEcs.

El objetivo de la generación de varios ficheros es controlar el acceso a los datos con distintas necesidades de seguridad. Por ejemplo, un validador no debe tener acceso de escritura en los ficheros de los datos relacionados con los títulos.

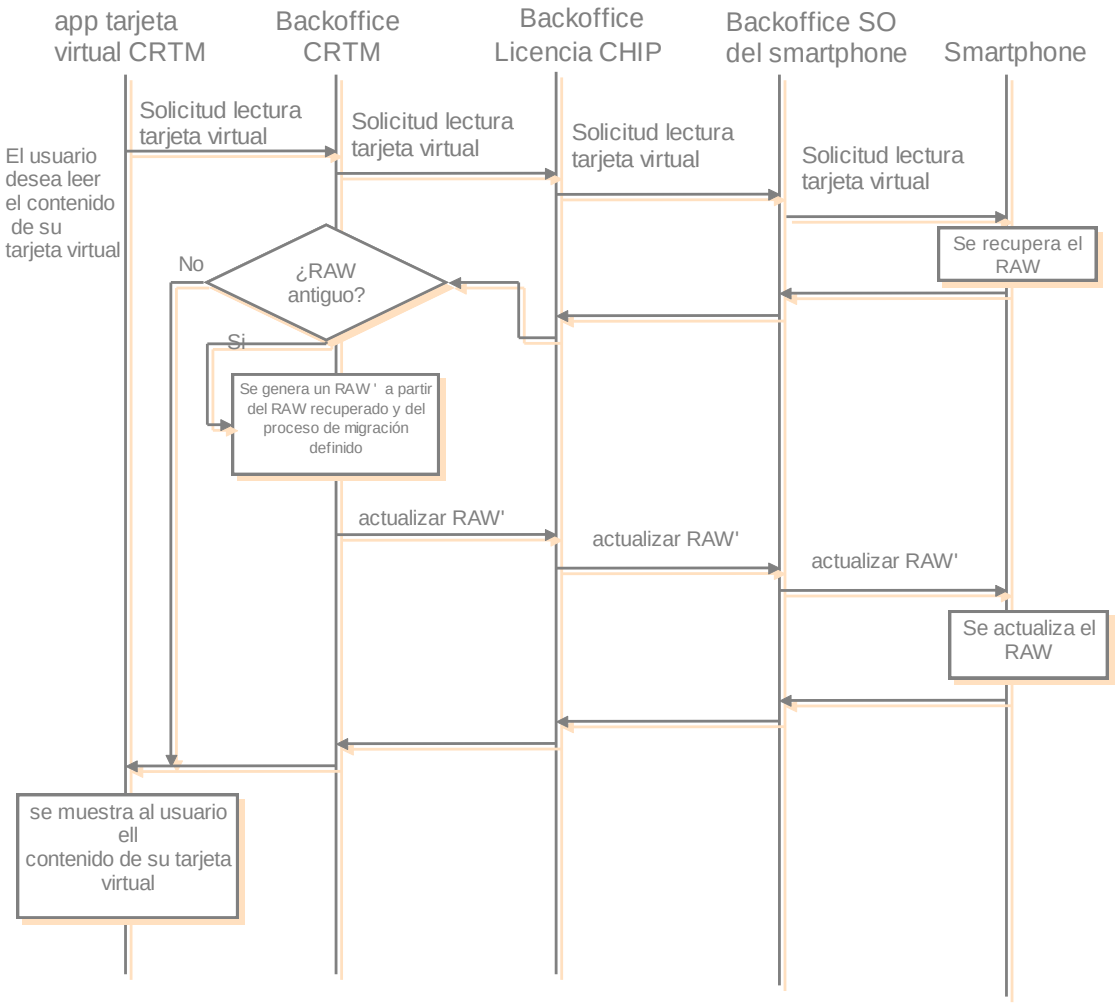
La tarjeta de del CRTM incluye los siguientes ficheros, en su mapa de memoria:

- Fichero Maestro [**FMtj**] que es único, obligatorio y representa la raíz de la estructura de ficheros.
- Fichero Dedicado [**FDat**] que contiene la aplicación que se usará para el transporte para todos los tipos de transacciones.
- Fichero Elemental [**FEdg**] de datos generales de la aplicación.
- Fichero Elemental [**FEdp**] de datos de facturación
- Fichero Elemental [**FEap**] de datos de activación y perfiles.
- Fichero elemental [**FEdt**] de datos del título de transporte (se permiten hasta tres títulos, luego se incluyen tres ficheros de este tipo).
- Fichero elemental [**FEha**] de datos históricos de accesos (se permiten hasta tres, luego se incluyen tres ficheros de este tipo).
- Fichero elemental [**FErt**] de registro de transacciones.
- Fichero elemental [**FEcs**] de consumo.
- Fichero elemental [**FEvl**] de validez de aplicación y títulos.

Pero es previsible, que en el entorno virtual, la tarjeta del CRTM evolucione con mayor facilidad que en el mundo físico. Por ello, el adjudicatario de este contrato tendrá que soportar la utilización de varias estructuras de tarjetas virtuales del CRTM que pueden

coexistir en un mismo momento, pues se requiere un rango temporal en un proceso de migración de una estructura antigua a otra, más moderna.

La tarjeta del CRTM podría evolucionar para incorporar un monedero, una aplicación añadida coexistiendo, o incluso, podría evolucionar hacia una tarjeta ciudadana (incluyendo servicios sanitarios, transportes, etc…). Sea como fuere, el caso de uso debe soportar la migración del RAW. El siguiente esquema muestra un ejemplo de migración de raw.



6.1.11. GESTION

El adjudicatario de este concurso deberá facilitar la capa de servicios que permita al CRTM, bajo demanda, poder conocer la vida de una tarjeta.

Algunos de los servicios previstos, aunque pueden evolucionar o requerirse alguno más, son los siguientes:

- smartpone asociado a una UID
- lista de UIDs de un smartpone
- Estado de la UID
- Borrado de UID
- Bloquear un título determinado de un UID
- Desactivar UID
- Activar un título determinado de un UID que previamente se había bloqueado
- Reactivar UID

6.1.12. LISTA de TARJETAS NO PERMITIDAS

Estas listas, conocidas en el sistema BIT como LNS, indican los UIDs de tarjetas que bloquean un título o incluso todos los títulos para el uso del transporte público. Estas listas se publican en el SID del CRTM cada 24h y todos los actores del sistema (operadores de transportes, redes de ventas, etc…) lo actualizan en sus infraestructuras

Poder bloquear desde el CRTM una tarjeta virtual o un título de una tarjeta virtual, se utilizará un proceso activado desde MiddleSECU-VCS.

Los pasos para seguir serán del estilo siguiente:

1.- El SPAI-VCS envía al MiddleSECU-VCS la lista LNS de UIDs de tarjetas virtuales, con acciones de bloquear un determinado título o la tarjeta completa, para cada UID
2.- Por cada UID, el MiddleSECU-VCS envía un mensaje a back-office licencia del CHIP para recuperar el raw de la tarjeta virtual de un UID concreto
3.- Mediante la integración que tiene el back-office licencia del CHIP con el back-office del SO, se recupera el raw de la tarjeta virtual soliciatada, que finalmente se envía al MiddleSECU-VCS
4.- El MiddleSECU-VCS reenvía el raw recibido y la acción a realizar de bloquear un determinado título o la tarjeta completa al SECU-VCS que a su vez se lo entrega al LAT.
5.- EL LAT modifica el raw generando un raw' con el bloqueo indicado en la LNS y lo hace llegar al MiddleSECU-VCS
6.- El MiddleSECU-VCS envía un mensaje a back-office licencia del CHIP para recuperar actualizar con el raw' de la tarjeta virtual
7.- El back-office licencia del CHIP envía esta información al back-office del SO, que a su vez lo actualiza en el smarphone.

6.1.13. ASISTENCIA EN REMOTO

La Atención al Público será más cercana al usuario, gracias a la flexibilidad y acercamiento que puede ofrecer el ámbito tecnológico de la virtualización de tarjetas de transporte.

En este contexto, cuando el usuario ya posea una (o varias) tarjeta/s virtual/es en uso y tenga un problema con una de ella, como por ejemplo, que la tarjeta virtual deje de funcionar correctamente en un momento dado, será posible solucionarlo a distancia desde el back-office del CRTM.

Para ello, en el ámbito de este contrato, se tendrá que facilitar al CRTM la posibilidad de recuperar del smartphone del usuario la imagen que representa su tarjeta de transporte, además de poder enviar de nuevo, la imagen de la tarjeta de transportes modificada y corregida al smartphone del usuario

Es decir, el primer flujo es el necesario para realizar una lectura de saldo, siendo el segundo flujo, similar al flujo de escritura en una compra de título virtual, pero sin coste al usuario.

Por ejemplo, durante el ciclo de vida de una tarjeta, es posible que el conjunto de datos que esta alberga se vea alterado de formas que no sean correctas de acuerdo a la lógica BIT dictada por CRTM. Esto ocurren en la gran mayoría de los casos por errores en la lógica implementada en cada uno de los actores que manipulan la tarjeta: validadores, máquinas de venta, etc. En estas situaciones, la única alternativa que tenía el usuario, hasta el momento, era acudir a alguna de las oficinas de CRTM y 'reparar' la tarjeta.

Sin embargo, con la virtualización el sistema ofrecerá la capacidad de corrección de raw de tarjetas automáticamente, solucionando el problema en remoto y evitando al usuario un desplazamiento a una oficina de CRTM

6.2. Pruebas en el CDC

El Centro de Desarrollo y Conformidad (CDC) inaugurado en el año 2006, tiene por objetivo fundamental ser el centro de referencia tecnológico que garantiza la compatibilidad de todos los elementos, equipos y sistemas, tanto hardware como software, que constituyen o puedan constituir parte del Sistema de Billetaje Inteligente de la Comunidad de Madrid. Por ello, todas las comprobaciones del funcionamiento de todas las implementaciones enmarcadas en este contrato deberán realizarse en dicho centro, bajo la supervisión de personal del CRTM

6.2.1. Adquisición de terminales móviles para las pruebas.

Se necesita una muestra mínima de terminales móviles para probar que las implementaciones cumplen los requisitos funcionales (los 30 modelos más utilizados en España, revisado cada 6 meses).

En este caso se debe verificar que la virtualización de la tarjeta en el móvil es segura y correcta. Que todos los validadores de la red reconocen los terminales móviles, es decir, son capaces de leer la información de la tarjeta virtualizada procesarla, actualizarla y generar la transacción en un tiempo razonable. Éste debería estar por debajo de los 650 milisegundos. Si se cumplen estos objetivos con los 30 modelos de móviles más usados en España el CRTM tiene suficientes garantías para poder poner el sistema en producción.

6.2.2. Asistencia en las pruebas

Todas las pruebas de billetaje de la Comunidad de Madrid se realizan en el CDC con la supervisión y coordinación del CRTM. Es necesario contar con la asistencia de los técnicos de la empresa adjudicataria en la ejecución de las mismas. El adjudicatario deberá estar presente y colaborar en el desarrollo de las pruebas.

6.3. Seguridad

Este proyecto requiere un nivel muy alto de seguridad digital, que el adjudicatario deberá garantizar al CRTM

El sistema propuesto deberá garantizar la seguridad de los datos sensibles de la tarjeta virtual del CRTM en la parte más segura posible del smatphone; bien a través de su almacenamiento en un secure element (SE), o cuando no sea posible, dotando al software de las herramientas necesarias para garantizar, cuando menos, su integridad y la seguridad de los datos sensibles en un white-box.

Con independencia de ello, la empresa adjudicataria deberá contratar los servicios externos de una empresa de seguridad informática no vinculada al proyecto para que realicen pruebas de hacking ético y verifique que la app y la tarjeta virtualizada son seguras, revisando también, la “white-box”. En caso de que hacking ético ponga al descubierto algún fallo de seguridad (como, por ejemplo, clonación de tarjeta virtual en otro terminal móvil o acceso a los datos de la tarjeta virtual) el adjudicatario deberá tomar nuevas medidas para subsanarlo

Se deberá realizar el ejercicio de auditoria de hacking ético, al menos, una vez al año. Los resultados de dicha auditoria, y su demostración, serán verificados en el CDC, en presencia del adjudicatario y personal del CRTM

6.4. Refuerzo backoffice del CRTM

Este contrato contempla la posibilidad de reforzar los desarrollos en la parte del back-office del CRTM para acelerar la puesta en producción. A continuación, se describe, a alto nivel algunas de las líneas que podría reforzar el adjudicatario de este contrato si CRTM lo considerase oportuno:

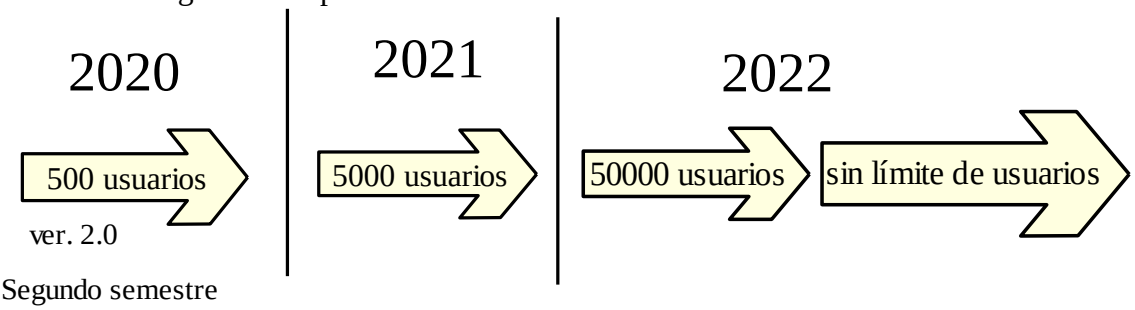
- Diseño e implementación de SECU-VCS. Se trata del actor encargado de poner en comunicación al backoffice de CRTM con los gestores de las tarjetas virtuales.
- Aplicación de gestión de la tarjeta virtual. Aplicación encargada de permitir al usuario final la compra de tarjetas virtualizadas de CRTM, así como la recarga de títulos en las mismas.
- Integración con la pasarela de pago del CRM. La aplicación anterior deberá integrarse con la pasarela de CRTM para cobrar las tarjetas virtuales emitidas a los usuarios finales, así como para cobrar los títulos recargados en estas. Además, se explorará la posibilidad de usar GPAY.

También podrían contemplarse las horas necesarias para las pruebas e integración:

- Integración de SECU-VCS con los sistemas del actor (adjudicatario de este pliego) encargado de la virtualización.
- Integración de SECU-VCS con el sistema que proporciona las operaciones lógicas de BIT, esto es el LAT (Lógica de Aplicación de Transporte).
- Integración y pruebas de SECU-VCS con los actores o subsistemas del backoffice de CRTM.
- Integración entre la aplicación de usuario y el SECU-VCS.
- Pruebas de homologación de todo el conjunto en las instalaciones del CDC.

7.- Fases del proyecto

Planificación gradual en producción:



ver. 2.0

Segundo semestre

- Ver 1.1: Tarjeta virtual emulada directamente. Esta versión sirve para las pruebas en el CDC y que los integradores de las aplicaciones de validación (sistema BIT) puedan adaptarse a los nuevos requisitos
- Ver 2.0: Aplicación de carga de títulos sobre la tarjeta virtual mediante todas las integraciones de backoffice previstas. Soporta sólo tarjeta Multi, con un solo título (multiviajes). Segundo trimestre 2020 en producción con un número reducido de usuarios
- Ver 3.0: se añade a la migración de la TTP física a TTP virtual, quedando inactiva la TTP física.
- Ver 4.0: se añade funcionalidad de atender incidencia en remoto.

8 GLOSARIO DE TERMINOS

AES
Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques y es uno de los algoritmos más populares usados en criptografía simétrica.

Backoffice
Se refiere a los procesos informáticos internos que realiza un actor del sistema

BIT o sistema BIT o proyecto BIT:
El BIT (Billetaje Inteligente del Transportes) es el núcleo de todo el cambio tecnológico que se está produciendo en el proceso de migrar la tecnología magnética de billetaje hacia la tecnología sin contactos. El BIT establece todas las reglas a todos los niveles, y esto, hace posible que dispongamos de la conocida TTP (tarjeta de transporte público). Es decir, la TTP es un producto del BIT.

HCE
Host card emulation. Término utilizado en el ámbito de emulación de tarjetas en teléfonos móviles.

HSM
Los Hardware Security Module (HSM) (Módulo de Seguridad Hardware) son los dispositivos garantes de la seguridad (con disponibilidad de 24x7x365). El CRTM se encarga de particularizar (preperso+perso) todos los HSM del sistema. Las tarjetas criptográficas utilizadas actualmente son PL600 y PSI-E2:PL1500. Estas tarjetas son capaces de embeber claves y comandos de forma segura (software de bajo nivel). Los HSMs incorporan un sistema antirrobo basado en la “tamperización”, esto es un proceso autodestructivo por si se intenta abrir o quitar un dispositivo HSM.

Mapa de memoria
Se entiende por mapa de memoria a el conjunto de ficheros en hexadecimal que se requieren para representar todos los atributos descritos en las especificaciones del sistema BIT.

NFC
Near field communication (NFC, comunicación de campo cercano en español) es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Los estándares de NFC cubren protocolos de comunicación y formatos de intercambio de datos, y están basados en ISO 14443 (RFID, radio-frequency identification) y FeliCa.1 Los estándares incluyen ISO/IEC 180922 y los definidos por el NFC Forum.

OTA

Over the air programming. Término utilizado en comunicaciones inalámbricas para referirse al medio del canal.

RAW
El formato RAW representa los ficheros elementales (FE) de la memoria de la tarjeta y su contenido en hexadecimal.

SAE
Sistemas de Ayuda a la Explotación. En el ámbito del transporte público, cada operador de transportes requiere de un SAE para que el centro de control del operador de transportes pueda seguir, en tiempo real, la situación de cada autobús, su ocupación y el ajuste con respecto al horario programado. Estos sistemas están integrados con CRTM y representan la oferta.

SAM
Un módulo de acceso seguro (SAM) es un dispositivo de seguridad, que sirve para almacenar claves maestras y comandos de bajos nivel que permiten realizar operaciones seguras con el exterior, de forma muy rápida. Los módulos SAM permiten acceder al contenido de la Tarjeta de Transporte Público (TTP), tanto en validación como en inspección. Además, a través de estos dispositivos es posible particularizar los HSMs que se ocupan de los procesos de personalización y carga/recarga. El sistema de seguridad de BIT, define comandos de bajo nivel específicos y mecanismos de seguridad propios del CRTM.

SECEBIT
SECEBIT (SEguridad CEntralizada para el sistema BIT) permite varios cientos de procesos concurrentes, se compone de al menos dos servidores criptográficos configurados en alta disponibilidad (balanceados), cada uno de los cuales incorpora al menos un módulo de hardware seguro (HSM) (tarjeta PCI), los HSMs son el núcleo del sistema SECEBIT, pero para que el servidor criptográfico pueda ofrecer el servicio del núcleo se precisa una capa software que establezca la comunicación entre el exterior y el núcleo. El CRTM dispone de este software (de alto nivel).

SID
Es el Servidor de Intercambio de Datos. La conexión es un canal seguro al que acceden todos los actores del sistema para subir las transacciones y descargar ficheros de configuración actualizados.

TLV
Son paquetes de datos (Tipo Longitud y Valor).
Las especificaciones BIT construyen los ficheros elementales incluidos en el mapa de memoria de la TTP como un conjunto de TLVs. También, por extensión, los TLVs se utilizan para nombrar los diferentes tipos de transacciones que se generan cada vez que la TTP interactua con cualquier lector. Dichas transacciones, de tipo TLV se envían al CRTM mediante el SID.

TTP:
Es la tarjeta de transporte público (tecnología sin contactos, norma ISO 14443A). Dicha tarjeta sigue las especificaciones de tamaño de la norma ISO 7816 y dispone de un chip tipo NXP DesFire. La tarjeta TTP es pasiva y los lectores/validadores del sistema inducen la corriente suficiente para su funcionamiento

En Madrid a fecha de firma

EL JEFE DE AREA DE SISTEMAS

Firmado digitalmente por: CRIADO FERNÁNDEZ LUIS
Fecha: 2020.10.06 10:06

EL DIRECTOR DE PLANIFICACION
ESTARTEGICA Y EXPLOTACIÓN

Firmado digitalmente por: GOMEZ LOPEZ FRANCISCO JAVIER
Fecha: 2020.10.06 10:39