DEFINICIÓN DEL MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE RECAUDO EN EL PROYECTO PRIMERA LÍNEA METRO DE QUITO Y MODELO DE INTEROPERABILIDAD DE RECAUDO ENTRE LOS SISTEMAS DE TRANSPORTE PÚBLICO DEL DISTRITO METROPOLITANO DE QUITO

ENTREGABLE 1
MANUAL DE NORMATIVIDAD TÉCNICA PARA EL SISTEMA INTEGRADO DE RECAUDO DEL SITM-Q

10/12/2018

Contenido

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Figuras

www.gsdplus.com

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Tablas

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Revisiones

Versión	Fecha	Elaborado por	Descripción
2	14/08/2018	GSD+	Atiende las observaciones de EPMMQ con fecha 1 de agosto de 2018

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Glosario

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Introducción

En el presente documento se expone la información de las soluciones tecnológicas que constituirán el entorno de interoperabilidad del Sistema Integrado de Recaudo (SIR) para el Sistema Integrado de Transporte Masivo del municipio de Quito (SITM-Q). Con esta información se fijan los lineamientos para permitir que cualquier usuario del SITM-Q requiera un único medio de pago para acceder a cualquiera de los subsistemas del SITM-Q. Asimismo, que puedan acceder a tarifas especiales según la regulación de tarifas vigentes para el Municipio de Quito.

Las especificaciones tecnológicas que se describen en este documento tienen en cuenta medios de pago recargables sin contacto (recargables) y medios de pago desechables de uso espontáneo (no recargable) compatibles con las cuatro partes del estándar ISO 14443:

- **ISO/IEC 14443-1**: Identification cards - Contactless integrated circuit cards Proximity cards - Part 1: Physical characteristics
- **ISO/IEC 14443-2**: Identification cards - Contactless integrated circuit cards Proximity cards - Part 2: Radio frequency power and signal interface
- **ISO/IEC 14443-3**: Identification cards - Contactless integrated circuit cards Proximity cards - Part 3: 3: Initialization and anti-collision
- **ISO/IEC 14443-4:** Identification cards - Contactless integrated circuit cards Proximity cards - Part 4: Part 4: Transmission protocol
- **ISO/IEC 14443-4:** Identification cards - Contactless integrated circuit cards Proximity cards - Part 4: Transmission protocol - Amendment 1: Handling of reserved fields and values

Específicamente, se presentan diez capítulos como se describe a continuación:

Capítulo 1 – Contexto

En este capítulo se define y explica la arquitectura que adoptará la red interoperable, se especifican las tecnologías para medios de pago recargables y no recargables. También, se explica el concepto de productos en medios de pago y finalmente se definen los ciclos de vida tanto para medios de pago y cómo para productos.

Capítulo 2 – Mapa de memoria de medios de pago

Una vez definida la tecnología del medio de pago, se define el mapa de memoria para dos tipos de medios de pago, i.e., medios de pago no recargables (medios de pago desechables de uso esporádico) y medios de pago recargables (medios de pago resistentes y de uso frecuente). El mapa de memoria hace referencia a la estructura de archivos y de datos que debe incorporarse para poder llevar a cabo transacciones interoperables con cada uno de los medios de pago del SIR. Se detallan los tipos de datos, tomando como referencia principal el estándar BS ENV 1545:

- **BS ENV 1545-1:1998**: Identification card systems - Surface transport applications Elementary data types, general code lists and general data elements

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- **BS ENV 1545-2:1998**: Identification card systems - Surface transport applications Transport and travel payment related data elements and code lists

Es importante tener en cuenta que algunos datos que se presentados a partir de este capítulo no están asignados, i.e., no tienen valores predeterminados ya que deben ser asignados posteriormente por un ente Registrador, tanto para el desarrollo de pruebas como para la puesta en operación de medios de pago, dispositivos en campo, sistemas concentradores y sistemas centrales. El Registrador es el ente encargado de la definición de códigos y valores para algunos campos establecidos en este documento.

Capítulo 3 – Datos en terminales de aceptación

Este capítulo presenta y explica la estructura de información contenida en cada uno de los archivos presentes en los terminales de aceptación. Así mismo, se explica la función de cada dato presente en dichos archivos y el uso de estos para diferentes esquemas tarifarios.

Capítulo 4 – Modelo transaccional

Se definen las posibles transacciones que se pueden efectuar con los medios de pago a través de la explotación del mapa de memoria de medios de pago. Asimismo, se especifican los procesos de manipulación de la información que deben llevar a cabo los equipos que interactúan con medios de pago para ejecutar las transacciones de uso de los medios de pago.

Capítulo 5 – Interfaces entre sistemas

En este capítulo se presenta el modelo de flujo de datos, los servicios para la transmisión de archivos, la descripción de archivos y finalmente las consideraciones de seguridad relacionadas a la transmisión de archivos entre niveles del sistema interoperable. Se presenta la definición del contenido y estructura que deben tener los esquemas de datos para la transmisión de archivos transaccionales y no-transaccionales entre el Sistema de Gestión Global y los sistemas de recaudo.

Capítulo 6 – Modelo de seguridad de las transacciones

Esta sección contiene la caracterización de la arquitectura de seguridad del sistema de recaudo interoperable, incluyendo la definición de módulos de acceso seguro (SAM) utilizados para el control de acceso a distintas funcionalidades de la red, definición de las llaves de seguridad que se almacenan en cada uno de los SAM, especificación de los permisos que debe tener cada actor en la red y el módulo SAM correspondiente para cada una de las operaciones.

Capítulo 7 – Datos asignados por el registrador

A lo largo del presente documento mencionarán identificadores y valores que deben ser asignados por un Registrador. En éste capítulo se presentan dichos identificadores y valores de acuerdo a su relevancia y de acuerdo al momento en que deben ser asignados.

Capítulo 8 – Casos de uso de medios de pago

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Esta capítulo incluye cada caso de uso que se puede presentar en el sistema, estos son definidos cómo cada interacción que puede realizar un medio de pago. Así mismo, para cada uno se incluyen: descripción, prerrequisitos, actores involucrados y transmisión de archivos de eventos.

Capítulo 9 – Protocolo de pruebas y certificación de equipos y sistemas

Se especifican subprocesos y flujos de prueba para cada componente de la especificación de interoperabilidad, incluyendo las pruebas de funcionalidad de medios de pago y de las interfaces con el Sistema de gestión global. Especificación de los ambientes de prueba usados para certificar los equipos, medios de pago y sistemas a nivel de pruebas controladas, QA y producción.

Capítulo 10 – Escenarios de prueba

En este capítulo se incluyen escenarios de prueba para emisores de medios de pago, distribuidores de productos y para procesos de aceptación de medios de pago. En cada uno de éstos subcapítulos se detalla un proceso de prueba para cada escenario.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Notación

La información numérica consignada en este documento está expresada en formato hexadecimal si el dato incluye el prefijo “0x”. En algunas ocasiones también se expresan números en formato binario, en cuyo caso se utiliza el prefijo “0b”. En caso en que el dato expresado conste de más de dos bytes, la representación es realizada en el sistema Big-Endian. Por otro lado, si el dato está expresado en formato decimal, este no incluye ningún prefijo. El siguiente ejemplo presenta las tres posibles representaciones del mismo número en este documento.

Decimal	Hexadecimal	Binario
9938	0x26D2	0b0010011011010010

La representación en bytes de cada dato corresponde al formato en el que deben ser almacenados los datos en el medio de pago, por lo que datos representados en el formato Big-Endian, deberán igualmente ser almacenados en este formato en el medio de pago. Cuando aplique, los archivos y registros definidos estarán compuestos por la concatenación secuencial de los Datos que los componen.

Es importante tener en cuenta que para los campos con codificación UTF-8 en caso de que no se utilice la totalidad de campos disponibles se debe completar el campo con caracteres en blanco (0x00) a la izquierda, i.e., los bytes más significativos deben llenarse con (0x00).

Este documento incluye datos cuyo tamaño en bits puede ser diferente a un múltiplo de 8. En estos casos se debe adicionar una secuencia de ceros a la izquierda del dato para completar un múltiplo de 8. Este proceso se debe realizar debido a que la representación de bits de los datos debe ser bit-alineada para poder expresar los datos en términos de bytes. A continuación, se presenta un ejemplo de un dato que requiere este procesamiento:

Dato	Tamaño (bits)	Tamaño (bytes)	Valor (binario)
6333	13	2	0b0001100010111101

Para todos los medios de pago descritos en este documento, cada vez que se haga mención de un archivo EF, se hace referencia a un archivo elemental [1], i.e., un archivo que permite almacenar datos necesarios para el funcionamiento de la aplicación interoperable. Ahora bien, cuando se hable de un archivo DF, se hace referencia a un directorio o aplicación que contiene direcciones para acceder a archivos EF. Según [2], un DF no puede contener otro DF, solo almacena archivos EF.

A lo largo del documento el nombre de los archivos que se almacenan en el medio de pago se escribe en mayúsculas. Para denotar directorios, se utilizan mayúsculas y negrita. Por ejemplo, USUARIO es un EF, mientras que **TRANSPORTE_QUITO** es un DF.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Cuando se habla de un dato almacenado dentro de un ARCHIVO (ya sea EF o DF) se hace siguiendo la convención ARCHIVO.dato.

Finalmente, cuando se habla de un registro asociado a un Producto, en un archivo específico, se denotará con la convención ARCHIVO(Producto). Por ende, un dato almacenado dentro de un registro asociado a un producto se denotará ARCHIVO(Producto).dato. También puede darse el caso en que se especifique un registro asociado a un archivo EF, en cuyo caso se denotará ARCHIVO(registro). El valor de saldo asociado a un producto se denotará Valor(Producto), si está asociado a un **MONEDERO** también puede denotarse como ValorMonedero, en caso de que esté asociado a un contador se puede denotar como ValorContadorN donde N es el número del contador.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

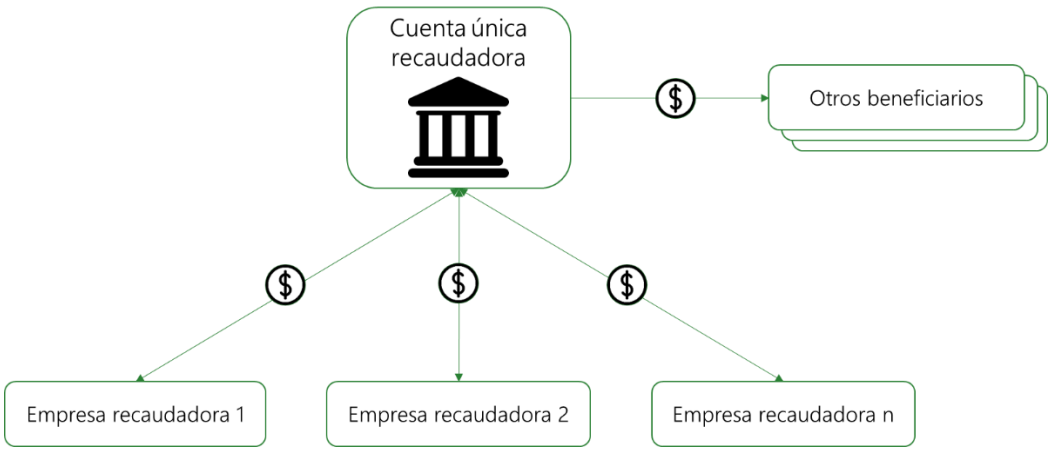
1. Contexto

1.1 Contexto de la Red Interoperable

La visión del SITM-Q contempla una integración tarifaria y de medios de pago para todos los modos de transporte actuales y futuros de la ciudad. Además, se contempla la prestación de servicios de la ciudad como acceso y uso de bibliotecas, acceso a instituciones educativas y de salud mediante un único medio de pago y acceso. Para lograr el objetivo de integración tarifaria y de medios de pago se requiere que los diferentes actores de la red se interconecten a través de una Cámara de compensación. Este mediador permite intercambiar la información transaccional de los usuarios entre entidades y así poder remunerar a todas las entidades de forma consistente.

La cámara de compensación tendrá una arquitectura centralizada, en la cual, todo el dinero recaudado por las empresas operadoras de recaudo se deposita en una única cuenta de ciudad, la cual puede ser manejada por la entidad reguladora de la Cámara de Compensación. La función principal de la Cámara de Compensación es estimar la remuneración para cada una de las empresas gestoras de los subsistemas de transporte. Esta actividad será supervisada y revisada por las empresas gestoras de cada subsistema. La Cámara de Compensación también está encargada de administrar el flujo de datos transaccionales entre los diferentes actores, tal como se describirá a lo largo de este documento.

Figura 1. Esquema de cámara de compensación



Fuente: elaboración propia

Los actores participantes en la red interoperable pueden cumplir diferentes roles dentro del sistema de transporte. Cada rol está asociado a un conjunto de funciones técnicas y administrativas. A continuación se hace una descripción general de los roles que pueden encontrarse en la red:

- *Autoridad de aplicación y control*

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Es la máxima autoridad de transporte de la ciudad, será la propietaria de la aplicación interoperable y estará a cargo de la cámara de compensación.

- *Administrador de las llaves del sistema*

  Es la entidad encargada de proteger y custodiar las llaves del sistema, así como también las especificaciones del modelo de seguridad, descrito en el capítulo 6.

- *Inicializador de medios de pago*

  Es el encargado de inicializar los medios de pago, cargándole llaves de producción para el control de acceso a archivos y funcionalidades. Este proceso es descrito en el capítulo 4.1.1.

- *Emisor de medios de pago*

  Encargado de emitir medios de pago.

- *Distribuidor de productos*

  Encargado de distribuir productos en medios de pago, y de recargar productos almacenados en medios de pago de usuarios.

- *Operador de recaudo*

  Encargado de recaudar y realizar recargas en medios de pago. También puede realizar transacciones de aceptación para conceder acceso al sistema.

- *Proveedor de recargas remotas*

  Encargado de recaudar y realizar recargas a medios de pago a través de canales remotos (sucursales web, sucursales telefónicas, etc.).

- *Registrador*

  Identifica y registra, por medio de códigos únicos los, elementos que conforman el sistema de billetaje electrónico. Además, define las reglas y parámetros de uso de los diferentes productos.

- *Proveedor de llaves*

  Entidad autorizada por la autoridad máxima de transporte para realizar la ceremonia de creación de llaves y diseñar la arquitectura de seguridad del sistema.

- *Entidad certificadora.*

  Puede ser la Autoridad de Aplicación y Control o cualquier otro organismo que esta designe para el seguimiento de los protocolos de pruebas y la certificación de Operadores de Recaudo.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Es importante destacar que una misma entidad, puede ejercer simultáneamente más de uno de los roles anteriormente descritos. De esta manera, se asegura flexibilidad en el modelo operacional de los actores de la red. Las actividades asociadas a cada rol, serán descritas de manera detallada a lo largo del presente documento.

1.2 Especificaciones Tecnológicas

1.2.1 Medio de Pago recargable

La tecnología Calypso Rev. 3.1 (referida de aquí en adelante como Calypso) es una referencia de medios de pago recargables sin contacto que cumplen con las especificaciones Calypso Rev. 3.1 [2].

Estas especificaciones no solo son compatibles con las cuatro partes del estándar ISO/IEC 14443 A y B, sino también con tecnología Java Card y con el estándar GlobalPlatform, ampliamente utilizados para implementación de aplicaciones interoperables de transporte en medios de pago bancarios (e.g., tarjetas híbridas y tarjetas EMV).

La tecnología Calypso está avalada y regulada actualmente por un grupo de entidades encargadas de la operación de los sistemas de transporte a nivel mundial, las cuales conforman la Asociación de Redes Calypso (CNA por sus siglas en inglés). Esta entidad tiene como objetivo transmitir la experiencia de los operadores de sistemas de transporte incorporando especificaciones técnicas en los productos Calypso, para que puedan adaptarse fácilmente a las necesidades de una red interoperable. La CNA trabaja investigando nuevas tendencias tecnológicas en SIT, como la compatibilidad con tarjetas bancarias y las tarjetas multi-aplicación, y con base en sus hallazgos incorporan nuevas funcionalidades en sus especificaciones técnicas.

En general, los medios de pago Calypso incluyen funcionalidades para:

- Comunicación entre terminales y medios de pago sin contacto mediante protocolos y algoritmos anticolisión tipo A y B según el estándar ISO/IEC 14443-3.
- Garantizar la integridad de la información en caso de interrupción de la comunicación entre un terminal y el medio de pago.
- Lectura y escritura de archivos.
- Control de acceso a la información almacenada en archivos y control de acceso a transacciones, con llaves y algoritmos de cifrado DES, DESX, y TDES.

  Nota: A pesar de la variedad de algoritmos de cifrado, todos los medios de pago Calypso que se emitan para el SITM-Q deben utilizar el algoritmo TDES)

Los archivos elementales dentro de una aplicación en el medio de pago Calypso deben ser de alguno de los siguientes tipos:

- *Archivos de registro lineales:* archivo con N registros de un mismo tamaño fijo.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- *Archivos de registro cíclicos:* están destinados a mantener bitácoras de acciones. La creación de un nuevo registro implica la eliminación del registro existente más antiguo.
- *Contadores:* los contadores son archivos con un único registro de N bytes que contiene N/3 contadores de 3 bytes.
- *Binarios:* archivos con capacidad de almacenar N bits en formato binario.

Los archivos lineales, cíclicos, y binarios se definen como en la ISO/IEC 7816-4.

Para el caso de los archivos lineales y cíclicos, el tamaño de cada registro debe ser de 1 a N (N puede variar de 120 a 250 dependiendo de las restricciones de memoria del medio de pago y de las capacidades específicas de la aplicación Calypso). El número de registros en un archivo debe ser de 1 a N (N puede variar de 120 a 250 dependiendo de las restricciones de memoria del medio de pago y de las capacidades específicas de la aplicación Calypso).

Los medios de pago Calypso cuentan con mecanismos de sesión segura y de ratificación, los cuales garantizan la integridad y protección de los datos en el medio de pago en caso de que se presente una interrupción de la comunicación entre un terminal y el medio de pago durante una transacción. Dichos mecanismos ejecutan simultáneamente:

- Autenticación de la aplicación interoperable, y del terminal.
- Autenticación de toda la información intercambiada durante la sesión.
- Pruebas para garantizar que las modificaciones a los medios de pago se hayan hecho correctamente.
- Restauración automática de transacciones en caso de una interrupción de la comunicación.

1.2.2 Medio de Pago no recargable

El medio de pago no recargables, MIFARE Ultralight EV1 de NXP, es una tarjeta que puede ser utilizada para viajes esporádicos por usuarios que no tienen intención de comprar un medio de pago de larga duración. Esta tarjeta puede ser plástica o de papel según como lo determine cada uno de los emisores del SIR. Se exige usar como mínimo la variante MF0UL11 [3] con un espacio de datos de usuario de 384 bits.

La tarjeta MIFARE Ultralight EV1 (denominada Ultralight o no recargables de aquí en adelante) está diseñada para operar en un ambiente compatible con las especificaciones técnicas de la ISO/IED 14443 A.

Adicionalmente, cuentan con una memoria fija compuesta por páginas, cada una de estas destinada a diferentes funciones como se expone en el Capítulo 2.2 de este documento. La memoria de las Ultralight es limitada. Sin embargo, cuenta con funciones de lectura y escritura que permiten almacenar información de valor y de permisos de viaje para un usuario esporádico.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Es importante resaltar que las tarjetas Ultralight no cuentan con mecanismos de cifrado para el control de seguridad. Por este motivo, el control de acceso queda a cargo del dispositivo de validación del medio de pago y de un módulo de acceso seguro. Específicamente, es necesario tomar información esencial del medio de pago no recargable para generar una firma digital, haciendo uso de uno de los módulos de acceso seguro (SAM) de Calypso, como se especifica en el Capítulo 6.

1.3 Productos en medios de pago

Los medios de pago pertenecientes a la red interoperable otorgan el acceso a los servicios de la red mediante el almacenamiento de diferentes productos. Cada uno de los productos define una serie de reglas de uso, con las cuales el usuario puede acceder a determinados servicios del sistema, según el perfil de usuario correspondiente.

La definición de estos productos disponibles en la red, de sus reglas de uso y de sus identificadores únicos, está a cargo del Registrador. De esta manera, se garantiza que todos los actores puedan administrar y proveer los diferentes servicios de la red, de manera efectiva, versátil y compatible.

Los medios de pago recargables, basados en tecnología Calypso Rev. 3.1, están en la capacidad técnica de almacenar varios productos de manera simultánea, permitiendo al usuario acceder a diferentes beneficios con el mismo medio de pago. Por su parte, los medios de pago no recargables, basados en tecnología MIFARE Ultralight EV1, contará con un único producto que brindará un acceso rápido a los servicios de la red, con una funcionalidad limitada.

1.3.1 Productos en medios de pago recargables

Los medios de pago recargables deben tener la capacidad de almacenar múltiples productos, los cuales ofrecen las funcionalidades de pago de la tarifa y acceso a la red interoperable de transporte para distintos tipos de usuarios. En medios de pago recargables, estos productos pueden ser de tipo general o de tipo especial. La definición de un producto en un medio de pago recargable se compone de:

- Un registro denominado contrato, con información de los derechos de viaje y la validez del producto. Este registro se almacena en un archivo llamado CONTRATOS.
- Un registro denominado servicio, con información de los servicios prestados al usuario haciendo uso del producto. Este registro se almacena en un archivo llamado SERVICIOS.
- Un valor de prioridad (determinado por el Registrador).
- Un archivo de valor.
- Información de validez y de tarifas almacenada en archivos de parámetros en dispositivos de aceptación de medios de pago recargables.

Un medio de pago recargable puede contener múltiples productos especiales. Sin embargo, solo puede existir un producto de tipo general en el medio de pago. Todos los medios de pago recargables deben tener el producto general.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Cada uno de los productos debe estar asociados a un archivo de valor que guarda información del saldo disponible en el medio de pago para acceder a ciertos derechos de viaje. El saldo puede tomar unidades de centavos (¢) de dólar de los Estados Unidos de América (USD) o unidades de viajes. Para el caso del producto general en medios de pago recargables, sus unidades de valor deben ser en centavos de USD. Dependiendo de las unidades de saldo asociadas a un producto debe utilizarse un tipo de archivo de valor particular. Los productos con unidades de valor en centavos de USD deben asociarse a un archivo denominado MONEDERO (solo hay un archivo MONEDERO en el medio de pago y este solo almacena un valor de saldo en centavos de USD). Los productos con unidades de viajes deben asociarse a uno de los contadores en el archivo de CONTADORES (solo hay un archivo CONTADORES en el medio de pago y este puede almacenar hasta seis valores (contadores) de saldo en unidades de viajes únicamente).

Ahora bien, para productos que le den a un usuario una cantidad limitada de viajes periódicos por un intervalo de tiempo determinado, será necesario fijar en los parámetros de validez del producto el número máximo de viajes a los que un usuario puede acceder y se llevará la cuenta de los servicios utilizados por el usuario con dicho producto en el medio de pago. Si la cantidad de viajes realizados dentro de una determinada unidad de tiempo (e.g. día, semana o mes) alcanza el límite, el usuario no puede seguir usando el producto.

Por otro lado, en los productos asociados a contadores (i.e., productos de los cuales se descuenta saldo en unidades de viajes), se descontará saldo del contador cada vez que un usuario haga uso del sistema, y también, se deben definir restricciones máximas de uso en un tiempo limitado si así lo requiere la regulación tarifaria vigente para el subsistema de transporte. Cada vez que el usuario hace uso del producto asociado a contador, ingresando al sistema con este, se debe descontar saldo de viaje del producto. El producto deja de ser válido cuando se acaba su saldo o cuando expira su validez.

El Registrador tiene la autoridad para definir límites máximo y mínimo de saldo, así como límites para el número de viajes por día, semana o mes, para cada uno de los productos. Si el saldo de un producto en centavos de USD es negativo, quiere decir que el usuario tiene una deuda con el SITM-Q.

Para cada producto deben definirse reglas tarifarias de conformidad con la regulación para el SITM-Q. Estas se definen teniendo en cuenta lo estipulado en la Ordenanza Metropolitana No. 0201 del 8 de febrero de 2018 [4]. Para definir la tarifa de un usuario con base en las reglas tarifarias del sistema, deben utilizarse conjuntamente los archivos almacenados en el medio de pago y los archivos de parámetros almacenados en cada terminal de pago, como se indica en las secciones 2.1 y 3 de este documento.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

1.3.2 Productos en medios de pago no recargables

Los medios de pago no recargables solo pueden almacenar un producto precargado, el cual debe ser cargado en el medio de pago con un saldo inicial (no recargable) durante la emisión. Este producto se definirá mediante:

- Un sector de memoria, denominado Datos de emisión, que contiene la información de los derechos de viaje y validez del producto.
- Un archivo de valor cuyas unidades pueden ser en centavos de USD o en unidades de viajes.
- Información de validez y de tarifas almacenada en dispositivos de aceptación de medios de pago no recargables.

1.4 Ciclos de Vida

El ciclo de vida de la aplicación interoperable o de un producto se define como un conjunto de estados para los cuales operan distintas funcionalidades en un determinado momento. En primer lugar, se encuentra el ciclo de vida de la aplicación. Este determina las funcionalidades globales de la aplicación en un momento dado, desde que el medio de pago es fabricado hasta que es desechado. Adicionalmente, cada producto tiene su propio ciclo de vida. Esto permite determinar de forma individual las funcionalidades de cada producto en un momento dado, desde que este es almacenado en la aplicación interoperable hasta que se restringe su uso.

1.4.1 Ciclo de vida de la aplicación interoperable en medios de pago recargables

El ciclo de vida de la aplicación consiste en un conjunto de estados excluyentes que describen las capacidades de la aplicación interoperable en un momento dado. Dicho estado es almacenado en ESTADO_APLICACIÓN.EstadoAplicación. El ciclo de vida consta de los siguientes estados:

- *Inicializada*: es el primer estado de la aplicación interoperable. Este estado se alcanza una vez un medio de pago pasa por un proceso de inicialización de la aplicación. Para esto, se debe definir la configuración del medio de pago (i.e., protocolos de comunicación, comandos, estructura de archivos); asignar un UID o serial único al medio de pago; haber cargado archivos de la aplicación; y asignar llaves de cifrado junto con AIDs para cada uno de los archivos. Este proceso se debe llevar a cabo en un entorno seguro por parte de una entidad personalizadora. Los medios de pago con la aplicación inicializada no pueden ser usados en la red interoperable. Este estado se mantiene hasta que un usuario solicita un medio de pago y este es emitido y activado.
- *Activada*: este estado permite usar el medio de pago en la red interoperable. Una aplicación pasa a *Activada* cuando esta pasa por el proceso de emisión del medio de pago. Una vez activada, la aplicación debe tener activado como mínimo un producto. Sin embargo, son una excepción los medios de pago para funcionarios, los cuales no tienen que almacenar ningún producto debido a que estos

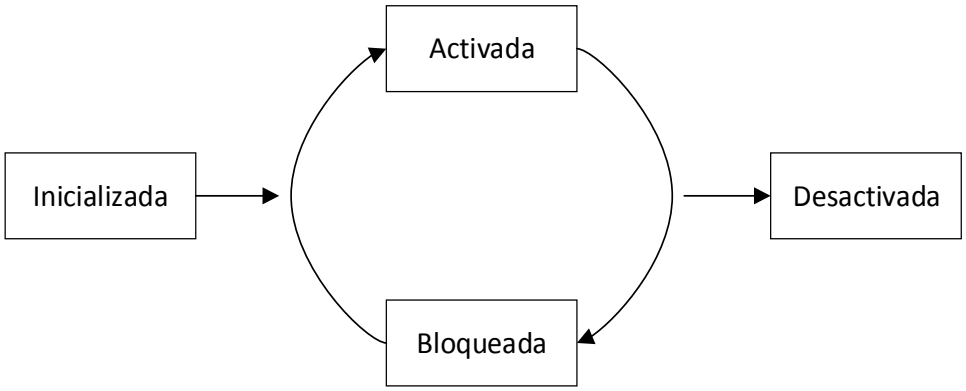
www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

almacenan un perfil de funcionario en USUARIO y un archivo FUNCTIONARIO con información propietaria para la aceptación del medio de pago.

- *Bloqueada*: este estado se alcanza cuando el emisor de medios de pago determina que existe un motivo por el cual la aplicación interoperable no puede ser usada temporalmente. Cuando la aplicación se encuentra en este estado no podrá ser usada en la red interoperable. Una vez se ha subsanado el motivo de bloqueo, el emisor podrá reactivar la aplicación y pasará a estado *Activada*.
- *Desactivada*: este estado se alcanza cuando la aplicación llega al fin de su ciclo de vida, ya sea por vencimiento de la vigencia de la aplicación o porque se ha determinado la desactivación definitiva del medio de pago. Cuando el medio de pago se encuentra en este estado no podrá ser usado en el sistema. La desactivación debe ser irreversible y ningún dispositivo debe cambiar de estado una aplicación que se encuentre desactivada.

La Figura 2 describe cómo pueden ocurrir las transiciones entre los estados de la aplicación interoperable. Como se puede observar, la aplicación interoperable siempre debe partir por el estado Inicializada, una vez pasa al estado de *Activada* la aplicación puede mantenerse en un ciclo de bloqueos hacia el estado Bloqueada y reactivaciones hacia el estado *Activada*. Por último, cuando la aplicación interoperable llega al fin de su ciclo de vida esta pasa al estado *Desactivada*, estado del cual no puede salir.

Figura 2. Ciclo de vida de la aplicación interoperable



Fuente: elaboración propia

1.4.1.1 Ciclo de vida de los productos en medios de pago recargables

Cada uno de los productos que se almacenan en un medio de pago tiene su propio ciclo de vida, el cual consiste en un conjunto de estados excluyentes que describen las funcionalidades del producto en un momento dado. Dicho estado es almacenado en SERVICIOS.EstadoProducto. El ciclo de vida de un producto consta de los siguientes estados:

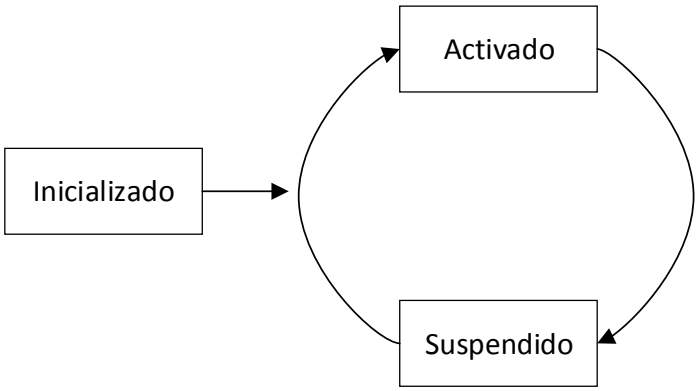
- *Inicializado*: este estado se alcanza cuando la aplicación interoperable ha sido igualmente inicializada. En este punto solamente se han creado los archivos correspondientes al producto y no contienen información. Igualmente, las llaves que protegen la modificación del producto no han sido cargadas.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- *Activado*: en este estado el producto podrá ser usado en la red interoperable. Los archivos CONTRATOS, SERVICIOS, MONEDERO y CONDATORES deben haber sido inicializados y se debe haber llevado a cabo el proceso de distribución del producto. Adicionalmente se deben haber definido los permisos de acceso con llaves de cifrado y módulos SAM para el producto correspondiente en el espacio designado para tal fin.
- *Suspendido*: este estado se alcanza cuando el emisor del producto determina que existe un motivo por el cual este no debe ser usado temporalmente. Cuando el producto se encuentra en este estado no podrá ser usado en la red interoperable. Una vez se ha subsanado el motivo de suspensión, el emisor podrá reactivar el producto y pasará al estado Activado.

La Figura 3 describe cómo pueden ocurrir las transiciones entre los estados de un producto almacenado en la aplicación interoperable.

Figura 3. Ciclo de vida de un producto



Fuente: elaboración propia

1.4.2 Ciclo de vida de la aplicación interoperable en medios de pago no recargables

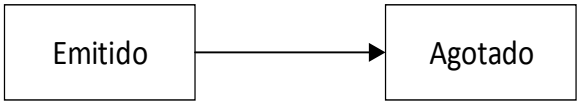
La aplicación almacenada en medios de pago no recargables consta de dos estados que definen su ciclo de vida. Estos estados a su vez definen las capacidades del medio de pago en un momento dado. Los estados del medio de pago se describen a continuación:

- *Emitido*: es el primer estado de los medios de pago no recargables. Este estado se alcanza una vez un medio de pago pasa por un proceso de escritura inicial de los datos de emisión, el valor inicial del saldo del contador y los parámetros adicionales definidos en este documento. Este proceso se debe llevar a cabo en un entorno seguro por parte de una entidad personalizadora. Una vez emitido un medio de pago precargado este está en capacidad de ser usado en la red interoperable. Solo es posible vender medios de pago que hayan sido emitidos previamente a los usuarios de la red interoperable.
- *Agotado:* es el estado final del medio de pago. Este estado se alcanza cuando se ha usado en su totalidad el saldo almacenado en el medio de pago precargado.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Cuando se alcanza este estado el medio de pago no se debe aceptar más en la red interoperable y puede ser desechado.

Figura 4. Ciclo de vida de los medios de pago precargados



Fuente: elaboración propia

2 Mapa de memoria de medios de pago

El presente capítulo define características técnicas de los medios de pago que pueden ser emitidos en el entorno interoperable del SIR para el SIMTQ. Cabe aclarar que las implementaciones de recaudo dentro del entorno interoperable deberán estar preparadas para aceptar la totalidad de los medios de pago que se describen a partir de este capítulo. Se definen dos tipos de medios de pago:

- Medios de pago recargables: son aquellos que pueden ser recargados constantemente con valor en sus productos. Están destinados a ser usados por usuarios frecuentes de los servicios de transporte.

  Los medios de pago recargables se deben se deben emitir con la tecnología Calypso, específicamente, deben cumplir con las especificaciones Calypso Rev. 3.1 [2], las cuales se han definido para ser usadas en servicios de transporte público, aunque su uso puede extenderse para múltiples aplicaciones.

- Medios de pago no recargables: son aquellos medios de pago que son emitidos con un valor fijo disponible para viajes y que no pueden ser recargados. Están destinados a usuarios esporádicos, usuarios espontáneos o turistas que no desean adquirir un medio de pago recargable. Los medios de pago no recargables se deben emitir con la tecnología MIFARE Ultralight EV1 [3], la cual está diseñada para tener una vida útil corta a un bajo costo, haciéndola ideal para viajes espontáneos.

En principio, se presentan las características técnicas generales y las funcionalidades de cada una de las tecnologías de medios de pago. Se presentan las características más relevantes para efectos de aplicar la normatividad técnica definida en el presente documento. En caso de considerarlo necesario, el lector deberá referirse a la documentación técnica completa de cada tecnología con el fin de obtener más información.

2.1 Aplicación interoperable en medios de pago recargables

Los medios de pago con aplicaciones interoperables se caracterizan por guardar información de productos y de transacciones realizadas para darle acceso a un usuario del SITM-Q. Para hacer esto posible, es necesario que todos los medios de pago, tanto recargables como no recargables, almacenen un mapa de memoria con la estructura de archivos y las estructuras de datos que contienen la información necesaria para dar

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

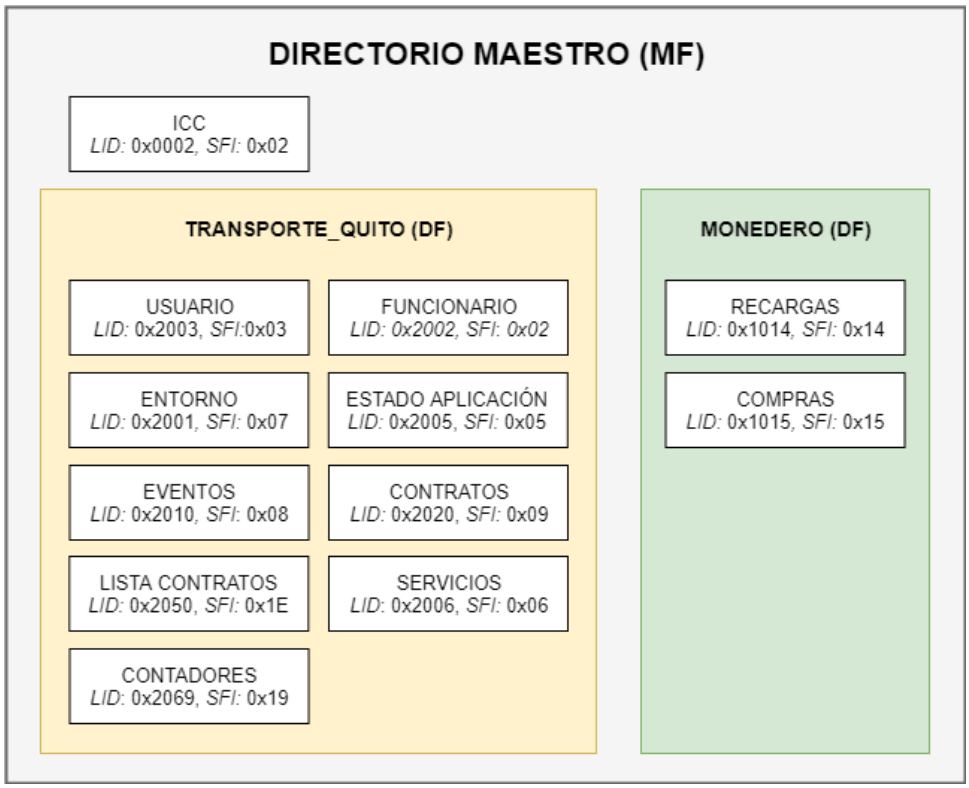
acceso a los subsistemas del SITM-Q. En esta sección se especifica el mapa de memoria de cada uno de los medios de pago. Todos los campos que se especifiquen como RFU están destinados para uso futuro.

2.1.1 Especificaciones generales de la estructura de archivos

El presente capítulo está compuesto por una descripción detallada de la información que se debe almacenar en los medios de pago Calypso para el SIR del SITM-Q. Inicialmente, se presentan los archivos que deben grabarse en el medio de pago y luego, se hace una descripción detallada con la información que debe contener cada uno de los archivos presentados en la definición general (definiciones disponibles en [5]). La definición de los tipos de datos se hace con base en los estándares ISO/IEC 7816-5 [6], ISO 3166, BS EN 1545-1:2005 [7], BS EN 1545-2:2005 [8], ISO 8601 [9].

La estructura de archivos del medio de pago (ver [10]) está compuesta por tres aplicaciones/directorios, como se muestra en la Figura 5, i.e., el directorio **MAESTRO**, la aplicación **TRANSPORTE_QUITO** y el **MONEDERO** (equivalente a la aplicación *Stored Value* de [2]). Los parámetros de archivos DF y EF en la aplicación interoperable se muestran en la Tabla 1.

Figura 5. Estructura de archivos en medios de pago Calypso



Fuente: elaboración propia

El identificador de directorios (AID) hace referencia al nombre que se le da al directorio en el medio de pago. Con el fin de evitar conflictos entre aplicaciones por AID, se

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

deben seguir las recomendaciones para selección de AIDs de las Especificaciones Calypso Rev. 3.1 y de la norma ISO/IEC 7816-5. Se puede hacer uso de los AID registrados o propietarios para Calypso, pero no se debe hacer uso de los AID compatibles con Rev. 2.

Tabla 1. Parámetros de archivos DF y EF en medios de pago recargables

DF	LID	Archivo EF	Tipo	Registros	Tamaño (bytes)	LID	SFI
MAESTRO	**0x3F00**	ICC	Lineal	1	29	0x0002	0x02
APP TRANSPORTE	**0x2000**	USUARIO	Lineal	1	90	0x2003	0x03
		FUNCIONARIO	Lineal	1	128	0x2002	0x02
		ENTORNO	Lineal	1	30	0x2001	0x07
		ESTADO APLICACIÓN	Lineal	1	12	0x2005	0x05
		EVENTOS	Cíclico	10	50	0x2010	0x08
		CONTRATOS	Lineal	6	35	0x2020	0x09
		LISTA CONTRATOS	Lineal	1	42	0x2050	0x1E
		SERVICIOS	Lineal	6	20	0x2006	0x06
		CONTADORES	Lineal	1	18	0x2069	0x19
MONEDERO	**0x1000**	RECARGAS	Cíclico	1	29	0x1014	0x14
		COMPRAS	Cíclico	3	29	0x1015	0x15

2.1.1.1 Condiciones de acceso y llaves de seguridad

Los medios de pago Calypso cuentan con comandos para el manejo de datos en las aplicaciones. Estos comandos se agrupan en cuatro según [2], y para cada grupo de comandos es necesario definir unas condiciones de acceso particulares. Para cada uno de los tipos de archivo que puede tener un medio de pago Calypso, los grupos de comandos se definen en la Tabla 2.

Tabla 2. Grupos de comandos para medios de pago Calypso

Grupo	DF	EF (Linear/Binario)	EF (Cíclico)	EF (Contadores)
0	Rehabilitar	Leer	Leer	Leer
1	Invalidar	Actualizar	Actualizar	Actualizar
2	RFU	Escribir	Escribir	Disminuir
3	RFU	RFU	Agregar	Aumentar

- Leer: extrae información de registro de archivo.
- Actualizar: permite reescribir un registro o parte de él, reemplazando información existente por información nueva.
- Escribir: permite sobrescribir la información de un registro o parte de él, reemplazando la información existente por el resultado de la operación OR lógica

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

entre la nueva información y la información existente. Por ejemplo, al escribir 0x05 sobre un campo que tiene almacenado 0x03, quedará almacenado 0x05. De manera similar, al escribir 0x02 sobre un campo que tiene almacenado 0x03, quedará almacenado 0x03. Útil para actualizar consecutivos y fechas de validez.

- Invalidar: invalida un DF.
- Rehabilitar: valida un DF que se encuentra en estado inválido (revierte el efecto de invalidar).
- Disminuir: disminuye el valor de uno o múltiples contadores.
- Aumentar: aumenta el valor de uno o múltiples contadores.

Ahora bien, en un sistema de recaudo interoperable basado en Calypso existen dos tipos de llaves que permiten controlar la seguridad del sistema, i.e., llaves del sistema (*system keys*), y llaves de trabajo (*work keys*).

El acceso a los comandos descritos anteriormente, se controla por medio de llaves de trabajo que son almacenadas en los directorios del medio de pago. Cada uno de los directorios en un medio de pago Calypso, debe almacenar tres, y solo tres, llaves de trabajo para controlar el acceso a sus archivos (ver Tabla 3) y a cada uno de los grupos de funciones que se especifican en la Tabla 2.

Tabla 3. Tipos de llaves en aplicaciones de medios de pago Calypso

Índice de la llave	Llave	Descripción
Llave # 1	Llave de emisor	Se debe utilizar para los comandos “Put Data” y “Change key” [2]. Se debe utilizar para autorizar la modificación de los datos de los archivos que requieren Sesión # 1. Se puede usar para verificar el valor de cualquier archivo de datos, para autorizar la modificación de los datos de los archivos que requieren la Sesión # 2 o la Sesión # 3. Esta clave generalmente se usa para modificar los datos globales de la aplicación.
Llave # 2	Llave de recarga	Se puede usar para verificar el valor de cualquier archivo de datos, para autorizar la modificación de los datos de los archivos que requieren la Sesión # 2 o la Sesión # 3. Esta clave se usa generalmente como una clave de recarga.
Llave # 3	Llave débito	Se usará para el comando Verificar PIN. Se puede usar para verificar el valor de cualquier archivo de datos, para autorizar la modificación de los datos de los archivos que requieren la Sesión # 3. Esta clave generalmente se usa como una clave de débito.

Adicionalmente, existen otros procesos y transacciones en el SIR que deben controlarse haciendo uso de llaves del sistema, principalmente, la personalización de

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

módulos SAM, y la transferencia de llaves de trabajo de SAMs a medios de pago. Dichos procesos se describen con más detalle en el Capítulo 6.

2.1.2 Aplicación MAESTRA

La aplicación **MAESTRA** contiene información relacionada con las características del protocolo de comunicación del medio de pago y del fabricante de medios de pago. La estructura de archivos que debe tener la aplicación **MAESTRA** junto con las condiciones de acceso para cada archivo se muestra en la Tabla 4**.**

Tabla 4. Estructura de archivos para APLICACIÓN MAESTRA en medios de pago recargables

				Grupo 0	Grupo 1	Grupo 2	Grupo 3
Archivo	**Tipo**	**Registros**	**Tamaño registro (bytes)**	**Leer Rehabilitar**	**Actualizar Invalidar**	**Escribir Disminuir**	**Agregar Aumentar**
APLICACIÓN MAESTRA (MF)							
ICC	Lineal	1	29	Siempre	Nunca	Nunca	-

2.1.1.1. Estructura de datos ICC

El archivo ICC contiene información de fábrica de la tarjeta, e información técnica relacionada con el protocolo de comunicación del medio de pago. Asimismo, contiene información importante de la inicialización del medio de pago, como la fecha de inicialización, el serial asignado al medio de pago durante la inicialización y datos del responsable de la inicialización.

Tabla 5. Estructura de datos para el archivo ICC en medios de pago recargables

Dato	Bytes	Descripción
RFU	10	Reservado para uso futuro
SerialMedioPago	8	Identificador único del medio de pago
Protocolo	1	Indica el protocolo de comunicación con el cual es compatible el medio de pago
BitRate	1	Tasa de transmisión de datos del protocolo 14443B
PaísFabricante	2	Código del país del fabricante del medio de pago
IdFabricante	1	Identificador único del fabricante del medio de pago según especificaciones Calypso
InformaciónFabricante	1	Campo libre para guardar información adicional sobre el fabricante
FechaInicialización	2	Fecha de inicialización del medio de pago
RFU	3	Reservado para uso futuro
Total	29	

(8 bytes) SerialMedioPago

Definición	Identificador único del medio de pago

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Tipo	SerialNumber (BS EN 1545-1)
Uso	Cada aplicación en el medio de pago debe guardar información del número serial del medio de pago. El número serial puede ser el mismo para todas las aplicaciones almacenadas en el medio de pago. Sin embargo, dos medios de pago distintos no pueden tener el mismo NumeroSerial. Este identificador se utiliza no solo para identificar de forma única al medio de pago, sino también para generar las llaves diversificadas que se almacenan en cada uno de los medios de pago.

(1 byte) Protocolo

Definición	Denota los protocolos de comunicaciones compatibles con el medio de pago sin contacto
Tipo	INTEGER (0..)
Uso	Es asignado por el fabricante de la tarjeta y puede tomar los siguientes valores: 0x00: ISO 14443 B 0x01: ISO 14443 A Se utiliza en caso de que se requiera verificar el tipo de protocolo ISO 14443 que utiliza la tarjeta.

(1 byte) BitRate

Definición	Tasas de transmisión de información en bits por segundo compatibles con el medio de pago
Tipo	OCTET
Uso	BitRate es un campo de un byte que se codifica como se muestra en la ISO 14443-3 Ejemplo: un medio de pago que requiere la misma tasa de transmisión en ambas direcciones y que soporta tasas de transmisión de 212 Kbps y 424 Kbps tendría un campo BitRate igual a 1011011 (0xB3). Se utiliza en caso de que se requiera verificar la tasa de transmisión de datos del medio de pago.

(2 bytes) PaísFabricante

Definición	Código identificador del país del fabricante del medio de pago
Tipo	Country (ISO 3166)
Uso	Código de país para el fabricante de acuerdo con el código numérico de 3 dígitos ISO 3166, en tres dígitos BCD corridos un cero a la izquierda (ejemplo, 0x0218 para Ecuador). Se utiliza en caso de que se requiera conocer información sobre el proveedor del medio de pago.

(1 byte) IdFabricante

Definición	Código identificador del fabricante del medio de pago
Tipo	Software Issuer (Calypso Technote 001, T6)
Uso	Código único estandarizado según Calypso Technote 001, tabla T6. Se utiliza en caso de que se requiera conocer información sobre el proveedor del medio de pago.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

(1 byte)	InformaciónFabricante
Definición	Campo libre para almacenar información adicional del fabricante
Tipo	OCTET
Uso	Este campo se puede usar para almacenar de forma libre cualquier dato adicional que se quiera del fabricante del medio de pago. En caso de no utilizarse su valor debe ser 0x00. Se utiliza en caso de que se requiera conocer información sobre el proveedor del medio de pago.

(2 bytes)	FechaInicialización
Definición	El día en que el medio de pago es inicializado
Tipo	CompactDate (BS EN 1545-1)
Uso	Campo para registrar la fecha en la que se inicializó el medio de pago. Consta de una cadena de 16 bits 0byyyyyyymmmmddddd, donde: 'yyyyyyy': Número de años después de 2010 (2010 = 0b0000000) 'mmmm': mes del año (entre 0b0001 y 0b1100) 'ddddd': día del mes (entre 0b00001 y 0b11111)

2.1.3 Aplicación de TRANSPORTE_QUITO

La aplicación **TRANSPORTE_QUITO** es un directorio que contiene un conjunto de archivos EF con la información necesaria para efectuar las operaciones de recarga de saldo y cobro de tarifas para cada uno de los servicios del SITM-Q. Adicionalmente, contiene dos EF con información del usuario portador del medio de pago, uno es el archivo USUARIO, y otro el archivo FUNCIONARIO (se debe usar en caso de que el medio de pago sea para un funcionario de la red). La Tabla 6 presenta la estructura general de los archivos que deben ser almacenados en el medio de pago.

Tabla 6. Estructura de archivos y condiciones de acceso para TRANSPORTE_QUITO en medios de pago recargables

				Grupo 0	Grupo 1	Grupo 2	Grupo 3
Archivo	**Tipo**	**Registros**	**Tamaño Registro (bytes)**	**Leer Rehabilitar**	**Actualizar Invalidar**	**Escribir Disminuir**	**Agregar Aumentar**
APLICACIÓN TRANSPORTE_QUITO (DF)							
USUARIO	Lineal	1	90	Siempre	Sesión 2	Nunca	-
FUNCIONARIO	Lineal	1	128	Siempre	Sesión 3	Sesión 3	-
ENTORNO	Lineal	1	30	Siempre	Sesión 1	Sesión 1	-
ESTADO APLICACIÓN	Lineal	1	12	Siempre	Sesión 3	Nunca	-
EVENTOS	Cíclico	10	50	Siempre	Sesión 3	Nunca	Sesión 3

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

CONTRATOS	Lineal	6	35	Siempre	Sesión 2	Nunca	-
LISTA CONTRATOS	Lineal	1	42	Siempre	Sesión 2	Sesión 2	-
SERVICIOS	Lineal	6	20	Siempre	Sesión 3	Nunca	-
CONTADORES	Lineal	1	18	Siempre	Sesión 2	Sesión 3	Sesión 2

2.1.1.2. Estructura de datos USUARIO

Este archivo contiene información del propietario del medio de pago la cual permite definir las características del perfil al que este está asignado. Los perfiles de usuario permiten calcular tarifas diferenciadas según el tipo de usuario.

Tabla 7. Estructura de datos para el archivo USUARIO en medios de pago recargables

Dato	Bytes	Descripción
FechaNacimientoUsuario	4	Fecha de nacimiento del portador del medio de pago
Perfil	SEQ	Información del portador
CódigoPerfil	1	Código numérico relacionado con el perfil del portador
FechaFinPerfil	2	Fecha de fin de validez del perfil de usuario
NombreUsuario	39	Nombre del usuario portador del medio de pago
CredencialUsuario	24	Número de identificación del portador
RFU	20	Reservado para uso futuro
Total	90	

(4 bytes) FechaNacimientoUsuario

Definición	Fecha de nacimiento del usuario de la tarjeta
Tipo	BirthDate (BS EN 1545-1)
Uso	Valor en BCD (0xYYYYMMDD). Se deja en blanco si el perfil de usuario es general, es decir, (0x00000000). Ejemplo: Fecha de nacimiento 6 de abril de 1994 FechaNacimientoUsuario = 0x19940406

Perfil	
Definición	Perfil del usuario portador del medio de pago

(1 byte) CódigoPerfil

Definición	Código que clasifica el segmento especial al cual pertenece el usuario
Tipo	ProfileCodeIOP (BS EN 1545-1)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Uso	Sus posibles valores son: - General (0x00) - Adulto personalizado (0x01) - Estudiante (0x02) - Adulto mayor (0x03) - Discapacitado (0x04) - Invidente (0x05) - Funcionario (0x09) Este valor se utiliza para definir la tarifa para el usuario al momento de efectuar una transacción débito y para saber qué perfiles pueden acceder al beneficio del viaje a crédito. También se utiliza en el momento de efectuarse una recarga para definir el producto que va a recargarse.

(2 bytes) FechaFinPerfil

Definición	Fecha de vencimiento de la validez del perfil
Tipo	EndDate (BS EN 1545-1)
Uso	Campo para registrar el fin de validez del perfil de usuario. Se utiliza para determinar la validez de productos al momento de efectuar transacciones débito o crédito. Este valor también se puede actualizar en caso de que se decida extender su validez.

(39 bytes) NombreUsuario

Definición	Nombre del propietario del medio de pago personalizado
Tipo	Name (BS EN 1545-1)
Uso	Nombre en codificación UTF-8. Se utiliza para verificar la identidad de un portador del medio de pago.

(24 bytes) CredencialUsuario

Definición	Indica el código de identificación del usuario
Tipo	HolderId (BS EN 1545)
Uso	Credencial del usuario en codificación UTF-8. Se utiliza para verificar la identidad de un portador del medio de pago.

2.1.1.3. Estructura de datos FUNCIONARIO

La presencia de este archivo es opcional y solo es necesario si el medio de pago pertenece a un funcionario dentro de la red interoperable. Debido a que cada Operador de Recaudo puede establecer sus propias reglas de acceso para sus funcionarios, se deja a discreción de cada Operador de Recaudo la estructura de este archivo. De esta forma sólo los funcionarios de cada Operador de recaudo tendrán acceso a su propia infraestructura. Si llega a utilizarse el archivo FUNCIONARIO, es decir, si el medio de pago se destina para controlar el acceso de funcionarios al

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

sistema, no deben incluirse en el mapa de memoria de la tarjeta los archivos CONTRATOS, LISTA_CONTRATOS, SERVICIOS, CONTADORES, ni **MONEDERO**. Adicionalmente, todas las reglas de acceso tendrán que definirse en el bloque de memoria destinado para FUNCIONARIO.

Tabla 8. Estructura de datos para el archivo FUNCIONARIO en medios de pago recargables

Dato	Bytes	Descripción
BloqueFuncionario	128	Archivo transparente que puede ser utilizado únicamente para guardar información para usuarios con perfil de funcionario, según las condiciones que establezca el registrador.
Total	128	

(128 bytes) BloqueFuncionario

Definición	Registro para almacenar de un funcionario de la red
Tipo	OCTET STRING
Uso	Este campo debe utilizarse únicamente para guardar información de un usuario con perfil de funcionario según como lo decida el Registrador de la red. Esta información puede incluir información sobre las condiciones de acceso del funcionario a la red, identificación, etc.

2.1.1.4. Estructura de datos ENTORNO

Este archivo se encarga de almacenar toda la información invariable relacionada con el emisor del medio de pago, y las variables que indican cuál es la red interoperable donde es aceptada la aplicación interoperable. Este archivo se crea durante el proceso de inicialización y nunca debe ser modificado una vez el medio de pago entra en circulación.

Tabla 9. Estructura de datos para el archivo ENTORNO en medios de pago recargables

Dato	Bytes	Descripción
VersiónAplicación	1	Versión de la aplicación interoperable
PropietarioAplicación	SEQ	Entidad que emite y controla la especificación de la aplicación
IdRedPropietario	3	Código identificador de la red a la que pertenece el propietario
IdPropietario	2	Código identificador del propietario de la aplicación
EmisorAplicación	SEQ	Entidad autorizada para emitir la aplicación interoperable
IdRedEmisor	3	Código Identificador de la red a la cual pertenece el emisor

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

IdEmisor	2	Código identificador del emisor
IdSAM	4	Código identificador del SAM utilizado para la emisión
FechaEmisión	2	Fecha en la que se lleva a cabo el proceso de emisión del medio de pago
FechaFinAplicación	2	Fecha a partir de la cual la aplicación interoperable deja de ser válida
RFU	11	Reservado para uso futuro
Total	30	

(1 byte) **VersiónAplicación**

Definición	Se refiere a la versión de la aplicación interoperable
Tipo	VersionNumber (BS EN 1545)
Uso	Los 4 primeros bits para versión mayor y siguientes 4 bits para versión menor. La versión inicial debe ser 1.0. (0x10). Se utiliza para en operaciones con terminales de pago para definir secuencias de comandos según versión de la aplicación.

PropietarioAplicación	
Definición	Información de la entidad que emite y controla la especificación de la aplicación. Equivale a la autoridad de aplicación y control

(3 bytes) **IdRedPropietario**

Definición	Identificador de la red a la cual pertenece el propietario de la aplicación.
Tipo	NetworkId (BS EN 1545)
Uso	Este valor es asignado por el Registrador y se define como un código identificador único en formato NetworkId según BS EN 1545-1. Se utiliza para verificar la validez del medio de pago en una red, en caso de que exista más de una red interoperable.

(2 bytes) **IdPropietario**

Definición	Identificador de la entidad propietaria de la aplicación
Tipo	CompanyId (BS EN 1545)
Uso	Código identificador único del propietario de la aplicación interoperable. Se utiliza para identificar a la entidad que desarrolla la aplicación de transporte cargada en un medio de pago.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

EmisorAplicación	
Definición	Entidad autorizada para emitir la aplicación interoperable

(3 bytes)	**IdRedEmisor**
Definición	Identificador de la red a la cual pertenece el emisor de la aplicación. Asignado por el Registrador
Tipo	NetworkId (BS EN 1545)
Uso	Código identificador único del emisor de la aplicación interoperable. Se utiliza para verificar a qué red pertenece el emisor del medio de pago.

(2 bytes)	**IdEmisor**
Definición	Identificador de la entidad que emite la aplicación
Tipo	CompanyId (BS EN 1545)
Uso	Código identificador único del emisor de la aplicación interoperable en formato CompanyId según BS EN 1545-1. Se utiliza con fines de control de emisión de medios de pago.

(4 bytes)	**IdSAM**
Definición	Identificador del SAM usado en la emisión del medio de pago.
Tipo	SerialNumber (BS EN 1545)
Uso	Identificador de módulo SAM según Especificaciones Calypso Rev. 3.1. Se utiliza para llevar trazabilidad de las transacciones efectuadas con un medio de pago, y de los módulos de acceso seguro utilizados en transacciones débito, crédito, reembolso, emisión, etc., con el fin de controlar evasión y operaciones fraudulentas.

(2 bytes)	**FechaEmisión**
Definición	Fecha que en la que se emite la aplicación de transporte
Tipo	DateCompact (BS EN 1545)
Uso	Se utiliza para verificar la validez del medio de pago y garantizar la trazabilidad de la operación de emisión.

(2 bytes)	**FechaFinAplicación**
Definición	El día en que la aplicación ya no es válida
Tipo	EndDate (BS EN 1545)
Uso	Campo para registrar el fin de validez del perfil de usuario. Se utiliza para verificar la validez de una aplicación en el medio de pago durante el proceso de aceptación, también para efectos de cambio de estado de la aplicación. En caso de que no haya restricción para el fin de validez de la aplicación, el campo se llenará con 0xFFFF

2.1.1.5. Estructura de datos ESTADO_APLICACIÓN

Indica el estado de la aplicación interoperable con base en la definición de su ciclo de vida. Asimismo, almacena información sobre el número de acciones realizadas a través

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

de la lista LAM (ver Capítulo 4.1.11), para poder implementar acciones pendientes sobre el medio de pago.

Tabla 10. Estructura de datos para el archivo ESTADO APLICACIÓN en medios de pago recargables

Dato	Bytes	Descripción
EstadoAplicación	1	Indica estado de la aplicación con relación a su ciclo de vida
NúmeroAcciónAplicada	1	Contador de acciones que se han aplicado a través de la lista LAM
RFU	10	Reservado para uso futuro
Total	12	

(1 byte) EstadoAplicación

Definición	Indica el estado actual de la aplicación interoperable
Tipo	INT1 (BS EN 1545-1)
Uso	El campo puede tomar los siguientes valores - Inicializada (0) - Activada (1) - Desactivada (2) - Bloqueada (3) Se utiliza para determinar la validez de una aplicación durante el proceso de aceptación del medio de pago.

(1 byte) NúmeroAcciónAplicada

Definición	Indica el número acciones que se han aplicado en el medio de pago a través de la lista LAM
Tipo	INTEGER (0..255)
Uso	El contador es un número entero sin signo. Se puede llevar el conteo de hasta 255 acciones con la lista LAM. Cuando el NúmeroAcciónAplicada en el medio de pago es menor que NúmeroAcciónMedioPago en la lista LAM guardada en los terminales, es necesario efectuar una acción en el medio de pago para cambiar EstadoAplicación

2.1.1.6. Estructura de datos EVENTOS

Este archivo registra ciertos eventos efectuados con el medio de pago. Los eventos que se deben registrar en este archivo son:

- Distribución de producto
- Uso de producto
- Uso de producto con transbordo
- Recarga de producto
- Devolución de la tarifa

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- Devolución del monto de la última recarga
- Emisión del medio de pago

Para hacer más eficiente la lectura de este archivo se recomienda utilizar la funcionalidad "*Read Record Multiple*" descrita en [2]. La estructura de datos de cada registro en EVENTOS se especifica en la Tabla 11. Una coordenada GPS se representa en el campo IdUbicación de la siguiente forma:

- El primer byte corresponde a la parte entera de la coordenada de latitud en formato DD (decimal degrees). Este número se debe interpretar como un byte con signo.
- El segundo, tercer y cuarto byte corresponden a la parte decimal de la coordenada de latitud en formato DD (decimal degrees).
- El quinto byte corresponde a la parte entera de la coordenada de longitud en formato DD (decimal degrees). Este número se debe interpretar como un byte con signo.
- El sexto, séptimo y octavo byte corresponden a la parte decimal de la coordenada de longitud en formato DD (decimal degrees).

Ejemplo: la coordenada GPS 40.741895, -73.989308 se convierte de la siguiente forma:

Primer byte: 40 -> 0x30

Segundo, tercer y cuarto byte: 741895 -> 0x0B5207

Quinto byte: -73 -> 0xB7

Sexto, séptimo y octavo byte: 0x0F187C

Campo final: 0x300B5207B70F187C

Tabla 11. Estructura de datos para un registro del archivo EVENTOS en medios de pago recargables

Dato	Bytes	Descripción
IdProducto	2	Identificador del producto utilizado en la transacción registrada
PunteroProducto	1	Número del registro en el archivo CONTRATOS asociado a un producto con IdProducto
InformaciónGeneral	SEQ	Información principal del evento
IdEntidad	2	Código de identificación de la entidad que registra el evento
FechaHoraEvento	4	Fecha y hora del evento
TipoEvento	1	Tipo de evento
MontoEvento	4	Monto de la transacción (recarga, débito, devolución)
ConsecutivoEvento	3	Número consecutivo del evento en la tarjeta
IdDispositivo	2	Código de identificación del terminal que ejecuta la transacción
InformaciónUbicación	SEQ	Información de ubicación del evento
ConfigUbicación	1	Código que indica el tipo de dato utilizado para registrar la ubicación del evento

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

IdUbicación	8	Ubicación del evento. Corresponde al IdEstación o al IdBus según el subsistema
InformaciónAceptación	SEQ	Información de aceptación del evento
IdRuta	7	Identificador único de la ruta en el cual se hace uso del medio de pago
NúmeroTransbordos	1	Contador de transbordos efectuados durante la última ventana de tiempo disponible para transbordos
NúmeroPassbacks	1	Contador de passbacks efectuados durante la última ventana de tiempo disponible para passbacks
RFU	12	Reservado para uso futuro
Total	50	

(2 bytes) IdProducto

Definición	Identificador del producto en la red interoperable.
Tipo	ProductId (BS EN 1545-1)
Uso	Código identificador único asignado por el Registrador para el producto. Se utiliza para identificar un producto al momento de registrar un evento, asociado a una transacción con cierto producto.

(1 byte) PunteroProducto

Definición	Código que permite identificar los archivos asociados al producto
Tipo	InstancePointer (BS EN 1545-1)
Uso	El código puede tomar los valores desde 0x01 a 0x06 e indica el número del registro para cada producto en los archivos SERVICIOS y CONTRATOS, así como el número de contador en el archivo CONTADORES (en caso de que el producto use un contador). El valor de puntero producto NO puede repetirse en todo el archivo de LISTA_CONTRATOS

InformaciónGeneral	
Definición	Secuencia que almacena información general sobre un evento

(2 bytes) IdEntidad

Definición	Código de identificación de la entidad que ha generado el evento en el medio de pago
Tipo	CompanyId (BS EN 1545)
Uso	El identificador de la entidad que emite la aplicación de transporte. Es necesario para identificar la entidad que efectúa el evento (e.g., operador)

(4 bytes) FechaHoraEvento

Definición	Fecha y hora de ocurrencia del evento
Tipo	DateTimeCompact (BS EN 1545)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Uso	Secuencia de datos que registra la fecha y la hora del evento en formato DateTimeCompact según BS EN 1545-1. Se utiliza al momento de estimar tarifas condicionadas por eventos pasados (e.g., tarifas variables por distancia o transferencias).

(1 byte) TipoEvento

Definición	Indica el tipo de evento registrado en la aplicación
Tipo	INTEGER (0..255)
Uso	Valor entero entre 0x00 y 0xFF. Puede tomar los siguientes valores: - No especificado (0) - Distribución de producto (1) - Recarga de producto (2) - Emisión del medio de pago (3) - Modificación de datos de usuario (4) - Uso de producto (5) - Uso de producto con transbordo (6) - Uso de producto para salida de sistema cerrado (7) - Devolución de recarga (8) - Devolución de tarifa (9) - Reembolso del saldo (A) Se utiliza para identificar el tipo de transacción al momento de validar una operación registrada en el medio de pago, ya sea con fines de estimación de tarifa o con fines de control.

(4 bytes) MontoEvento

Definición	Indica el monto intercambiado entre el dispositivo y el medio de pago
Tipo	Amount (BS EN 1545)
Uso	Valor del monto para el evento en formato Amount según BS EN 1545. En el caso de un evento de Distribución de producto o Emisión del medio de pago, la unidad del monto corresponde a USD. De lo contrario la unidad de valor del monto es definida por IdProducto. Se utiliza para operaciones de devolución o para propósitos de verificación de saldo y control de evasión de pago.

(3 bytes) ConsecutivoEvento

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Definición	Número de eventos que se han registrado al momento de registrar un nuevo evento
Tipo	INTEGER (0..16777215)
Uso	Debe aumentarse en 1 respecto al evento anterior almacenado en la tarjeta. Si es el primer evento, su valor deberá ser 1.

(2 bytes) IdDispositivo

Definición	Identificador del dispositivo usado en el evento.
Tipo	DeviceId (BS EN 1545-1)
Uso	Este campo debe ser asignado por el registrador. Se utiliza para relacionar el dispositivo utilizado en la transacción con el medio de pago y el módulo SAM, con fines de control y trazabilidad transaccional.

InformaciónUbicación	
Definición	Secuencia de datos con información de la ubicación de un evento

(1 byte) ConfigUbicación

Definición	Código que indica el tipo de dato utilizado para registrar la ubicación del evento
Tipo	LocationQualifierCode (BS EN 1545-1)
Uso	Puede ser 0 si es un ID registrado por el Registrador y 16 si es una coordenada GPS.

(8 bytes) IdUbicación

Definición	Ubicación del evento
Tipo	LocationId (BS EN 1545-1)
Uso	Puede ser un ID definido por el Registrador para identificar una ubicación fija o una ruta de transporte. También puede ser una coordenada geográfica (por ejemplo, para registrar un evento de pago en un terminal de pago al interior de un vehículo en movimiento). En caso de ser una coordenada geográfica, los 4 bytes más significativos de Ubicación definen la latitud de la coordenada, y los 4 bytes menos significativos representan la longitud de la coordenada. Ambos campos deben estar en formato de punto flotante según IEEE 754. El valor de ubicación del evento puede ser útil para estimar tarifas basadas en distancia, o tarifas variables por zonas. También puede ser utilizado con fines de análisis de datos una vez se haya centralizado la información en la Cámara de Compensación.

InformaciónAceptación	
Definición	Secuencia de datos con Información sobre un evento de aceptación del medio de pago

(7 bytes) IdRuta

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Definición	Indica el tipo de modo de transporte usado en la transacción de aceptación del medio de pago
Tipo	OCTET STRING
Uso	El campo debe tomar el valor del identificador de la ruta en la cual se usa el medio de pago, al momento de registrarse el evento. Debido a que los identificadores pueden tener tamaños diferentes es necesario utilizar notación byte-alineada para completar el tamaño total del campo von veros (0), usando notación Big Endian

(1 bytes) NúmeroTransbordos

Definición	Contador de transbordos efectuados
Tipo	CountOfJourneyLegs (BS EN 1545-2)
Uso	El contador es un número que registra la cantidad de transbordos que se han realizado con el producto dentro de la ventana de tiempo disponible para que un usuario con cierto perfil haga transbordos. Se puede llevar el conteo de hasta 255 transbordos.

(1 byte) NúmeroPassbacks

Definición	Contador de passbacks acumulados
Tipo	NumberOfPassbacks (BS EN 1545-2)
Uso	El contador es un número que registra la cantidad de passbacks que se han realizado con el producto dentro de la ventana de tiempo disponible para que un usuario con cierto perfil haga passbacks. Se puede llevar el conteo de hasta 255 passbacks. Se utiliza para diferenciar la tarifa que se le debe aplicar al usuario en caso de que se use consecutivamente el mismo medio de pago en un terminal.

2.1.1.7. Estructura de datos CONTRATOS

Para hacer más eficiente la lectura de este archivo se recomienda utilizar la funcionalidad "*Read Record Multiple*" descrita en [2].

Cada uno de los registros en este archivo debe estar asociado con uno y solo un producto identificado por el campo IdProducto. Los registros deben almacenarse de tal forma que el registro número 1 sea el del producto con PunteroProducto (en el archivo de LISTA CONTRATOS) igual a 0x01, y así sucesivamente para los demás productos.

La estructura de datos de cada registro en CONTRATOS se presenta en la Tabla 12.

Tabla 12. Estructura de datos para un registro del archivo CONTRATOS en medios de pago recargables

Dato	Bytes	Descripción
IdProducto	2	Identificador del producto
DistribuidorProducto	SEQ	Información del distribuidor del producto
IdRedProducto	3	Identificador de la red interoperable a la que pertenece el producto
IdDistribuidorProducto	2	Identificador del distribuidor del producto

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

NúmeroReactivaciónProducto	2	Identifica la última reactivación de un producto previamente suspendido
NúmeroAcciónAplicadaProducto	2	Identifica la última acción remota sobre el medio de pago
FechaDistribución	4	Fecha y hora de la distribución del producto
ValidezProducto	SEQ	Información sobre la validez del producto
InicioValidezProducto	4	Fecha y hora de inicio de validez del producto
FinValidezProducto	4	Fecha y hora de fin de validez del producto
RFU	12	Reservado para uso futuro
Total	35	

(2 bytes)	**IdProducto**
Definición	Identificador del producto en la red interoperable.
Tipo	ProductId (BS EN 1545-1)
Uso	Código de identificación único asignado al producto.

DistribuidorProducto	
Definición	Secuencia de datos sobre distribuidor del producto

(3 bytes)	**IdRedProducto**
Definición	Identificador de la red interoperable a la cual pertenece el distribuidor del producto
Tipo	NetworkId (BS EN 1545-1)
Uso	Código de identificación único asignado la red a la que pertenece el distribuidor del producto. Se utiliza con fines de clasificación, control y trazabilidad de la información en el Sistema Central.

(2 bytes)	**IdDistribuidorProducto**
Definición	Identificador de la entidad que distribuye el producto
Tipo	CompanyId (BS EN 1545-1)
Uso	Código de identificación único asignado al distribuidor del producto. Se utiliza para identificar a la entidad que emite el medio de pago. Es útil para asociar cada una de las transacciones del medio de pago con su emisor entre Niveles 3 y 4 del modelo interoperable de flujo de información.

(2 bytes)	**NúmeroReactivaciónProducto**
Definición	Identifica la última reactivación de un producto que ha sido previamente suspendido a través de listas LAP_A

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Tipo	INTEGER (0..65535)
Uso	Valor en formato entero sin signo. Puede tomar valores de 0 a 65535. Se utiliza para verificar si es necesario aplicar una acción de reactivación o suspensión de producto en el medio de pago.

(2 bytes) NúmeroAcciónAplicadaProducto

Definición	Identifica la última acción sobre el producto llevada a cabo con listas LAP_R
Tipo	INTEGER (0..65535)
Uso	Valor en formato Entero sin signo. Puede tomar valores de 0 a 65535. Se utiliza para verificar si es necesario aplicar una acción de recarga de un producto en el medio de pago.

(4 bytes) FechaDistribución

Definición	Fecha y hora de distribución del producto
Tipo	DateTimeCompact (BS EN 1545-1)
Uso	Secuencia de datos que registra la fecha y la hora de la distribución del producto. Se utiliza para determinar la validez de un producto, también puede ser usado con fines de análisis de datos en el Sistema Central.

ValidezProducto	
Definición	Secuencia de datos con información sobre las restricciones de validez del producto almacenado en el medio de pago.

(4 bytes) InicioValidezProducto

Definición	Fecha y hora de inicio de la validez del producto
Tipo	DateTimeCompact (BS EN 1545-1)
Uso	Secuencia de datos que registra la fecha y la hora a partir de la cual empieza a ser válido un producto almacenado en el medio de pago. Se utiliza para determinar la validez de productos durante el proceso de aceptación de medios de pago. También para cambiar el estado de un producto.

(4 bytes) FinValidezProducto

Definición	Fecha y hora de vencimiento del producto
Tipo	DateTimeCompact (BS EN 1545-1)
Uso	Secuencia de datos que registra la fecha y la hora a partir de la cual deja de ser válido un producto almacenado en el medio de pago. Se utiliza para determinar la validez de productos durante el proceso de aceptación de medios de pago. También para cambiar el estado de un producto. Si no hay restricción de validez se llena con 0xFFFFFFFF

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

2.1.1.8. Estructura de datos LISTA_CONTRATOS

Almacena una secuencia de datos que indica los productos almacenados en el medio de pago. Su propósito es determinar la disponibilidad y prioridad de uso de cada producto. La información de cada producto está almacenada en grupos de 7 bytes dentro del archivo.

La estructura de datos de cada grupo de bytes en LISTA_CONTRATOS se presenta en la Tabla 13.

Tabla 13. Estructura de datos para cada grupo de bytes (que representa un producto) dentro de LISTA CONTRATOS en medios de pago recargables

Dato	Bytes	Descripción
IdProducto	2	Identificador del producto
PunteroProducto	1	Identificador de la información del producto en particular en los archivos de CONTRATOS, SERVICIOS y CONTADORES
PrioridadProducto	1	Número que denota la prioridad del producto
RFU	3	Reservado para uso futuro

(2 bytes) IdProducto

Definición	Código que identifica el producto en la red interoperable.
Tipo	ProductId (BS EN 1545-1)
Uso	Código de identificación único asignado por el Registrador para el producto almacenado en el medio de pago. Se utiliza para identificar el producto que va a utilizarse al momento de efectuar una transacción de aceptación.

(1 byte) PunteroProducto

Definición	Código que permite identificar los archivos asociados al producto
Tipo	InstancePointer (BS EN 1545-1)
Uso	El código puede tomar los valores desde 0x01 a 0x06 e indica el número del registro para cada producto en los archivos SERVICIOS y CONTRATOS, así como el número de contador en el archivo CONTADORES (en caso de que el producto use un contador). El valor de puntero producto NO puede repetirse en todo el archivo de LISTA_CONTRATOS

(1 byte) PrioridadProducto

Definición	Número que denota la prioridad del producto
Tipo	INTEGER (0..255)
Uso	Se debe tener en cuenta en transacciones de uso de productos.

2.1.1.9. Estructura de datos SERVICIOS

Para hacer más eficiente la lectura de este archivo se recomienda utilizar la funcionalidad "*Read Record Multiple*" descrita en [2].

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Al igual que para el archivo CONTRATOS, cada uno de los registros en este archivo debe estar asociado con uno y solo un producto, identificado con el campo IdProducto. Los registros deben almacenarse de tal forma que el registro número 1 sea el del producto con PunteroProducto (en el archivo de LISTA_CONTRATOS) igual a 0x01, y así sucesivamente para los demás productos.

La estructura de datos de cada registro en SERVICIOS se presenta en la Tabla 14.

Tabla 14. Estructura de datos para el archivo SERVICIOS en medios de pago Calypso

Dato	Bytes	Descripción
IdProducto	2	Identificador del producto
EstadoProducto	1	Denota el estado de un producto en la aplicación interoperable
NúmeroSemanaAño	1	Número de la semana del año en la cual se realizó la última transacción de aceptación del medio de pago
NúmeroViajesDíaSemana	4	Contador de los viajes que ha realizado el usuario cada día de la semana
NúmeroViajesMes	2	Contador de los viajes que ha realizado el usuario en el mes
NúmeroActualAceptaciones	2	Contador del número total de transacciones de aceptación de medio de pago realizadas con el producto
RFU	8	Reservado para uso futuro
Total	20	

(2 bytes) IdProducto

Definición	Código que identifica el producto en la red interoperable.
Tipo	ProductId (BS EN 1545-1)
Uso	Código de identificación único asignado por el Registrador para el producto almacenado en el medio de pago. Se utiliza para identificar el producto que va a utilizarse al momento de efectuar una transacción de aceptación.

(1 bytes) EstadoProducto

Definición	Indica el estado actual del producto
Tipo	INTEGER (0..3)
Uso	Puede tomar los siguientes valores: - Inicializado (0) - Activado (1) - Suspendido (2) Se utiliza para verificar la validez de un producto para cualquier transacción que lo requiera.

(1 byte) NúmeroSemanaAño

Definición	Semana del año en la que se efectuó el último uso del producto

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Tipo	ISO 8601
Uso	Este dato determina la última semana del año en la cual se realizó la última transacción de aceptación de medio de pago con el producto. Se utiliza para reiniciar los contadores NúmeroViajesSemana y NúmeroViajesMes, asociados al número de viajes por semana.

(4 bytes) NúmeroViajesDíaSemana

Definición	Contador de uso que se ha hecho por día de la semana con el producto
Tipo	TripsPerDayOfWeek (BS EN 1545-2)
Uso	Contador de los viajes que ha realizado el usuario cada día de la semana. Nunca debe superar los valores máximos definidos en los archivos de parámetros de los terminales. En el caso de que se trate de un transbordo no se debe sumar un viaje. Este contador se puede utilizar para controlar la cantidad de viajes que un usuario hace con un producto por semana.

(2 bytes) NúmeroViajesMes

Definición	Contador de viajes efectuados en el mes con el producto
Tipo	Quantity (BS EN 1545-1) / CountOfJourneysPerPeriod (BS EN 1545-2)
Uso	Este campo posee dos contadores, los primeros 4 bits del dato indican el número del mes, este campo deberá tomar valores entre 1 y 12 únicamente. Los siguientes 12 bits se usarán para contar el número de aceptaciones por mes y debe volver a cero en cada cambio de mes. Este campo es útil para limitar la cantidad de viajes que hace un usuario al mes, en caso de que se emita un producto especial con ese tipo de restricción.

(2 bytes) NúmeroActualAceptaciones

Definición	Contador del número total de aceptaciones del producto
Tipo	Quantity (BS EN 1545-1)
Uso	Número total de transacciones de aceptación de medio de pago realizadas con el producto. Un viaje puede incluir varios productos usados en las diferentes transacciones de aceptación que conforman dicho viaje. Los transbordos no se contabilizan como viajes. Este contador no debe volver a cero bajo ninguna circunstancia.

2.1.1.10. Estructura de datos CONTADORES

El archivo de CONTADORES permite almacenar información de valor en unidades de viajes para productos especiales en un único registro. El registro de Contadores se divide en 6 campos, cada uno de 3 bytes. El número de cada contador debe asociarse al campo PunteroProducto del archivo LISTA_CONTRATOS, es decir, el valor de PunteroProducto 0x01 indica que el contador para este producto es el número 1.

La estructura de datos del archivo CONTADORES se especifica en la Tabla 15.

Tabla 15. Estructura de datos para el archivo CONTADORES en medios de pago recargables

Dato	Bytes	Descripción

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Contadores	18	Registro con contadores para almacenar información de valor de cualquiera de los 6 productos disponibles en la aplicación.
Total	18	

(12 bytes)	**Contadores**
Definición	Registro con contadores para información de valor de productos
Tipo	Cada campo en el registro es tipo Quantity (BS EN 1545-1)
Uso	El registro debe dividirse en 6 partes, cada una de ellas asociada a un contador (valor de producto) y se debe garantizar que cada contador sea un entero de 3 bytes.

2.1.4 Aplicación MONEDERO

El **MONEDERO** es una aplicación especial de Calypso denominada *Stored Value* [2], y se utiliza para administrar las unidades de transporte en USD que se almacenan en el medio de pago para acceder a los servicios del SITM-Q. Este directorio se compone de los EF RECARGAS (*Loads Log*) y COMPRAS (*Purchase Log*), los cuales deben ser incluidos únicamente para cumplir con los requerimientos del estándar Calypso Rev. 3.1.

El valor almacenado en la aplicación **MONEDERO** se denotará ValorMonedero.

No es necesario hacer uso de la información almacenada en RECARGAS o en COMPRAS para hacer ejecutar las funcionalidades del Capítulo 4.1.

Tabla 16. Estructura de archivos y condiciones de acceso para el MONEDERO en medios de pago Calypso

				Grupo 0	**Grupo 1**	**Grupo 2**	**Grupo 3**
Archivo	**Tipo**	**Registros**	**Tamaño Registro (bytes)**	**Leer Rehabilitar**	**Actualizar Invalidar**	**Escribir Disminuir**	**Agregar Aumentar**
MONEDERO (SV)							
RECARGAS	Cíclico	1	29	Siempre	Nunca	Nunca	Nunca
COMPRAS	Cíclico	3	29	Siempre	Nunca	Nunca	Nunca

2.1.1.11. Estructura de datos RECARGAS

Tabla 17. Estructura de datos para el archivo RECARGAS en medios de pago Calypso

Dato	Bytes	Descripción
FechaCarga	2	Fecha en la que se realiza la transacción de recarga
RFU	1	Reservado para uso futuro
KVC	1	Versión de la llave con la que se efectúa la transacción de recarga
RFU	1	Reservado para uso futuro

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

NuevoSaldo	3	Saldo en el monedero después de realizada la última transacción de recarga
MontoCarga	3	Monto de la recarga
TiempoCarga	2	Hora en la que se hace la recarga del monedero
IdSamCarga	4	Identificador del SAM con el que se hace la recarga
ConsecutivoRecargaSAM	3	Consecutivo de transacción de recarga en el SAM
ConsecutivoRecargaTarjeta	2	Consecutivo de transacción de recarga en la tarjeta
FirmaLo	3	Los 3 MSBytes de la firma utilizada para la recarga
RFU	4	Reservado para uso futuro
Total	29	

(2 bytes) FechaCarga

Definición	Fecha en la que se registra el evento de recarga de **MONEDERO**
Tipo	Date (Calypso Rev. 3.1)
Uso	La fecha se registra en formato DateCompact según BS EN 1545-1. Calypso Rev. 3.1 (Stored Value - Load Log: Date)

(1 byte) KVC

Definición	Versión de la llave usada para la transacción de recarga
	KVC (Calypso Rev. 3.1)
Uso	Calypso Rev. 3.1 (Stored Value - Load Log: KVC)

(3 bytes) NuevoSaldo

Definición	Valor de saldo almacenado en el MONEDERO después de la recarga
Tipo	Balance (Calypso Rev. 3.1)
Uso	Debe utilizarse como binario entero con signo. Calypso Rev. 3.1 (Stored Value - Load Log: Balance)

(3 bytes) MontoCarga

Definición	Valor de la recarga efectuada al MONEDERO
Tipo	Amount (Calypso Rev. 3.1)
Uso	Debe utilizarse como binario entero con signo. Calypso Rev. 3.1 (Stored Value - Load Log: Balance)

(2 bytes) TiempoCarga

Definición	Hora a la que se efectúa la recarga del MONEDERO
Tipo	Time (Calypso Rev. 3.1)
Uso	La hora debe almacenarse en formato TimeCompact según BS EN 1545-1 Calypso Rev. 3.1 (Stored Value - Load Log: Time)

(4 bytes) IdSamCarga

Definición	Identificador único del SAM utilizado para hacer la recarga
Tipo	SAM ID (Calypso Rev. 3.1)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Uso	Identificador de módulo SAM según Especificaciones Calypso Rev. 3.1 Calypso Rev. 3.1 (Stored Value - Load Log: SAM ID)

(3 bytes) ConsecutivoRecargaSAM

Definición	Número de recargas realizadas con el SAM después de que se efectúa la recarga del MONEDERO
Tipo	SAM TNum (Calypso Rev. 3.1)
Uso	Número consecutivo generado por el SAM al momento de efectuar la transacción de recarga. Se genera según lo especificado en las Especificaciones Calypso 3.1 Calypso Rev. 3.1 (Stored Value - Load Log: SAM TNum)

(2 bytes) ConsecutivoRecargaTarjeta

Definición	Número de recargas realizadas al MONEDERO después de que se efectúa la recarga del **MONEDERO**
Tipo	SV TNum (Calypso Rev. 3.1)
Uso	Número consecutivo generado por la tarjeta al momento de efectuar la transacción de recarga. Calypso Rev. 3.1 (Stored Value - Load Log: SV TNum)

(3 bytes) FirmaLo

Definición	Los 3 MSBytes de la firma utilizada para la recarga
Tipo	SignatureLo (Calypso Rev. 3.1)
Uso	Calypso Rev. 3.1 (Stored Value - Load Log: SignatureLo)

2.1.1.12. Estructura de datos COMPRAS

Tabla 18. Estructura de datos para el archivo COMPRAS en medios de pago Calypso

Dato	Bytes	Descripción
MontoCompra	2	Monto de la compra
FechaCompra	2	Fecha en la que se realiza la transacción de compra
TiempoCompra	2	Hora en la que se hace la compra con el monedero
KVC	1	Versión de la llave con la que se efectúa la transacción de compra
IdSamCompra	4	Identificador del SAM con el que se hace la recarga
ConsecutivoCompraSAM	3	Consecutivo de transacción de compra en el SAM
NuevoSaldo	3	Saldo en el monedero después de realizada la última transacción de compra
ConsecutivoCompraTarjeta	2	Consecutivo de transacción de compra en la tarjeta
FirmaLo	3	Los 3 MSBytes de la firma utilizada para la compra
RFU	7	Reservado para uso futuro
Total	29	

(2 bytes) MontoCompra

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Definición	Valor de la compra efectuada con el MONEDERO
Tipo	Amount (Calypso Rev. 3.1)
Uso	Debe utilizarse como binario entero con signo. Se define en las Especificaciones Calypso Rev. 3.1 como Amount, como parte de la aplicación Stored Value (MONEDERO). Su valor debe ser positivo y menor que el saldo almacenado en el MONEDERO al momento de efectuar la compra. Calypso Rev. 3.1 (Stored Value - Purchase Log: Amount)

(2 bytes) FechaCompra

Definición	Fecha en la que se registra el evento de compra con el MONEDERO
Tipo	Date (Calypso Rev. 3.1)
Uso	La fecha se registra en formato DateCompact según BS EN 1545-1 Calypso Rev. 3.1 (Stored Value - Purchase Log: Date)

(2 bytes) TiempoCompra

Definición	Hora a la que se efectúa la compra con el MONEDERO
Tipo	Time (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero. Se registra como TimeCompact según BS EN 1545-1. Calypso Rev. 3.1 (Stored Value - Purchase Log: Time)

(1 byte) KVC

Definición	Versión de la llave usada para la transacción de recarga
Tipo	KVC (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero. Calypso Rev. 3.1 (Stored Value - Purchase Log: KVC)

(4 bytes) IdSamCompra

Definición	Identificador único del SAM utilizado para hacer la compra
Tipo	SAM ID (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero. Calypso Rev. 3.1 (Stored Value - Purchase Log: SAM ID)

(3 bytes) ConsecutivoCompraSAM

Definición	Número de compras realizadas con el SAM después de que se efectúa la compra con el MONEDERO
Tipo	SAM TNum (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero. Calypso Rev. 3.1 (Stored Value - Purchase Log: SAM TNum)

(3 bytes) NuevoSaldo

Definición	Valor de saldo almacenado en el MONEDERO después de la compra
Tipo	Balance (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero Calypso Rev. 3.1 (Stored Value - Purchase Log: Balance)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

(2 bytes)	ConsecutivoCompraTarjeta
Definición	Número de compras realizadas con el MONEDERO después de que se efectúa la compra con el MONEDERO
Tipo	SV TNum (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero Calypso Rev. 3.1 (Stored Value - Purchase Log: SV TNum)

(3 bytes)	FirmaLo
Definición	Los 3 MSBytes de la firma utilizada para la compra
Tipo	SignatureLo (Calypso Rev. 3.1)
Uso	Se utiliza para registrar la última transacción de compra con el monedero Calypso Rev. 3.1 (Stored Value - Purchase Log: SignatureLo)

2.2 Aplicación interoperable en medios de pago no recargables

El medio de pago MIFARE Ultralight EV1 es una tarjeta de bajo costo que permite ofrecer una alternativa a los medios de pago recargables con la aplicación interoperable. En la red interoperable se exige usar como mínimo la variante MF0UL11 [3] con un espacio de datos de usuario de 384 bits. Esta tarjeta consta de una memoria fija compuesta por páginas. Cada una de estas destinada a diferentes funciones como se muestra a continuación:

<table>
<tr><th>Página</th><th colspan="4">Número de byte en la página</th><th>Descripción</th></tr>
<tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td></td></tr>
<tr><td>0x00</td><td colspan="4">Número serial</td><td rowspan="3">Datos de fabricación y bytes de bloqueo (Lock bytes)</td></tr>
<tr><td>0x01</td><td colspan="4">Número serial</td></tr>
<tr><td>0x02</td><td>Número serial</td><td>Datos internos</td><td colspan="2">Lock bytes</td></tr>
<tr><td>0x03</td><td>OTP</td><td>OTP</td><td>OTP</td><td>OTP</td><td>Bytes de programación única (One Time Programmable)</td></tr>
<tr><td>0x04</td><td colspan="4" rowspan="5">Memoria de usuario</td><td rowspan="5">Páginas de almacenamiento libre de datos</td></tr>
<tr><td>0x05</td></tr>
<tr><td>…</td></tr>
<tr><td>0x0E</td></tr>
<tr><td>0x0F</td></tr>
<tr><td>0x10</td><td colspan="4">CFG0</td><td rowspan="4">Páginas de configuración</td></tr>
<tr><td>0x11</td><td colspan="4">CFG1</td></tr>
<tr><td>0x12</td><td colspan="4">PWD</td></tr>
<tr><td>0x13</td><td colspan="2">PACK</td><td colspan="2">RFUI</td></tr>
<tr><td></td><td colspan="4">Contadores de un solo sentido</td><td>Tres contadores de 24 bits cada uno</td></tr>
</table>

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- Las páginas 0x00, 0x01 y 0x02 están destinadas a almacenar el UID de 7 bytes de la tarjeta, así como los *lock bytes* que definen las capacidades de lectura y escritura de cada página.
- La página 3 almacena los 4 bytes de programación única (OTP). Cada bit de los OTP puede ser escrito únicamente una vez. A pesar de que es posible usarlo como un contador de 32 estados, no se debe hacer uso de los campos OTP para que los medios de pago no recargables puedan ser reutilizados.
- La memoria de usuario se ubica entre las páginas 0x04 y 0x0F. Esta permite la lectura y escritura libre de los datos.
- Las páginas 0x10, 0x11, 0x12 se denominan páginas de configuración. Estas almacenan diferentes parámetros que definen la accesibilidad de los datos almacenados en la tarjeta, así como una contraseña que puede brindar protección básica a la escritura o lectura de los datos.
- Por último, existen 3 contadores de un solo sentido. Estos contadores solo pueden ser incrementados hasta alcanzar un valor máximo de 0xFFFFFF. Una vez se llega a este valor cada contador no puede ser usado de nuevo.

2.2.1 Estructura de datos interoperable para medios de pago no recargables

Los medios de pago MIFARE Ultralight EV1 deben hacer uso de la memoria de usuario para almacenar la información de emisión del medio de pago, así como el último evento de aceptación del medio de pago efectuado con este.

Adicionalmente se debe almacenar un saldo utilizando el contador # 1 del medio de pago.

Los datos de emisión se deben almacenar al momento de escribir en el medio de pago por primera vez en la emisión de esta. A continuación, se describen los datos que se deben almacenar.

Tabla 19. Estructura de datos de emisión en medios de pago no recargables

Nombre del dato	Tipo de dato	Tamaño (bytes)	Descripción
VersiónAplicación	VersionNumber (BS 1545)	1	Se refiere a la versión de la aplicación almacenada en el medio de pago. 4 primeros bits vara versión mayor y siguientes 4 bits para versión menor. La versión inicial debe ser 1.0. (0x10)
IdRed	NetworkId (BS 1545)	3	Red de aceptación de origen del medio de pago
IdEmisor	CompanyId (BS 1545)	2	Código de identificación de la entidad que ha emitido el medio de pago
FechaEmisiónMedioPago	DateCompact (BS 1545)	2	Fecha en que el medio de pago fue emitido en la red interoperable

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

FechaFinValidezMedioPago	EndDate (BS 1545)	2	El día en que el medio de pago ya no es válido. Representa el número de días transcurridos desde el 1 de enero de 2010
		10	**Tamaño total**

Los datos de último uso se deben almacenar cada vez que se usa el medio de pago en una transacción de aceptación del medio de pago en la red interoperable. A continuación, se describen los datos que se deben almacenar.

Tabla 20. Estructura de datos de transacciones para medios de pago no recargables.

Nombre del dato	Tipo de dato	Tamaño (bytes)	Descripción
IdEntidad	CompanyId	2	Código de identificación de la entidad que ha generado el evento en el medio de pago
FechaHoraEvento	DateTimeCompact	4	Fecha y hora de ocurrencia del evento
TipoEvento	Integer (0..255)	1	Indica el tipo de evento registrado en la aplicación. - Emisión del medio de pago precargado (3) - Uso de medio de pago precargado (5) - Uso de medio de pago precargado para salida de sistema cerrado (7)
MontoEvento	Amount	2	Tarifa aplicada en el evento de uso de medio de pago precargado, o en la emisión del medio de pago.
IdDispositivo	DeviceId	2	Identificador del dispositivo usado en el evento
IdUbicación	LocationId	8	Ubicación del evento. Corresponde al IdEstación o al IdBus según el subsistema
IdRuta	OCTET STRING	7	Indica la información de ruta a la que ingresa el usuario haciendo uso del medio de pago, debe registrarse siguiendo los mismos lineamientos para identificadores reportados en el Capítulo 3.2.1.
		26	**Tamaño total**

El saldo del medio de pago precargado se compone de unidades de transporte que corresponden a centavos de USD. Este saldo se calcula con base en el valor almacenado en el contador # 1 del medio de pago. Debido a que solo es posible incrementar el valor del contador, el saldo del medio de pago se debe calcular con la siguiente fórmula:

$$Saldo\ disponible = 0\text{xFFFFFF} - Valor\ Contador\ \#\ 1$$

En este sentido, si se quisiera precargar el medio de pago con 200 USD (20.000 centavos = 0x004E20), el valor del contador #1 debería ser de 0xFFB1DF. Por último, siempre se debe almacenar en el medio de pago una firma digital generada con la función PSO del SAM-C1 [11]. Esta se obtiene mediante un cálculo criptográfico que procesa los datos almacenados en el medio de pago y que representan estado de este. La firma digital PSO permite verificar que el estado alcanzado en el medio de pago fue logrado con un SAM válido dentro de la red interoperable.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Los datos de emisión, los datos de último evento y la firma PSO deben ser almacenados de la siguiente manera en la memoria del medio de pago:

Página	Número de byte en la página			
	1	**2**	**3**	**4**
0x04	Datos de emisión			
0x05	Datos de emisión			
0x06	Datos de emisión		RFU	RFU
0x07	Datos de último evento			
0x08	Datos de último evento			
0x09	Datos de último evento			
0x0A	Datos de último evento			
0x0B	Datos de último evento			
0x0C	Datos de último evento			
0x0D	Datos de último evento		RFU	RFU
0x0E	RFU	RFU	RFU	RFU
0x0F	PSO *digital signature*			
	Contador #1 (Saldo disponible)			

2.2.2 Parámetros adicionales

A continuación, se describen ciertos parámetros que deben ser ajustados para el correcto uso del medio de pago.

- Una vez almacenados los datos de emisión en el medio de pago, se deben bloquear las páginas que almacenan estos datos y los OTP bytes. Por lo tanto, el byte 2 de la página 2 (*lock byte* 0) debe tomar el valor de 0xF8
- El byte 3 de la página 2 (*lock byte* 1) no debe ser modificado y debe permanecer con el valor 0x00
- Las páginas 0x10, 0x11, 0x12 y 0x13 (páginas de configuración) no deben ser modificadas y deben permanecer con los valores establecidos por defecto.

2.2.3 Seguridad

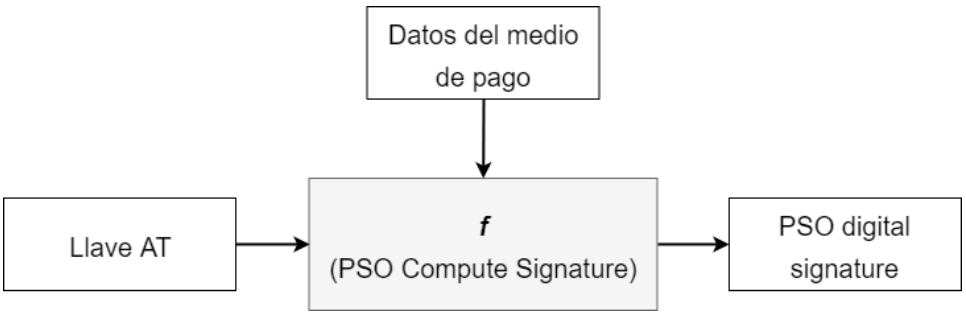
La seguridad del medio de pago precargado está basada en la firma digital PSO que se almacena en el mismo. Esta busca contrarrestar intentos de clonación o alteración de medios de pago precargados. A pesar de esto la efectividad de esta medida depende en su totalidad de los dispositivos lectores de medios de pago. Esto se debe a que deben ser estos quienes deben verificar la firma de efectuar una transacción de aceptación con un medio de pago precargado, así como recalcular y grabar una nueva firma PSO cada vez que se escribe nueva información en este. Por lo tanto, todos los dispositivos lectores de medios de pago de la red interoperable deben incorporar funcionalidades de cálculo y verificación de firmas digitales PSO, mediante el uso de módulos SAM-C1, para todas las transacciones que se lleven a cabo con los medios de pago no recargables.

El cálculo de la *firma digital* se lleva a cabo mediante la siguiente función:

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

$$Firma\ PSO\ = f(llave, datos\ del\ medio\ de\ pago)$$

Figura 6. Función para cálculo del CMAC de estado para medios de pago precargados



Fuente: elaboración propia

La función f se define en [11] como PSO Compute Signature. Para el uso de esta función es necesario garantizar que:

- La llave AT sea diversificada, tomando como diversificador el serial del SAM que almacena la llave
- El tamaño de la firma digital PSO debe ser de 4 bytes
- Los datos del medio de pago usados en el cálculo de la firma digital consisten en una secuencia de 58 bytes compuestos por los siguientes datos del medio de pago:
  - Datos almacenados entre las páginas 0x00 y 0x0E (60 bytes)
  - Valor del contador # 1 (3 bytes)
  - UID del medio de pago (7 bytes)

El cálculo y verificación la firma PSO debe ser realizado únicamente por el SAM del dispositivo lector de medios de pago.

3 Datos en terminales de aceptación de medios de pago

Todos los terminales (i.e., dispositivos de cobro, recarga, o verificación de validez de medios de pago) que sean utilizados para aceptación de medios de pago deben almacenar archivos de parámetros con información tarifaria para cada uno de los días de operación del sistema. Asimismo, cada terminal de pago debe estar asociado a un único esquema tarifario, así como a un grupo de rutas específico dentro de un subsistema y una red interoperable particulares. Esta información debe estar codificada en formato XML de conformidad con los esquemas XML (XSD) que se presentan en [12], [13] y [14].

Particularmente, la información con las reglas tarifarias del sistema debe quedar almacenada en el archivo TARIFAS.xml, la información asociada al terminal debe

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

guardarse en el archivo TERMINAL.xml, y la información asociada a los días de operación del sistema debe guardarse en el archivo DIAS.xml.

El propósito de estos archivos es facilitar la actualización de la información de tarifas en caso de que haya un cambio en la regulación tarifaria, ya que con base en la información que se guarda en ellos se definen las tarifas para el usuario.

Es importante tener en cuenta que todos los campos que sean de tipo *string* (a excepción de los atributos identificadores) en los archivos de parámetros deben escribirse en mayúsculas y sin espacios (el espacio puede reemplazarse por guion bajo "_").

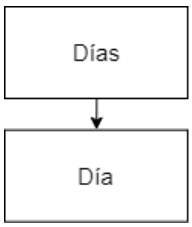
3.1 Archivo con información de días de operación

El archivo DIAS.xml permite clasificar los días del año por tipo, para relacionarlos con las reglas de operación del sistema y con el esquema tarifario. El archivo se compone de dos tipos de datos estructurados como se muestra en la Figura 7. La estructura Días debe contener 365 valores de Día (366 para años bisiestos), uno para cada día del año, y para cada día es necesario definir un tipo. La estructura Día debe definirse así:

Día

Atributo	NumeroDia: hace referencia al número del día del año. Este dato debe tomar valores entre 1 y 365 únicamente.
Valor	TipoDia: código para determinar el tipo de día.

Figura 7. Esquema de datos estructurados en el archivo DIAS.xml almacenado en terminales



Fuente: elaboración propia

Es importante tener en cuenta que un día del año solo puede y debe estar asociado a un tipo de día específico. Los tipos de días deben definirlos las autoridades que establecen las reglas y tarifas para cada uno de los subsistemas del SITM-Q.

Ejemplo:

El lunes 1 de enero es día feriado, y se ha determinado una regla tarifaria especial para ese día. Por esta razón, es necesario diferenciarlo de todos los demás como día feriado, haciendo uso de un registro Día en el archivo DIAS.xml así:

```
<Dia NumeroDia="1">
    <TipoDia>FERIADO</TipoDia>
</Dia>
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

3.2 Archivo con información de tarifas y validez de productos

El archivo TARIFAS.xml (ver Figura 8), guarda dos conjuntos de reglas (i.e., ReglasTarifas y ReglasValidez). El primero está directamente relacionado con el esquema tarifario, y el segundo está relacionado con la validez de los productos que se pueden almacenar en un medio de pago.

Los Operadores de Recaudo del SIR deben aplicar la regulación tarifaria a cada subsistema con base en la regulación tarifaria vigente para el SITM-Q.

Las reglas tarifarias que pueden aplicarse a un usuario al momento de efectuarse una transacción de pago se definen a partir del contenido de ReglasTarifas en TARIFAS.xml, cuya estructura se diseña para poder aplicar el esquema tarifario vigente para el DMQ [4]. Específicamente:

1. Tarificación plana o única: precio fijo por viaje que permite al usuario realizar Transbordos de forma independiente a la distancia recorrida.

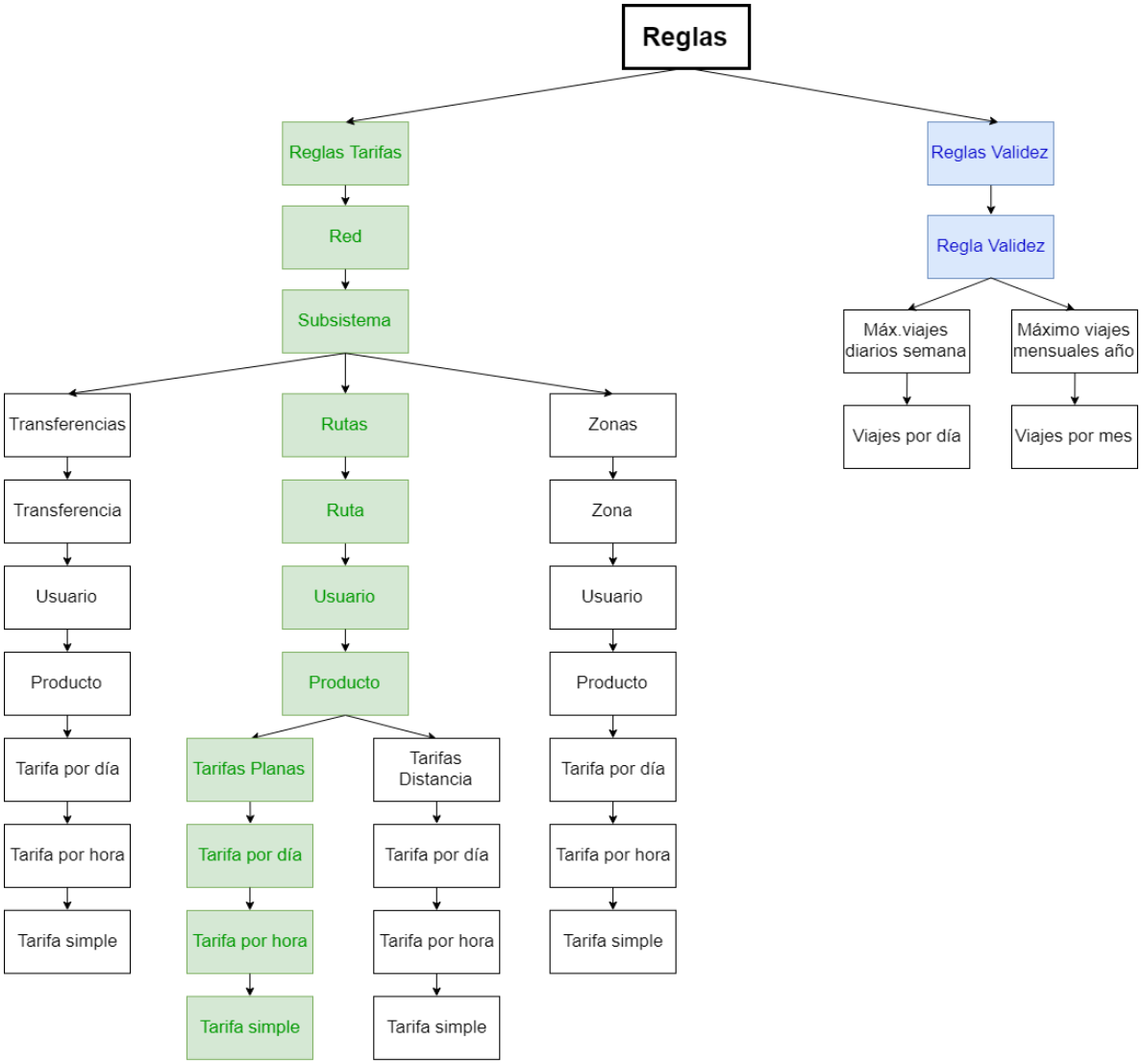
2. Tarifa variable por distancia de recorrido: precio diferencial de acuerdo con el uso que se haga del servicio de transporte. Se determina con base en la cantidad de kilómetros recorridos desde que se realiza la validación de acceso a uno de los subsistemas de transporte hasta el momento que se produce la salida de este.

3. Tarifa variable por etapas o Transbordos: precio diferenciado en función del número de intercambios o Transbordos que el usuario realice en cada viaje entre los subsistemas del SITM-Q, durante un periodo de tiempo autorizado.

4. Tarifa por zona: precio basado en el cobro por zonas dividiendo la ciudad en zonas y realizando el cobro de acuerdo con el número de zonas transitadas por el viajero.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 8. Esquema de datos estructurados en el archivo TARIFAS.xml almacenado en terminales



Fuente: elaboración propia

Las tarifas podrán ser fijadas en unidades de centavos de USD o en unidades de viajes, diferenciándose por red, subsistema, y ruta simple, ruta compuesta, zona, o transferencia. También por usuario y producto (ver Figura 8), teniendo en cuenta las tarifas preferenciales en [4] y también considerando que se ha establecido la posibilidad de hacer cobro de tarifas a través de abonos diarios, semanales o mensuales que permiten cierto número de viajes o viajes ilimitados en una ruta, zona o en todo el sistema. Esto aplica para todos los tipos de productos que pueden almacenarse en un medio de pago, según lo establecido en este documento. Otra consideración importante es que las tarifas pueden diferenciarse por hora o tipo de día.

Para definir el esquema tarifario vigente para el SITM-Q en el archivo TERMINAL.xml, será necesario utilizar los datos estructurados marcados en verde en la Figura 8. Se deja abierta la posibilidad de efectuar cobros diferenciados por zonas, Transbordos y

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

distancia, haciendo uso de las estructuras en blanco de la Figura 8. Adicionalmente, para el caso de las tarifas variables por distancia, será posible fijar tarifas en unidades de centavos de USD por kilómetro.

En la Figura 8 las estructuras de datos marcadas en azul hacen referencia a restricciones de validez que deben utilizarse para fijar limitaciones de saldo para cada producto (por ejemplo, las restricciones del producto especial para invidentes). Se deja abierta la posibilidad de limitar el número de viajes por día, semana o mes, según lo establecido en [4].

A continuación, se presenta una descripción de las especificaciones que deben tener los identificadores de las estructuras de datos en TARIFAS.xml, junto con una descripción de detallada de los tipos de tarifas que pueden almacenarse en TARIFAS.xml y la forma como deben definirse cada uno de los esquemas tarifarios descritos anteriormente. Finalmente, se presentan las especificaciones para definir reglas de validez de un producto.

3.2.1 Identificadores

Para todos los datos estructurados en TARIFAS.xml que tengan un atributo identificador, i.e., Usuario (IdUsuario), Red (IdRed), Subsistema (IdSubsistema), Ruta (IdRuta), Zona (IdZona), Tarifa (IdProducto), se puede utilizar como identificador el carácter **"*"** para denotar que la regla aplica para todas las redes, subsistemas, rutas, zonas, o productos que no estén especificadas con otra estructura de datos del mismo tipo y cuyo identificador sea diferente a **"*"**. En otras palabras, toda la información encerrada dentro de la estructura con identificador igual a **"*"** debe utilizarse para definir el caso por defecto.

Por ejemplo, si una estructura Ruta se define con `IdRuta="*"`, su información debe utilizarse para todas las rutas que no estén especificadas por otra estructura Ruta.

Es importante tener en cuenta que en caso de que nuevas redes, subsistemas, rutas, transferencias, zonas, perfiles de usuario, o productos se definan para el SIR, será necesario que el Registrador les asigne nuevos códigos siguiendo los lineamientos que se describen a continuación. Todos los identificadores que no se especifiquen en esta norma deben ser definidos por el Registrador. El carácter `"*"` (asterisco) es reservado y no puede utilizarse en los identificadores de ningún tipo de dato en los archivos de parámetros del terminal.

Ahora bien, todos los identificadores distintos de `"*"` deben:

- Ser cadenas de caracteres. Los caracteres solo pueden tomar los siguientes valores: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
- Ser únicos
- Cada carácter del identificador tendrá un orden así:

0	**A**	…	**1**
Primer	Segundo		Último

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Carácter Carácter Carácter

- Cumplir con especificaciones de tamaño y orden según su tipo que se denotan a continuación.

3.1.1.1 Identificador de Red

El identificador debe ser de 6 caracteres y debe asociarse al valor hexadecimal tipo NetworkId [15] almacenado en el medio de pago. Teniendo en cuenta que solo existe una red actualmente, que es la del SITM-Q, su identificador se determina a continuación:

Ejemplo: el identificador de red para el SITM-Q que debe almacenarse en el medio de pago es 0x218000, por lo tanto, su identificador en el archivo de parámetros debe ser igual a $\mathrm{IdRed} = \text{”}218000\text{”}$.

El valor de este campo se determina de la siguiente forma:

Código ISO 3166 para Ecuador (218 = 0b001000011000)

Código para la red del SITM-Q en Ecuador (0 = 0b000000000000)

Por lo tanto $\mathrm{IdRed} = \text{”}0\mathrm{b}001000011000000000000000\text{”}$

3.1.1.2 Identificador de Subsistema

El identificador debe ser de 10 caracteres en formato “RRRRRRSSSS”. Los primeros seis caracteres deben ser iguales al identificador de la red a la cual pertenece el subsistema. Los caracteres 7 a 10 deben ser únicos para identificar a un subsistema dentro de la red. Para los subsistemas que pertenecen actualmente al SITM-Q deben asignarse lo siguientes valores numéricos para los caracteres 7 a 10 del identificador:

- Metro “0000”
- Metrobús “0001”
- Cables “0002”
- Convencional “0003”

Ejemplo: el subsistema Metrobús que pertenece a la red del SITM-Q ($\mathrm{IdRed} = \text{”}218000\text{”}$) debe identificarse con $\mathrm{IdSubsistema} = \text{"}2180000001\text{”}$.

3.1.1.3 Identificador de Ruta

El identificador de ruta debe ser de 14 caracteres en formato "RRRRRRSSSSrrrr". Los caracteres 1 a 6 (“RRRRRR”) deben llenarse con el identificador de la red a la cual pertenece la ruta, los caracteres 7 a 10 (“SSSS”) deben llenarse con el identificador del subsistema al cual pertenece la ruta. El carácter 11 (“r”) debe ser igual al carácter “A” para denotar que se está identificando una ruta y no de una zona. Los caracteres 11 a

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

14 (“rrr”) deben ser únicos para identificar a una ruta del subsistema. Los códigos de ruta deben ser asignados por el Registrador.

Ejemplo: la ruta Terminal Ofelia – Calacali del subsistema Metrobús que pertenece a la red del SITM-Q puede identificarse con $\mathrm{IdRuta} = \text{"2180000001A82A"}$.

3.1.1.4 Identificador de Zona

El identificador de zona debe ser de 14 caracteres en formato "RRRRRRSSSSzzzz". Los caracteres 1 a 6 (“RRRRRR”) deben llenarse con el identificador de la red a la cual pertenece la ruta, los caracteres 7 a 10 (“SSSS”) deben llenarse con el identificador del subsistema al cual pertenece la ruta. El carácter 11 (“z”) debe ser igual a “B” para denotar que se está identificando una zona, y no una ruta. Los caracteres 12 a 14 (“zzz”) deben ser únicos para identificar a una zona del subsistema.

Ejemplo: la zona de la Ofelia asociada al subsistema Quito Cables que pertenece a la red del SITM-Q puede identificarse con $\mathrm{IdZona} = \text{"218000002B082"}$.

3.1.1.5 Identificador de Usuario

El identificador de usuario debe ser de 2 caracteres, los cuales deben estar asociados a valores numéricos tipo ProfileCodeIOP según [7], tal como se almacenan en el medio de pago.

Teniendo en cuenta los tipos de usuarios que están regulados actualmente según [4], el identificador de usuario debe tomar los siguientes valores:

- General Anónimo “00”
- General Personalizado “01”
- Estudiante “02”
- Adulto Mayor “03”
- Discapacitado “04”
- Invidente “05”
- Funcionario “09”

Ejemplo: el perfil de usuario General Anónimo se registra en el medio de pago con CódigoPerfil=0x00, y en el archivo TARIFAS.xml debe tener denotarse con $\mathrm{IdUsuario} = \text{"00"}$

3.1.1.6 Identificador de Producto

El identificador del dato Producto será el identificador del producto asociado a la regla tarifaria. Este identificador debe ser de 4 caracteres hexadecimales. los primeros dos

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

caracteres serán “0C” para especificar que se trata de un contrato asociado a un producto distribuido en la red, y los dos caracteres siguientes se asocian a un producto específico, reservando los caracteres “FF” para operaciones con medios de pago tipo no recargables. A continuación se muestra la codificación asignada a los productos existentes hasta el momento:

- Producto General “0C01”
- Producto Especial de Estudiante “0C02”
- Producto Especial de Adulto Mayor “0C03”
- Producto Especial de Discapacitado “0C04”
- Producto Especial de Invidente “0C05”
- Medio de pago no recargable “0CFF”

3.1.1.7 Identificador de Transferencia

El identificador de transferencia (IdTransferencia) se utiliza para denotar una o más Transbordos desde una red, subsistema, ruta o zona, hacia una red, subsistema, ruta o zona. Las trasferencias deben denotarse como cadenas de identificadores de redes, subsistemas, rutas o zonas, unidas por el carácter “–”. El origen de la transferencia debe ser el campo más a la izquierda y el fin de la transferencia debe ser el más a la derecha:

Inicio **...** **Fin**

Ejemplo 1: la transferencia del subsistema Metrobús al sistema Convencional se define así: IdTransferencia = "2180000001-2180000003"

Ejemplo 2: la transferencia de la ruta con IdRuta = "2180000001A001” al subsistema Convencional se define así: IdTransferencia = ” 2180000001A001-2180000003"

3.2.2 Tarifas diferenciadas por tiempo

Para hacer la diferenciación de tarifas por hora es necesario utilizar los datos estructurados TarifaDia, TarifaHora y TarifaSimple (ver Figura 8).

El dato TarifaDia contiene el atributo TipoDia, que permite asociar la tarifa con el tipo de día del año según como se define en el archivo DIAS.xml para cada uno de los 365 días del año. Este atributo es obligatorio, único, y puede ser igual a `"*"` para denotar que una tarifa es válida para todos los tipos de días. Sin embargo, es posible definir varios registros de TarifaDia con TipoDia diferente a `"*"`, aun cuando se ha guardado

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

un registro con TipoDia igual a "*". En este caso, la tarifa con TipoDia igual a "*" tendrá menor prioridad con respecto al resto de tarifas TarifaDia.

Es importante tener en cuenta que todas las TarifasDia que se definan dentro de una estructura Tarifa asociada a un producto específico (ver Figura 8) deben tener un único TipoDia.

El dato estructurado TarifaDia se compone de los datos que se presentan a continuación:

Nombre del Campo	Descripción
TipoDia	Código relacionado con el tipo de día.
TarifaHora	Dato estructurado con información de la tarifa que aplica para la ventana de tiempo definida por inicio y duración.

Las tarifas por hora se definen a partir del dato TarifaHora, el cual se compone de los datos que se presentan a continuación:

Campo	Descripción
Inicio	Tiempo en minutos desde las 00:00 utilizado para denotar la hora a la cual inicia la validez de la tarifa. Debe ser un entero entre 0 y 1440.
Fin	Tiempo en minutos desde las 00:00 utilizado para denotar la hora a la cual termina la validez de la tarifa. Debe ser un entero entre 0 y 1440.
TarifaSimple	Dato estructurado con información de la tarifa que aplica para la ventana de tiempo definida por Inicio y Fin.

Teniendo en cuenta que TarifaDia puede contener múltiples registros de tarifas diferenciadas por hora, i.e., múltiples registros de TarifaHora, con el fin de denotar el caso por defecto, i.e., el que aplica para todas las horas no definidas con registros TarifaHora, debe utilizarse un registro TarifaHora con Inicio igual a cero y con Fin igual a cero. En caso de no definirse el caso por defecto, cualquier franja horaria no definida se deberá interpretar cómo no válida para el uso del producto.

Adicionalmente, las ventanas de tiempo definidas por registros TarifaHora no pueden intersecarse, i.e., solo puede aplicar una tarifa diferenciada por hora para una hora específica del día.

Es importante tener en cuenta que la hora de transacción siempre debe tomarse en unidades de minutos, pero debe estimarse con una resolución de segundos. Por ejemplo, si una transacción va a efectuarse a las 10:45:59, su valor en minutos es:

$$10 \times 60 \ + 45 + \frac{59}{60} = 645{,}983$$

Puede darse el caso en que el valor de Inicio de una TarifaHora (se denotará como Inicio_1 para ejemplificar) sea igual al valor de Fin (se denotará Fin_2 para ejemplificar) de otra TarifaHora. En caso de que la hora de la transacción sea igual a $\mathrm{Inicio}_1 = \mathrm{Fin}_2$, se le cobrará al usuario con la tarifa más baja de las dos.

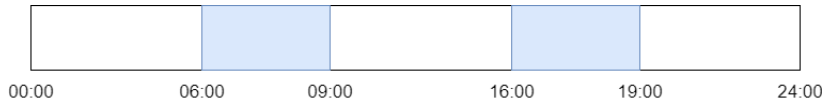
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Las tarifas simples, i.e., tarifas constantes que no dependen del día ni de la hora de operación, se definen a partir de la estructura TarifaSimple, que se compone de los datos que se presentan a continuación:

Campo	Descripción
Valor	Valor de la tarifa. Debe ser un número entero no negativo.
Unidades	Unidades de la tarifa. Puede tomar los siguientes valores únicamente: - Centavos de USD (1) - Viajes (2) - Centavos de USD por km (3)

Ejemplo:

Suponga que quiere definirse una tarifa diferenciada por día y por hora para el producto general (IdProducto = 1), la regla debe aplicar para los días feriados, y consiste en cobrar una tarifa más elevada para los intervalos de tiempo que se muestran a continuación:



Se quiere cobrar una tarifa de 100 ¢ para las franjas de las 6:00-9:00 y las 16:00-19:00. Para el resto del día feriado se quiere cobrar una tarifa de 50 ¢. Para los días que no sean feriados se quiere cobrar una tarifa de 30 ¢ todo el día. La definición de la Tarifa para el producto general puede hacerse como se muestra a continuación:

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

```
<Producto IdProducto="1">
  <TarifaDia TipoDia="FERIADO">
    <TarifaHora>
      <Inicio>360</Inicio>
      <Fin>540</Fin>
      <TarifaSimple>
        <Valor>100</Valor>
        <Unidades>1</Unidades>
      </TarifaSimple>
    </TarifaHora>
    <TarifaHora>
      <Inicio>960</Inicio>
      <Fin>1140</Fin>
      <TarifaSimple>
            <Valor>100</Valor>
            <Unidades>1</Unidades>
      </TarifaSimple>
    </TarifaHora>
    <TarifaHora>
      <Inicio>0</Inicio>
      <Fin>0</Fin>
      <TarifaSimple>
            <Valor>50</Valor>
            <Unidades>1</Unidades>
      </TarifaSimple>
    </TarifaHora>
  </TarifaDia>
  <TarifaDia TipoDia="*">
      <TarifaHora>
            <Inicio>0</Inicio>
            <Fin>0</Fin>
            <TarifaSimple>
                  <Valor>30</Valor>
                  <Unidades>1</Unidades>
            </TarifaSimple>
      </TarifaHora>
  </TarifaDia>
</Producto>
```

3.2.3 Tarifa plana

Las tarifas planas deben diferenciarse por red, subsistema, ruta, usuario y producto. Para esto es necesario utilizar los datos estructurados Red, Subsistema, Ruta, Usuario y Producto respectivamente (ver Figura 8). Todas las tarifas planas deben definirse dentro de la estructura TarifasPlanas.

La clasificación de tarifas por red, subsistema, y ruta se hace teniendo en cuenta que el SIR puede llegar a operar para múltiples redes, compuestas por múltiples subsistemas, cada subsistema puede ofrecer múltiples rutas de transporte para distintos tipos de usuarios, quienes pueden tener un medio de pago con múltiples productos.

Para definir una tarifa plana es necesario definir su red, subsistema, ruta, usuario y producto asociados. Una vez hecho esto, se asociará la estructura TarifaDia, descrita anteriormente.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Ejemplo 1: se quiere definir la tarifa plana para todas las rutas intracantonales urbanas del subsistema Convencional del SITM-Q cuyo valor es de 30 ¢ para el usuario general de la red, y aplica para todos los días y horas del año.

```
<Red IdRed="218000">
  <Subsistema IdSubsistema="2180000003">
    <Rutas>
      <Ruta IdRuta="*">
        <Usuario IdUsuario="00">
          <Producto IdProducto="*">
            <TarifasPlanas>
              <TarifaDia TipoDia="*">
                <TarifaHora>
                  <Inicio>0</Inicio>
                  <Fin>0</Fin>
                  <TarifaSimple>
                    <Valor>30</Valor>
                    <Unidades>1</Unidades>
                  </TarifaSimple>
                </TarifaHora>
              </TarifaDia>
            </TarifasPlanas>
          </Producto>
        </Usuario>
      </Ruta>
    </Rutas>
  </Subsistema>
</Red>
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Ejemplo 2: adicional a la tarifa definida en el Ejemplo 1, se quiere definir la tarifa plana para una nueva ruta con $\mathbf{IdRuta} = "218000\mathbf{A001}"$ dentro del subsistema Convencional del SITM-Q. El valor de la tarifa será de 35 ¢ para el usuario general de la red, y aplica para todos los días y horas del año.

```
<Red IdRed="218000">
  <Subsistema IdSubsistema="2180000003">
    <Rutas>
      <Ruta IdRuta="2180000003A001">
        <Usuario IdUsuario="00">
          <Producto IdProducto="*">
            <TarifasPlanas>
              <TarifaDia TipoDia="*">
                <TarifaHora>
                  <Inicio>0</Inicio>
                  <Fin>0</Fin>
                  <TarifaSimple>
                    <Valor>35</Valor>
                    <Unidades>1</Unidades>
                  </TarifaSimple>
                </TarifaHora>
              </TarifaDia>
            </TarifasPlanas>
          </Producto>
        </Usuario>
      </Ruta>
      <Ruta IdRuta="*">
        <Usuario IdUsuario="00">
          <Producto IdProducto="*">
            <TarifasPlanas>
              <TarifaDia TipoDia="*">
                <TarifaHora>
                  <Inicio>0</Inicio>
                  <Fin>0</Fin>
                  <TarifaSimple>
                    <Valor>30</Valor>
                    <Unidades>1</Unidades>
                  </TarifaSimple>
                </TarifaHora>
              </TarifaDia>
            </TarifasPlanas>
          </Producto>
        </Usuario>
      </Ruta>
    </Rutas>
  </Subsistema>
</Red>
```

3.2.4 Tarifa variable por distancia

El esquema de tarifas variables por distancia se define en [4], como un valor que debe hacerse en función de la distancia en kilómetros recorrida por un usuario desde que se

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

hace la validación de ingreso a uno de los subsistemas hasta que se hace válida la salida del mismo subsistema. Con esto en mente, será posible definir tarifas variables por distancia diferenciadas por subsistema haciendo uso de unidades en centavos de USD por kilómetro. Es importante tener en cuenta que todas las tarifas variables por distancia deben estar definidas dentro de la estructura TarifasDistancia.

Ejemplo: se quiere definir la tarifa variable por distancia para todas las rutas intracantonales urbanas del subsistema Convencional del SITM-Q cuyo valor es de 4 ¢/km para el usuario general de la red, y aplica para todos los días y horas del año. Suponga que el Registrador ha decidido asignarle el código (3) a las unidades de centavos de USD por kilómetro (¢/km).

```
<Red IdRed="218000">
  <Subsistema IdSubsistema="2180000003">
    <Rutas>
      <Ruta IdRuta="*">
        <Usuario IdUsuario="00">
          <Producto IdProducto="*">
            <TarifasDistancia>
              <TarifaDia TipoDia="*">
                <TarifaHora>
                  <Inicio>0</Inicio>
                  <Fin>0</Fin>
                  <TarifaSimple>
                    <Valor>4</Valor>
                    <Unidades>3</Unidades>
                  </TarifaSimple>
                </TarifaHora>
              </TarifaDia>
            </TarifasDistancia>
          </Producto>
        </Usuario>
      </Ruta>
    </Rutas>
  </Subsistema>
</Red>
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

3.2.5 Tarifa variable por transferencia

Las reglas tarifarias que aplican para las Transbordos deben denotarse dentro de la estructura Transbordos y debe hacerse uso del identificador de Transbordos.

Ejemplo: se quiere fijar gratis la tarifa de transferencia desde el subsistema Metrobús al sistema convencional para todos los usuarios, para todos los días y todas las horas del día.

```
<Red IdRed="218000">
  <Subsistema IdSubsistema="2180000003">
    <Transferencias>
      <Transferencia IdTransferencia="2180000001-2180000003">
        <Usuario IdUsuario="*">
          <Producto IdProducto="*">
            <TarifaDia TipoDia="*">
              <TarifaHora>
                <Inicio>0</Inicio>
                <Fin>0</Fin>
                <TarifaSimple>
                  <Valor>0</Valor>
                  <Unidades>1</Unidades>
                </TarifaSimple>
              </TarifaHora>
            </TarifaDia>
          </Producto>
        </Usuario>
      </Transferencia>
    </Transferencias>
  </Subsistema>
</Red>
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

3.2.6 Tarifa variable por zonas

Las reglas tarifarias que aplican para las zonas asociadas a un subsistema deben especificarse dentro de la estructura Zonas y debe hacerse uso del identificador de zonas

Ejemplo: se quiere fijar en 12 centavos de USD la tarifa por pasar por la zona del Condado asociada al subsistema Convencional (IdZona=”2180000003B001”) para todos los usuarios, para todos los días y todas las horas del día.

```
<Red IdRed="218000">
  <Subsistema IdSubsistema="2180000003">
    <Zonas>
      <Zona IdZona="2180000003B001">
        <Usuario IdUsuario="*">
          <Producto IdProducto="*">
            <TarifaDia TipoDia="*">
              <TarifaHora>
                <Inicio>0</Inicio>
                <Fin>0</Fin>
                <TarifaSimple>
                  <Valor>12</Valor>
                  <Unidades>1</Unidades>
                </TarifaSimple>
              </TarifaHora>
            </TarifaDia>
          </Producto>
        </Usuario>
      </Zona>
    </Zonas>
  </Subsistema>
</Red>
```

3.2.7 Reglas de validez de productos

El archivo TARIFAS.xml almacena información sobre las reglas de validez de los productos haciendo uso de la estructura Regla Validez (ver Figura 8), cuyos datos se describen a continuación:

Nombre del Campo	Descripción
TiempoPassback	Número de minutos en los que aplica la restricción de acceso anti-passback, a partir de la última transacción de aceptación del medio de pago.
TiempoTransbordo	Tiempo máximo expresado en minutos en el cual se pueden efectuar Transbordos dentro de un viaje, a partir de la última transacción de aceptación del medio de pago.
TransbordosPermitidos	Número de Transbordos permitidos dentro de TiempoTransbordo
PassbacksPermitidos	Número de accesos permitidos dentro del rango de tiempo “TiempoPassback”, si se iguala este número dentro de “TiempoPassback” se debe aplicar el sistema anti-passback.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

MaxDuracionViaje	Tiempo máximo expresado en minutos que puede tardar un viaje en el subsistema actual. Se utiliza como medida para evitar fraude.
MaxViajesDiasSemana	Estructura de datos que guarda información sobre el número máximo de viajes que pueden realizarse con un producto para cada día de la semana. Esta estructura se compone de hasta ocho datos tipo ViajesDia, uno para cada día de la semana. El dato ViajesDia contiene la información del número de viajes máximo que puede efectuarse con cierto producto para el día NumeroDia. NumeroDia hace referencia al número del día en la semana empezando desde el lunes, i.e., lunes tendrá NumeroDia igual a 1, mientras que el Domingo tendrá NumeroDia igual a 7, el número 8 solo será usado para días feriados. NumeroDia solo puede tomar valores entre 1 y 8. Es posible que en MaxViajesDiasSemana se almacenen menos de 8 registros de ViajesDia, en este caso, para el día de la semana que no tenga un registro se asumirá que no hay limitación de viajes, i.e., es posible que el usuario haga viajes ilimitados con el producto para el día sin registro de ViajesDia. El valor de ViajesDia solo puede estar entre 0 y 15, teniendo en cuenta la restricción de memoria del medio de pago con el campo NúmeroViajesDíaSemana en el(los) archivo(s) de SERVICIOS.
MaxViajesMes	Estructura de datos que guarda información sobre el número máximo de viajes que pueden realizarse con un producto para cada mes del año. Esta estructura se compone de hasta doce datos tipo ViajesMes, uno para cada mes del año. El dato ViajesMes contiene la información del número de viajes máximo que puede efectuarse con cierto producto para el mes NumeroMes (NumeroMes hace referencia al número del mes en el año empezando desde enero, i.e., enero tendrá NumeroMes igual a 1, mientras que el diciembre tendrá NumeroMes igual a 12. NumeroMes solo puede tomar valores entre 1 y 12. Es posible que en MaxViajesDiasMes se almacenen menos de 12 registros de ViajesMes, en este caso, para el mes del año que no tenga un registro se asumirá que no hay limitación de viajes, i.e., es posible que el usuario haga viajes ilimitados con el producto para el mes sin registro de ViajesMes.
ValorMínimo	Valor mínimo que puede tomar el producto en su archivo de valor. Valor representado como entero con signo.
ValorMáximo	Valor máximo que puede tomar el producto en su archivo de valor. Valor representado como entero.

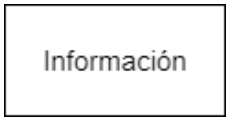
www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Cada uno de estos campos se utiliza cuando se lleva a cabo el proceso de aceptación del medio de pago, según lo establecido en el Capítulo 4.1 del presente documento.

3.3 Archivo con información de terminales

El archivo TERMINAL.xml se utiliza para almacenar información del dispositivo y su relación con la red interoperable (ver estructura de TERMINAL.xml en la Figura 9). Esta información se utiliza en complemento con la información almacenada en el archivo de parámetros para determinar la regla tarifaria al momento de efectuar una transacción de pago.

Figura 9. Esquema de datos estructurados en el archivo TERMINAL.xml almacenado en terminales



Fuente: elaboración propia

Particularmente, se almacenan los siguientes parámetros del sistema y de la ruta asociada al terminal de pago en la estructura de datos Información (ver Figura 9):

1. IdRed: código identificador de la red interoperable a la que pertenece el terminal.

2. IdSubsistema: código identificador del subsistema al que pertenece el terminal.

3. IdRuta: ruta dentro del sistema asociada al terminal de pago.

4. IdOperador: identificador único del operador que gestiona la ruta que se asocia al terminal de pago. Se almacena este dato con fines de cruce de cuentas para cada operador por la cantidad de usuarios atendidos.

5. IdEstación: identificador único asignado a la estación o bus, según corresponda.

6. IdDispositivo: identificador único asignado al terminal.

7. EsquemaTarifas: código relacionado con el esquema tarifario que aplica para el terminal. Este valor puede tomar los valores (en *string*): PLANA, DISTANCIA, o ZONAS. Es importante tener en cuenta que el esquema tarifario variable por Transbordos tiene prioridad sobre todos los esquemas tarifarios, siempre que aplique.

Teniendo en cuenta que solo puede haber un dato estructurado de Información en el archivo TERMINAL.xml, solo es posible que un terminal de pago esté asociado a una red, a un subsistema, a una ruta, un operador, y un esquema de tarificación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

4 Modelo transaccional

En este capítulo se presenta una definición de las posibles transacciones que se pueden efectuar con los medios de pago a través de la explotación del mapa de memoria. Además, se presenta la especificación de los procesos de manipulación de la información que deben llevar a cabo los equipos que interactúan con medios de pago para ejecutar las transacciones de uso de los medios de pago. Estas especificaciones se hacen tanto para medios de pago recargables como para medios de pago no recargables.

4.1 Transacciones en medios de pago recargables

4.1.1 Inicialización de aplicaciones

Este proceso es realizado por el proveedor de medios de pago. Sin embargo, se documentará cómo una transacción para referencia futura.

Para proceder con la inicialización de las aplicaciones en el medio de pago, es necesario que se defina su configuración, haciendo uso de las especificaciones que se presentan en este documento. Es decir, es necesario que se cargue la estructura de archivos de la aplicación al medio de pago, así como también las llaves de cifrado de la aplicación.

Cargar la estructura de archivos de una aplicación implica cargar los archivos EF contenidos en la aplicación.

1. Asignar serial de 8 bytes para el medio de pago. Cada aplicación en el medio de pago puede estar asociada al mismo serial.
2. Definir información del ATR.
3. Cargar información de fábrica del medio de pago (protocolo, PUPI, TSC, etc.).
4. Cargar información de arranque del medio de pago (*startup information* según [2]).
5. Cargar directorio **MAESTRO.**
6. Asignar AID al directorio **MAESTRO** (3MTR.ICA: 0x334D54522E494341).
7. Escribir información de fábrica del medio de pago, i.e., llenar los campos del archivo ICC.
8. Cargar el directorio **TRANSPORTE_QUITO**, incluir únicamente el archivo de FUNCIONARIO si el medio de pago es para un funcionario, si no, omitirlo, y cargar todos los archivos EF definidos para el directorio **TRANSPORTE_QUITO** a excepción del archivo de FUNCIONARIO.
9. Asignar AID al directorio **TRANSPORTE_QUITO** (1TIC.ICA: 0x315449432E494341).
10. Cargar aplicación **MONEDERO.**

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

11. Asignar AID al directorio **MONEDERO** (0ETP.ICA: 0x304554502E494341).

12. Cargar llaves de emisor para cada aplicación.

13. Cargar llaves de carga para cada aplicación.

14. Cargar llaves débito para cada aplicación.

15. Dejar en blanco todos los archivos contenidos en el medio de pago, i.e., llenar todos los campos de memoria con 0x00.

4.1.2 Emisión del medio de pago

Una vez un medio de pago ha sido inicializado, este debe ser emitido según los requerimientos del usuario (e.g., personalización de perfil o distribución de productos especiales). Una vez emitido un medio de pago, este puede ser usado en la red interoperable. Para lograr la emisión del medio de pago se deben llevar a cabo las siguientes acciones:

1. Llenar todos los campos del archivo ENTORNO.
2. En caso de que se emita un medio de pago para un funcionario, crear el archivo FUNCIONARIO con la información determinada por la entidad a la cual pertenece el funcionario.
3. Modificar el estado de la aplicación al estado Activada. Esto significa que el valor de ESTADO_APLICACION.EstadoAplicación = 1 (Activada).
4. Crear una nueva entrada en EVENTOS con la información de emisión del medio de pago.
5. Posterior a la emisión del medio de pago se debe distribuir el producto general.

La implementación recomendada de lógica de emisión es la siguiente:

```
Esperar por medio de pago.
Al detectar medio de pago:
EMISIÓN ( ) {
        Escribir archivo ENTORNO.
        Actualizar ESTADO_APLICACION.EstadoAplicación.
        Escribir Evento de emisión de medio de pago.
        Distribuir producto general.
}
```

4.1.3 Modificación de datos de usuario

Este proceso permite especificar el perfil de un propietario de un medio de pago para obtener tarifas y cobros diferenciados con sus productos. Se sugiere que la modificación de datos de usuario ocurra al momento de la emisión del medio de pago con el fin de otorgar funcionalidades especiales desde que el medio de pago entra en circulación. Este proceso también puede llevarse a cabo una vez el medio de pago ha sido emitido. Sin embargo, se deja a discreción del emisor del medio de pago la

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

conveniencia de realizarlo posteriormente. La modificación de datos de usuario requiere de la escritura del archivo USUARIO de la siguiente forma:

1. Escribir USUARIO.FechaNacimientoUsuario en caso de ser necesario (esto es necesario para usuarios con perfil de Estudiante o Adulto Mayor).
2. Escribir USUARIO.CódigoPerfil (en caso de ser funcionario CódigoPerfil = 0x09).
3. En caso de que el usuario sea un funcionario, configurar el archivo FUNCIONARIO según los criterios definidos por el emisor de medios de pago.
4. Escribir USUARIO.FechaFinPerfil si se ha determinado fijar un vencimiento para la validez del perfil de usuario, si no, llenar el campo con 0xFFFF.
5. Escribir USUARIO.NombreUsuario en codificación UTF-8, siguiendo notación Big-Endian.
6. Escribir USUARIO.CredencialUsuario.
7. Posteriormente a la modificación de los datos de usuario y si el perfil de usuario es diferente al perfil de Funcionario, se deben distribuir los productos especiales asociados.

La implementación recomendada de la lógica de personalización es la siguiente:

```
Esperar por medio de pago.
Al detectar medio de pago:
Ejecutar Acciones de listas.
PERSONALIZACIÓN (Datos de Usuario, Perfil de Usuario) {
        Revisar ESTADO_APLICACION.EstadoAplicación.
        Escribir archivo Usuario.
        Escribir evento de personalización.
        Distribuir productos especiales que correspondan.
}
```

4.1.4 Distribución de productos

Este proceso consiste en activar un producto en un medio de pago con el fin de ser usado en la red interoperable. La distribución de un producto solo puede ser realizada por los distribuidores autorizados de cada producto. Esto quiere decir que la disponibilidad de un producto depende en su totalidad de la entidad a quien se solicite un producto.

La aplicación interoperable puede almacenar varios productos de forma simultánea, una vez se hayan definido las condiciones de uso del servicio mediante la escritura de los registros del archivo de CONTRATOS, SERVICIOS y LISTA_CONTRATOS. Ahora bien, cada producto tendrá un valor de prioridad el cual será utilizado al momento de efectuar el cobro de la tarifa con el medio de pago. El valor de prioridad debe almacenarse en el campo LISTA_CONTRATOS(Producto).PrioridadProducto. Los productos especiales deben tener mayor prioridad que el producto general, y si existen distintos productos especiales en un mismo medio de pago, es necesario que para cada uno de ellos se defina un valor de prioridad. En caso de que se generen nuevos

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

productos en el futuro, se debe seguir la misma metodología de asignar prioridad en LISTA_CONTRATOS.

Con esto en mente, se describe a continuación el proceso de distribución de cada uno de estos productos, y a su vez, se especifican las condiciones que deben fijarse durante el proceso de distribución para poder acceder al viaje a crédito haciendo uso del Producto General.

Asimismo, en caso de que exista el producto, es posible realizar una renovación del vencimiento según los permisos que asigne el Registrador a cada distribuidor de productos. Una vez se distribuye un producto en un medio de pago, este pasa al estado *Activado* y puede ser usado según las reglas definidas en el contrato del producto.

Cuando un dispositivo distribuye un producto en un medio de pago, se debe verificar que no existe un producto activado del mismo tipo en el mismo. En caso de que exista un producto previamente cargado al medio de pago que sea de un tipo diferente al que se desea distribuir, es necesario que se utilice el primer registro en blanco para el archivo LISTA_CONTRATOS, y para los archivos CONTRATOS y SERVICIOS.

Las acciones que debe efectuar un dispositivo en un medio de pago Calypso para distribuir un producto deben ser las siguientes:

- Verificar que no existe el producto que se desea distribuir en el archivo LISTA_CONTRATOS.
- Configurar el correspondiente registro en el archivo CONTRATOS conforme a las especificaciones de este documento.
- Configurar el correspondiente archivo de valor asociado al producto (**MONEDERO** o CONTADORES), conforme a las especificaciones de este documento.
- Grabar el PunteroProducto.
- Configurar el correspondiente registro en el archivo SERVICIOS conforme a las especificaciones de este documento.
- Modificar el estado del producto a Activado. Esto significa que el valor de SERVICIOS(Producto).EstadoProducto se fija igual a 1 (i.e., Activado).
- Escribir la información necesaria del producto en un registro en blanco en el archivo LISTA_CONTRATOS.
- Crear una nueva entrada en el archivo EVENTOS con la información de distribución del producto.
- Recargar producto con saldo inicial, como mínimo se debe recargar la tarifa máxima aplicable para el producto que se va a distribuir.
- En el caso que se distribuya un producto con mayor prioridad que los productos ya presentes en el medio de pago, es necesario actualizar USUARIO. CódigoPerfil con el perfil relacionado al nuevo producto especial.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Vale la pena tener en cuenta que siempre que se defina un nuevo producto para la aplicación interoperable, será necesario asignar nuevos campos en los archivos CONTRATOS, SERVICIOS, y LISTA_CONTRATOS.

La implementación recomendada de la lógica de distribución de productos es la siguiente:

```
DISTRIBUCIÓN (Producto) {
        Revisar que el producto no esté distribuido en el medio de pago
        SI el producto ya está distribuido en el medio de pago
                Terminar
        SI NO
                Escribir archivo Contratos.
                Escribir archivo Servicios
                Escribir archivo ListaContratos.
                Escribir evento de distribución de producto
}
```

4.1.5 Recarga de productos en el medio de pago

Las reglas de recarga de productos almacenados en medios de pago dependen en gran medida del producto que se busca recargar. A continuación, se describen las reglas a aplicar en una transacción de recarga de productos:

- No está permitida la recarga de un producto almacenado en un medio de pago que esté en estado *Inicializado*, *Bloqueado* o *Desactivado*. Sin embargo, es posible realizar la recarga de un producto *Activado* o *Suspendido* en un medio de pago *Activo*.
- La recarga de un producto implica las siguientes acciones en el medio de pago:
  - Incrementar el valor del producto por el monto de la recarga en su archivo de valor, ya sea el valor de la aplicación MONEDERO o el valor del contador asociado al producto.
  - Crear una nueva entrada en EVENTOS con la información de recarga del producto.
- No es posible recargar el producto con archivo de valor MONEDERO por un valor inferior a la deuda total del producto, en caso de que haya una deuda.
- Al momento de saldar una deuda, el MONEDERO debe ser recargado mínimo con el valor de la deuda más la tarifa máxima aplicable para un usuario General del SITM-Q. Por ejemplo, si un usuario debe 30 ¢ por concepto de viaje a crédito, y la tarifa máxima aplicable para un usuario General es de 30 ¢, el monto mínimo que debe recargar es 60 ¢. Esto quiere decir que el MONEDERO quedaría con un saldo de 30 ¢.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- El saldo final del medio de pago después de la recarga, para todos los productos que sean recargables, debe ser mayor o igual a la máxima tarifa aplicable sin descuentos, si y solo sí, el medio de pago termina es entregado al usuario una vez se finaliza con el proceso de recarga.

Se sugiere el siguiente proceso para la recarga de productos con el fin de satisfacer las reglas mencionadas. Este proceso tiene en cuenta la manipulación del archivo de valor asociado al producto.

```
Esperar por medio de pago.
Al detectar medio de pago:
Ejecutar acciones de listas.
RECARGAR (Monto, Producto){
        Leer ENTORNO
                Determinar VersionAplicación
                Verificar FechaFinValidezAplicación
                Verificar IdRedpropietario, IdPropietario, IdRedEmisior e IdEmisor.
        Leer ESTADO_APLICACIÓN
                Verificar EstadoAplicación (Terminar si el medio de pago no está Activado)
        Leer SERVICIOS
          Verificar EstadoProducto debe ser activo
        Leer TARIFAS.XML
                Determinar Unidades
        SI Unidades = centavos de dólar
          Determinar ValorMonedero
                SI ValorMonedero + recarga >= tarifa máxima aplicable
                  Recargar MONEDERO por el monto total de la recarga
                        Guardar Evento de Recarga
                SI NO
                        Terminar
        SI Unidades = Viajes ( Número del contador = N, N > 0, N < 5)
                Recargar Contador # N por el monto total de la recarga
                Guardar Evento de Recarga
        TERMINAR
}
```

4.1.6 Devolución del monto de la última recarga hecha en el medio de pago

Si por errores operativos o técnicos al momento de hacer una recarga de productos en el medio de pago se recarga el monto incorrecto en algún producto (bien sean centavos de USD o viajes), el dispositivo de recarga tendrá que estar en la capacidad de devolver el monto recargado al producto. En esencia este procedimiento significa reducir el saldo del producto según el monto que se recargó de forma errónea. Para realizar este procedimiento, se debe tener en cuenta lo siguiente:

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- Solo se puede hacer la devolución del monto recargado en el dispositivo que efectuó la recarga.
- Solo se puede hacer la devolución a la recarga inmediatamente anterior. Esto quiere decir que el registro más reciente de EVENTOS debe corresponder a una recarga.
- La devolución se hace sobre el monto recargado, el cual se encuentra en el registro más reciente del archivo EVENTOS.
- La devolución del monto recargado en un producto implica las siguientes acciones en el medio de pago:
  - Reducir el valor del producto por el monto de la recarga errónea.
  - Crear una nueva entrada en EVENTOS con la información de devolución de recarga del producto.

Se sugiere el siguiente proceso para la devolución del monto recargado de forma errónea en un producto:

```
Esperar por medio de pago
Al detectar medio de pago:
Leer ENTORNO
    Verificar FechaFinValidezAplicación
    Determinar DistribuidorAplicación
    Determinar VersiónAplicación
    Verificar la aceptación del medio de pago según IdRed
Leer ESTADO_APLICACIÓN
    Verificar EstadoAplicación
Leer primer registro de EVENTOS
    SI el evento es de recarga de producto
        Verificar IdDispositivo
        Determinar PunteroProducto
        Determinar Unidades en TARIFAS.xml
        SEGÚN Unidades HACER
                CASO MONEDERO (Unidades = 0x01 o Unidades = 0x03)
                        Hacer la devolución del último monto recargado en el archivo
                        de valor MONEDERO
                CASO CONTADOR (Unidades = 0x02)
                        Hacer la devolución del último monto recargado en el
                        contador asociado al producto
        FIN SEGÚN
FIN SI
TERMINAR
```

4.1.7 Devolución de la tarifa

Pueden existir múltiples motivos por los cuales es necesario que un operador de recaudo haga la devolución de la tarifa pagada a un usuario. Pueden darse fallas logísticas o técnicas en la prestación del servicio, o eventos externos que igualmente

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

impidan la prestación del servicio. En tales casos el operador de recaudo debe realizar la devolución de la tarifa. Esta operación consiste en realizar una recarga, al monedero o contador, con el monto aceptado por el operador. La aceptación de una solicitud de devolución por parte del operador, puede estar sujeta a la comprobación de la información consignada en los registros del archivo EVENTOS. La devolución de la tarifa debe realizarse teniendo en cuenta las siguientes reglas y restricciones:

- Es posible realizar la devolución de la tarifa de productos asociados tanto al MONEDERO como al archivo de CONTADORES.
- Solo es posible realizar la devolución de la tarifa para las transacciones de aceptación inmediatamente anteriores que se hayan registrado en el archivo EVENTOS mediante eventos de uso de productos. Esto significa que no es posible realizar la devolución de la tarifa en transacciones de aceptación que sucedieron antes que una transacción de recarga de productos o una transacción de uso de devolución en el medio de pago.
- En SERVICIOS, deben devolverse los contadores afectados por el cobro de la tarifa
- La devolución del monto recargado en un producto implica las siguientes acciones en el medio de pago:
  - Aumentar el valor del producto por el monto de la recarga errónea.
  - Crear una nueva entrada en EVENTOS con la información de devolución de tarifa del producto.

4.1.8 Uso de productos en transacciones de aceptación

El uso de productos en transacciones de aceptación debe separarse en dos posibles transacciones: Aceptación en sistemas abiertos y Aceptación en sistemas cerrados. Un sistema abierto es aquel que requiere una validación con el medio de pago sólo a la entrada del sistema. Por el contrario, un sistema cerrado requiere que el usuario realice una validación con el medio de pago a la entrada y salida del sistema.

Cuando un usuario acerca su medio de pago a un dispositivo para acceder al servicio de transporte, este hace uso de los productos que tiene almacenados en su medio de pago. El uso de los productos debe cumplir con las siguientes reglas y restricciones tanto en sistemas abiertos cómo cerrados.

- Siempre se debe verificar la presencia de una acción disponible en listas LAM para el medio de pago o en listas LAP_A para productos antes de intentar usar un producto.
- No está permitido el uso de un producto almacenado en un medio de pago que no esté activado.
- No está permitido el uso de un producto suspendido.
- Se deben verificar si la aceptación es un Passback o Transbordo, de acuerdo a las reglas del producto establecidas en TARIFAS.xml
- La validez y las restricciones de uso de un producto deben verificarse con la información almacenada en los registros asociados al producto en CONTRATOS,

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

LISTA_CONTRATOS y SERVICIOS, así como también con la información almacenada en los archivos de parámetros en terminales.

- El cálculo de la tarifa a aplicar con un producto debe basarse en la información almacenada en los archivos de parámetros del terminal y en los registros de productos almacenados en los archivos CONTRATOS, SERVICIOS y LISTA_CONTRATOS del medio de pago.
- El archivo de valor a tener en cuenta para ejecutar el débito de la tarifa debe determinarse leyendo el archivo TARIFAS.xml, y determinando las Unidades de la tarifa a aplicar, según los lineamientos descritos en la sección 1.6.2. Si el cobro debe realizarse en Centavos de USD (1) o en Centavos de USD por km (3), el débito debe ejecutarse del archivo MONEDERO. En caso contrario, si el cobro es en Viajes (2), el débito se ejecutará del contador indicado por el campo PunteroProducto del archivo LISTA_CONTRATOS.
- Un producto es válido si no se ha alcanzado el límite de viajes utilizados en el periodo de tiempo definido para el producto (i.e., diario, semanal, mensual).
- Al usar cualquiera de los productos previamente definidos, siempre debe aumentar en 1 el valor de SERVICIOS(Producto).NúmeroActualAceptaciones, para llevar un número consecutivo de aceptaciones.
- Deben respetarse las reglas de validez de productos almacenadas en el archivo TARIFAS.xml, es decir, la validez de un producto se determina con base en dicha información.
- Es posible hacer uso de la facilidad de viaje a crédito si se ha permitido un valor mínimo de producto menor a cero en el archivo de parámetros TARIFAS.xml.
- En caso de definir el uso de transbordos en el SITM-Q también es posible hacer uso del viaje a crédito si se desea.
- Una vez se satisface el pago de la tarifa mediante el uso de productos, se debe otorgar acceso al usuario para la prestación del servicio.
- Es importante tener en cuenta que los transbordos no deben contarse como viajes. Es decir que cada vez que se hace un transbordo, únicamente se incrementa el campo EVENTOS.NúmeroTransbordos, no se incrementa ninguno de los contadores del archivo SERVICIOS(Producto).
- Cuando un producto es válido para su uso, se deben llevar a cabo las siguientes acciones para realizar "*Uso del Producto*" de forma adecuada:
  - Obtener la tarifa aplicable y las unidades de débito para el producto.
  - Obtener el valor mínimo para el producto del archivo TARIFAS.xml en caso de que se establezca crédito para productos.
  - Obtener el saldo del producto, del archivo de valor.
  - Debitar la tarifa aplicable del archivo de valor (MONEDERO o CONTADORES).
  - Escribir el evento de "Uso de Producto", "Uso de Transbordo" o "Salida" según corresponda.
  - Actualizar los contadores de SERVICIOS(Producto) según corresponda.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- Otorgar acceso al sistema si el débito de la tarifa se hizo satisfactoriamente.

- Si USUARIO.CodigoPerfil = 9 (funcionario) se deben aplicar las reglas de aceptación del medio de pago definidas por la entidad a la que pertenece el funcionario y que se encuentran almacenadas en el archivo FUNCIONARIO. Estas reglas solo se pueden aplicar de forma local en los dispositivos de aceptación del medio de pago de la entidad a la que pertenece el funcionario.

2.1.1.1. Aceptación en sistemas abiertos

En un sistema abierto los productos tienen definido un número de Passbacks permitidos dentro de una ventana de tiempo, este caso sólo se evalúa si se realiza más de una transacción de aceptación dentro de la misma estación o bus. Adicionalmente los productos deben tener una ventana y un número de transbordos permitidos, caso que sólo aplica si la estación o bus es diferente al registrado en la transacción de aceptación inmediatamente anterior. Por esto, se hace necesaria la verificación de transbordos y passbacks dentro de la transacción de aceptación. Si por el contrario, el uso de producto no es un Passback ni un transbordo, se debe buscar el producto válido con mayor prioridad y saldo mayor a la tarifa aplicable para su uso.

Se sugiere el siguiente proceso para la implementación de la transacción de Aceptación en sistemas abiertos, con el fin de satisfacer las reglas mencionadas:

```
Comprobar Listas
Revisar EstadoAplicación
   SI el medio de pago está bloqueado o desactivado TERMINAR
Revisar ultimo evento de Uso de Producto o Uso de Transbordo
Revisar EstadoProducto del Producto usado en el último evento
   SI el producto está activo y vigente
      Revisar IdEstación
        SI IdEstación es igual al del último evento (IdUbicación)
           SI esta en ventana de Passback de acuerdo a TARIFAS.xml
              SI hay Passbacks permitidos para el producto según TARIFAS.xml
                 Hacer Uso de Producto (Passback)
              SI NO
                 Buscar un producto con menor prioridad, válido y con saldo
                 SI existe un producto
                    Hacer Uso de Producto
                    TERMINAR
                 SI NO
                    Se niega el acceso
                    TERMINAR
        SI IdEstación es diferente al del último evento (IdUbicación)
           SI se está en ventana de transbordo y hay transbordos permitidos según
TARIFAS.xml
              SI es un transbordo
                 Hacer Uso de Producto (Transbordo)
                 TERMINAR
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

```
        FIN SI
Buscar el producto activo de mayor prioridad con saldo
   SI hay producto activo con saldo
      Hacer Uso de Producto
   SI NO
      Se niega el acceso
TERMINAR
```

2.1.1.2. Aceptación en sistemas cerrados

Un sistema cerrado implementa controles de flujo para la entrada y salida de pasajeros. Por este motivo, se deben describir tanto la transacción para entrada, como para salida del sistema. La existencia de estas dos transacciones también repercute en el uso de un tipo evento adicional asociado a las salidas del sistema. Este esquema de funcionamiento también tiene repercusiones en el procedimiento que debe seguirse para comprobar ventanas de transbordo y passbacks. Por todo lo anterior, a continuación se describen, de manera diferenciada, cada una de las transacciones de aceptación posibles dentro del sistema cerrado.

4.1.8.1.1 Aceptación para entrada en sistemas cerrados

En un sistema cerrado los productos no tienen permitido el uso de passbacks, por esto se restringe el acceso dentro de una ventana de tiempo si más de una transacción de aceptación se hace en la misma estación o bus. Por otra parte, si el último evento de aceptación registrado es de salida, se puede evaluar la posibilidad de un transbordo. Para comprobar si un transbordo puede ser otorgado, se debe verificar la ventana de transbordo y un número de transbordos permitidos para el producto asociado a la transacción de salida. Adicionalmente, la estación o bus donde se intenta ingresar es diferente al registrado en la transacción de salida inmediatamente anterior. Si por el contrario, el uso de producto no es un passback ni un transbordo, se debe buscar el producto válido con mayor prioridad y saldo mayor a la tarifa aplicable para su uso.

Se sugiere el siguiente proceso para la implementación de la transacción de Aceptación para entrada en sistemas cerrados, con el fin de satisfacer las reglas mencionadas:

```
Comprobar Listas
Revisar EstadoAplicación
   SI el medio de pago está bloqueado o desactivado TERMINAR
Revisar ultimo evento de Entrada
   Buscar el evento de Salida asociado al último evento de Entrada
      SI hay evento de Salida
         Revisar EstadoProducto
            SI producto activo
               Revisar IdEstación
                  SI IdEstación es diferente a IdEstación del evento de Salida
                     SI se permite el transbordo y se está en ventana de transbordos
                        Uso de  Producto (Transbordo) con el producto del ultimo evento
                        TERMINAR
```


www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

```
                    FIN SI
                FIN SI
            FIN SI
    SI no hay evento de Salida
        Revisar ventana de Passback del producto asociado al evento de Entrada
            SI está dentro de la ventana de Passback
                Se niega el acceso
                TERMINAR
            FIN SI
    FIN SI
Buscar el producto activo de mayor prioridad con saldo
  SI hay producto activo con saldo
    Hacer uso de producto
  SI NO
    Se niega el acceso
TERMINAR
```

4.1.8.1.2 Aceptación para salida en sistemas cerrados

Cuando un usuario intenta salir del sistema de transporte, deberá pasar su medio de pago por un validador, donde una transacción de aceptación para salida se llevará a cabo. En esta transacción, se comprueba que el usuario haya entrado legítimamente al mismo subsistema con una transacción válida de aceptación para entrada. En caso de encontrarse alguna irregularidad, se niega el paso al usuario, quien tendrá que comunicarse con un funcionario del sistema.

Se sugiere el siguiente proceso para la implementación de la transacción de Aceptación para salida en sistemas cerrados:

```
Revisar el ultimo evento de aceptación para entrada
SI hay evento de aceptación para entrada
        SI IdSistema es diferente al del evento aceptación para entrada
                Negar el paso
                TERMINAR
        FIN SI
        Revisar tiempo máximo de viaje del subsistema
        SI la diferencia de tiempo entre TapIn y TapOut es mayor
                Negar el paso
                TERMINAR
        FIN SI
        SI NO
                Escribir evento de TapOut
                TERMINAR
        FIN SI
SI NO
        Negar el paso
FIN SI
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

4.1.9 Reemplazo o reconstrucción del medio de pago

Los emisores de medios de pago deben estar en la capacidad de reconstruir el estado de un medio de pago averiado o extraviado. Este proceso consiste en la reconstrucción de la aplicación en un nuevo medio de pago y la reconstrucción de la información esta tenía almacenados. La reconstrucción de un medio de pago solo puede ser llevada a cabo por la entidad que lo emite. El requisito principal para poder hacer la reconstrucción del medio de pago es conocer el serial del medio de pago a reconstruir.

Debido a que la información de un medio de pago no se envía de inmediato hacia las Empresas Operadoras de Recaudo, ni hacia la Cámara de Compensación, puede existir un retraso entre la última operación realizada con un medio de pago y el momento en que es posible realizar su reconstrucción. Por esta razón, para poder llevar a cabo este proceso, el Operador de Recaudo debe esperar hasta tener toda la información del medio de pago disponible. Para eso, es necesario que la información se haya centralizado en el Nivel 4 (ver Sección 8.1 sobre Modelo interoperable de flujo de datos). Teniendo en cuenta que cada distribuidor de productos, i.e., cada emisor autorizado es el responsable de la reconstrucción del medio de pago, es necesario que en el nivel 4 se clasifiquen las transacciones de todos los medios de pago según su emisor y que dicha información se pase al Nivel 3 para que cada distribuidor cuente con la información actualizada de sus medios de pago.

El medio de pago extraviado o averiado deberá pasar al estado de *Desactivado* y toda la información guardada en sistema central se asignará al nuevo medio de pago.

Este proceso debe ser llevado a cabo efectuando las siguientes acciones:

- Emisión de un medio de pago nuevo. Se debe tener en cuenta que el identificador “SerialMedioPago” debe ser nuevo y único.
- Escritura de toda la información del medio de pago averiado o extraviado en el medio de pago nuevo. Esto incluye la escritura de la última información registrada de los archivos ESTADO_APLICACION, USUARIO, FUNCIONARIO (si aplica), CONTRATOS, SERVICIOS, CONTADORES, LISTA_CONTRATOS y MONEDERO en el medio de pago antiguo.
- En caso de que el medio de pago reconstruido no posea el saldo suficiente para aplicar la tarifa máxima aplicable en MONEDERO será necesario efectuar una recarga por al menos la tarifa máxima aplicable.
- Teniendo en cuenta que el archivo EVENTOS no debe ser reconstruido, los eventos que quedarán registrados después de una reconstrucción deben ser los de Emisión del medio de pago, Distribución de productos y Recarga (si aplica).

4.1.10 Reembolso del saldo del medio de pago

Opcionalmente se puede implementar esta transacción en la que se debita todo el saldo del monedero de un medio de pago para ser retornado al usuario. El reembolso se puede implementar para medios de pago anónimos y/o personalizados, el objetivo de esta transacción es que el usuario recupere el saldo de su medio de pago si no va a

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

seguir haciendo uso del mismo. Este proceso debe ser llevado a cabo efectuando las siguientes acciones:

- Siempre se debe hacer el débito de la totalidad del saldo del monedero tanto para medios de pago anónimos como personalizados. Esto con el objetivo de evitar un mal uso del medio de pago.
- Cuándo se efectúa un reembolso de un medio de pago anónimo este debe ser entregado por el usuario, debido a que el medio de pago podría ser reutilizado.
- Debido a que se deben entregar los medios de pago anónimos sobre los que se efectúe reembolso, se deberán borrar todos los eventos previos al reembolso y los contadores: NúmeroSemanaAño, NúmeroViajesDíaSemana y NúmeroViajesMes del registro que corresponda al producto general del archivo SERVICIOS.
- Cuándo se efectúa el reembolso de un medio de pago personalizado no se debe retornar el medio de pago, así como tampoco se borrarán los eventos o contadores de SERVICIOS asociados al monedero.
- Cuándo se efectúa el reembolso de un medio de pago personalizado se debe registrar un evento de reembolso.

Se sugiere el siguiente proceso para el reembolso del saldo con el fin de satisfacer las reglas mencionadas:

```
Esperar por medio de pago.
Al detectar medio de pago:
Ejecutar acciones de listas.
   Leer ESTADO_APLICACIÓN
      Verificar EstadoAplicación (Terminar si el medio de pago no está Activo)
   Verificar el registro de SERVICIOS asociado al Producto General
      Verificar EstadoProducto (Terminar si el producto no está Activo)
   Obtener saldo del monedero
      SI saldo > 0
         Obtener código perfil de USUARIO
            SI Usuario es igual a “00” es un medio de pago anónimo
               Débito de todo el saldo de monedero
               Borrar todos los eventos del medio de pago
               Borrar contadores de SERVICIOS
               TERMINAR
            SI NO (Es un medio de pago personalizado)
               Débito de todo el saldo de monedero
               Escribir evento de Reembolso del saldo
               TERMINAR
      SI NO
         TERMINAR
```

4.1.11 Acciones a través de listas

Las acciones a través de listas de acción deben llevarse a cabo al iniciar cualquier interacción entre un Medio de Pago y un dispositivo de validación o de recarga. A continuación se describe el orden en que las listas deben ser verificadas.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

```
Esperar por medio de pago
Al detectar medio de pago:
Verificar ENTORNO
Leer SerialMedioPago
   VerificarLAM(SerialMedioPago)
   VerificarLAP_A(SerialMedioPago)
   VerificarLAP_R(SerialMedioPago)
   VerificarLAP_RP(SerialMedioPago)
FIN
```

Es importante tener en cuenta que cuándo se efectúe una acción de una lista sobre un medio de pago, se debe enviar la transacción a la Cámara de Compensación para que no se vuelva a emitir la lista con dicha entrada.

El proceso de verificación de cada una de las listas es descrito en las subsecciones siguientes. Posteriormente, se da una descripción detallada del formato a utilizar para cada una de las listas.

4.1.11.1 Verificar Lista LAM

El bloqueo, reactivación y desactivación de una aplicación interoperable almacenada en un medio de pago se debe realizar con el uso de la Lista de Acción para Medios de pago interoperables (LAM). Los dispositivos de aceptación de medios de pago deben almacenar la lista LAM actualizada. Las entradas de la lista indican la acción que se debe realizar sobre una aplicación en el medio de pago. Cada entrada debe incluir un SerialMedioPago, un NúmeroAcciónMedioPago y un CódigoAcción. El NúmeroAcciónMedioPago permite determinar si se debe ejecutar la acción indicada por CódigoAcción en el medio de pago con el correspondiente SerialMedioPago.

La acción indicada en CódigoAcción solo se debe aplicar si NúmeroAcciónMedioPago es mayor que ESTADO_APLICACIÓN.NúmeroAcciónAplicada.

El campo CódigoAcción puede tomar los siguientes valores:

- 1 (acción de reactivación)
- 2 (acción de desactivación)
- 3 (acción de bloqueo)

Es importante mencionar que cuando se ejecuta una acción de desactivación, el medio de pago debe invalidarse siguiendo las especificaciones de Calypso.

A continuación, se describe el proceso que debe seguir un dispositivo para ejecutar una acción sobre un medio de pago:

```
SerialMedioPago recibido por parámetro
SI SerialMedioPago EXISTE en la lista LAM ENTONCES
   Leer EstadoAplicación
  SI NúmeroAcciónMedioPago > NúmeroAcciónAplicada ENTONCES
            SEGÚN CódigoAcción HACER
                     CASO 1 (acción de reactivación)
```


www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

```
                    (Desbloquear aplicación)
                    ESTADO_APLICACIÓN.EstadoAplicación = 1 (activada)
                CASO 2 (acción de desactivación)
                    (Desactivar aplicación)
                    ESTADO_APLICACIÓN.EstadoAplicación = 2
(desactivada)
                CASO 3 (acción de bloqueo)
                    (Bloquear medio de pago)
                    ESTADO_APLICACIÓN.EstadoAplicación = 3 (bloqueada)
          FIN SEGÚN
          NúmeroAcciónAplicada = NúmeroAcciónMedioPago
  SI NO
     TERMINAR
  FIN
SI NO
   TERMINAR
FIN
```

4.1.11.2 Verificar Lista LAP_A

Un producto almacenado en un medio de pago puede ser suspendido si el distribuidor del producto determina que este no debe ser usado por un usuario. La suspensión de un producto se debe llevar a cabo a través de una Lista de Acción para Productos en dispositivos de aceptación de medios pago (LAP_A). Los dispositivos de aceptación deben almacenar la lista LAP_A actualizada. Las entradas de la lista indican qué productos almacenados en medios de pago deben ser suspendidos. Cada entrada debe incluir un SerialMedioPago, un CódigoProducto y un NúmeroSuspensiónProducto. El NúmeroSuspensiónProducto permite determinar si se debe ejecutar la acción de suspensión sobre el producto con el correspondiente CódigoProducto en el medio de pago con dicho SerialMedioPago.

La suspensión del producto solo se debe realizar si NúmeroSuspensiónProducto es mayor que CONTRATOS(Producto).NúmeroReactivaciónProducto.

A continuación, se describe el proceso que debe seguir un dispositivo para ejecutar una acción de suspensión de un producto:

```
SerialMedioPago recibido por parámetro
SI SerialMedioPago EXISTE en la lista LAP_A ENTONCES
        Leer LISTA_CONTRATOS
            Determinar PunteroProducto del producto indicado en CódigoProducto
        Leer CONTRATOS(Producto)
            Determinar NúmeroReactivaciónProducto
        SI NúmeroSuspensiónProducto > NúmeroReactivaciónProducto ENTONCES
            (Suspender producto)
        SERVICIOS.EstadoProducto = 2 (suspendido)
   FIN SI
FIN SI
```


Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

4.1.11.3 Acciones Lista LAP_R

Los productos almacenados en medios de pago pueden ser recargados de forma remota en dispositivos de recarga. Esto quiere decir que un distribuidor de productos puede solicitar a las entidades de la red interoperable la recarga de un producto en un medio de pago. Para lograr esto los dispositivos de distribución de productos (o de recarga) deben almacenar una Lista de Acción para Productos en dispositivos de Recarga (LAP_R). Las entradas de la lista LAP_R indican qué productos almacenados en medios de pago deben ser recargados. Cada entrada debe incluir un SerialMedioPago, un CódigoProducto, un NúmeroAcciónProducto y un MontoAcción. El NúmeroAcciónProducto permite determinar si se debe ejecutar la acción de recarga remota por el monto indicado en MontoAcción en el producto con el correspondiente CódigoProducto en el medio de pago con dicho SerialMedioPago.

La recarga del producto solo se debe realizar si NúmeroAcciónProducto es mayor que CONTRATOS(Producto).NúmeroAcciónAplicadaProducto. Si estas condiciones se cumplen, se debe generar un evento de recarga de producto según las reglas definidas en este documento para recarga de productos.

Se deben tener en cuenta las mismas reglas que para el proceso de Recarga de productos en el medio de pago.

A continuación, se describe el proceso que debe seguir un dispositivo para ejecutar una acción de recarga remota de un producto:

```
SerialMedioPago recibido por parámetro
SI SerialMedioPago EXISTE en la lista LAP_A ENTONCES
  Leer LISTA CONTRATOS
            Determinar PunteroProducto del producto indicado en CódigoProducto
      Leer CONTRATOS
            Determinar NúmeroAcciónAplicadaProducto del producto indicado en
CódigoProducto
      SI NúmeroAcciónProducto > NúmeroAcciónAplicadaProducto ENTONCES
            (Recarga remota de producto)
            Recargar archivo de valor por el monto MontoAcción
            NúmeroAcciónAplicadaProducto = NúmeroAcciónProducto
      SI NO
            TERMINAR
      FIN SI
FIN SI
```

4.1.11.4 Recarga automática de medios de pago

El SITM-Q podrá implementar la transacción de recarga automática de medios de pago, esta recarga se efectúa debitando de un producto bancario establecido por el usuario si el monto de su medio de pago está por debajo de un umbral fijado por el usuario. Para poder hacer uso de este beneficio el usuario deberá

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

asociar un producto bancario al servicio de recargas automáticas prestado por el proveedor de recargas remotas.

El proveedor de recargas remotas tendrá la responsabilidad de informar a la cámara de compensación de la nueva solicitud de inscripción mediante el evento S_Inscripcion_Automatica. Así mismo, la responsabilidad de la cámara de compensación será mantener actualizado el monto de todos los medios de pago inscritos en el servicio de recargas automáticas. De ésta forma, si el proveedor de recargas remotas detecta que alguno de los medios de pago inscritos tiene un saldo inferior al umbral establecido por su usuario se deberá ejecutar el débito del monto establecido por el usuario de su producto bancario asociado y el proveedor de recargas remotas emitirá una solicitud de recarga para que el medio de pago sea agregado a la lista LAP_R con la recarga correspondiente.

Es importante resaltar que el monitoreo del saldo para los medios de pago inscritos para recarga automática se hace a nivel del proveedor de recargas remotas, el cual tiene acceso de sólo lectura a la base de datos de la cámara. Así, cada vez que en la base de datos de la cámara se actualice el monto de MONEDERO para un medio de pago inscrito se deberá revisar si es necesario hacer el débito del producto bancario y efectuar la solicitud de recarga remota a cámara.

4.1.11.5 Acciones Lista LAP_RP

Los productos almacenados en medios de pago pueden ser renovados de forma remota en dispositivos de recarga o validación. Esto quiere decir que un distribuidor de productos puede solicitar a las entidades de la red interoperable la renovación de un producto en un medio de pago. Para lograr esto los dispositivos deben almacenar una Lista de Acción de Productos de Renovación de Producto (LAP_RP). Las entradas de la lista LAP_RP indican qué productos almacenados en medios de pago deben ser renovados. Cada entrada debe incluir un SerialMedioPago, un CódigoProducto y una FechaFinValidez. La FechaFinValidez permite determinar si se debe ejecutar la acción de renovación del producto con el correspondiente CódigoProducto en el medio de pago con dicho SerialMedioPago.

La renovación del producto solo se debe realizar si FechaFinValidez es posterior que CONTRATOS(Producto). FechaFinValidezProducto. Si estas condiciones se cumplen, se debe generar un evento de renovación de producto según las reglas definidas que para el proceso de Renovación de productos en el medio de pago.

A continuación, se describe el proceso que debe seguir un dispositivo para ejecutar una acción de renovación remota de un producto:

SerialMedioPago recibido por parámetro
SI SerialMedioPago EXISTE en la lista LAP_RP ENTONCES
  Leer LISTA CONTRATOS
    Determinar registro del producto indicado en CódigoProducto
    SI FechaFinValidez (LAP_RP) > CONTRATOS(Producto). FechaFinValidezProducto

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Renovación del Producto con Id CódigoProducto.
CONTRATOS(Producto). FechaFinValidezProducto = FechaFinValidez (LAP_RP)
SI NO
TERMINAR
FIN SI
FIN SI

4.1.11.6 Detalle del formato de cada lista

Cada lista de acción deberá ser almacenada en el dispositivo correspondiente como un archivo separado por comas (.csv). Cada vez que se recibe una nueva versión de esta lista, se debe sobrescribir la versión anterior de manera que siempre exista un único archivo en el dispositivo para cada lista. Cada línea del archivo corresponde a un registro asociado a un medio de pago. A continuación se describe el nombre de cada archivo y el contenido de una línea del archivo.

- Nombre del archivo LAM: listaLAM.csv
  - Contenido de una línea: Serial,NumeroAcción,CódigoAcción
- Nombre del archivo LAP_A: listaLAPA.csv
  - Contenido de una línea: Serial,IdProducto,NúmeroSuspensión
- Nombre del archivo LAP_R: listaLAPR.csv
  - Contenido de una línea: Serial,IdProducto,NúmeroAcción,Monto
- Nombre del archivo LAP_RP: listaLAPRP.csv
  - Contenido de una línea: Serial,IdProducto,FechaFinValidez

4.1.12 Reactivación de productos

Una vez un producto ha sido suspendido, solo el distribuidor del producto en el medio de pago está autorizado para reactivarlo. Por lo tanto, es responsabilidad del distribuidor de productos de definir las listas de acción privadas necesarias para realizar la reactivación de los productos que distribuye. En una acción de reactivación, se debe incrementar en una unidad el campo NúmeroReactivaciónProducto del contrato del producto. Esto con el fin de garantizar que una vez ha sido reactivado el producto este no puede ser suspendido nuevamente por una entrada antigua de la lista LAP_A. Se requiere una recarga en el monedero cuando este no cuenta con saldo disponible para pagar la tarifa máxima aplicable en todo el sistema de transporte.

El proceso que debe seguir un distribuidor de productos para reactivar un producto es el siguiente:

Esperar por medio de pago
Al detectar medio de pago:
Leer ENTORNO
Leer LISTA CONTRATOS
SI el producto con IdProducto en el medio de pago con SerialMedioPago puede ser reactivado
ENTONCES

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

AUMENTAR el campo CONTRATOS(Producto).NúmeroReactivaciónProducto en 1 en el registro del contrato asociado al producto.
SERVICIOS(Producto).EstadoProducto = 1 (activado)
FIN SI

4.1.13 Renovación de productos

Los productos incluyen reglas de validez y de vencimiento en su contrato. Es posible renovar un producto con el fin de modificar estas reglas de aceptación en la red interoperable. El producto a renovar no puede estar suspendido.

Por ejemplo, los productos especiales podrían estar sujetos a renovación periódica para perfiles futuros. En este caso, los distribuidores autorizados para distribuir cierto producto especial podrán efectuar una operación y se actualiza el archivo SERVICIOS para reiniciar los parámetros de uso del producto. Estas acciones aplican para cualquier producto que sea renovado. Estas acciones aplican para cualquier producto que sea renovado.

Por lo tanto, un evento de renovación de producto incluye la escritura del archivo CONTRATOS, la actualización del archivo SERVICIOS y la recarga opcional del producto.

```
Esperar por medio de pago
Al detectar medio de pago:
Verificar ENTORNO
Verificar ESTADO APLICACIÓN
Leer MONEDERO
SI Valor(MONEDERO)<=0
   (No puede renovarse un producto si no hay fondos en el monedero)
   TERMINAR
Leer SerialMedioPago
SI SerialMedioPago corresponde con el del medio de pago del producto a renovar
   Leer LISTA CONTRATOS
      Verificar EstadoProducto
      Actualizar CONTRATOS(Producto).FinValidezProducto
      Actualizar SERVICIOS(Producto).NúmeroSemanaAño
      Actualizar SERVICIOS(Producto).NúmeroViajesDíaSemana
      Actualizar SERVICIOS(Producto).NúmeroViajesMes
FIN SI
```

4.2 Transacciones en medios de pago no recargables

4.2.1 Emisión de los medios de pago no recargables

Cada vez que se desea emitir un medio de pago precargado para ser usado en la red interoperable esta debe ser inicializado con los datos de emisión, un saldo inicial y los parámetros necesarios. La inicialización de los medios de pago precargados debe ocurrir en un entorno controlado y seguro con el fin de evitar la emisión fraudulenta de medios de pago en la red interoperable. A continuación, se describen las acciones

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

que se deben llevar a cabo en un medio de pago precargado para lograr la emisión de este:

- Cargar los datos de emisión en las páginas destinadas para tal fin.
- Modificar los parámetros del medio de pago de tal forma que no se puedan volver a escribir los datos de emisión.
- Escribir el saldo inicial del medio de pago mediante el incremento del contador # 1 al valor designado de acuerdo con la definición de saldo.
- Definir las unidades del saldo.
- Registrar transacción de emisión llenando los datos de las páginas de información de transacciones (páginas 0x07 a 0x0D).
- Calcular la firma digital PSO inicial del medio de pago con base en los datos escritos y escribirlo en la página destinada para tal fin.

4.2.2 Uso de los medios de pago no recargables

Como se mencionó en la sección 4.1.8, el proceso de uso de medio de pago depende de si el sistema implementado es abierto o cerrado. A continuación se definen las reglas que debe cumplir el proceso de uso de medio de pago, independientemente del tipo de sistema. Las condiciones específicas a sistemas abiertos y cerrados, y el procedimiento recomendado en cada caso, se describirán en las siguientes secciones.

- No está permitido el uso de un medio de pago vencido
- Deben verificarse todas las reglas de validez en el archivo TARIFAS.xml
- No está permitido el uso de un producto almacenado en un medio de pago que no esté activado.
- La validez y las restricciones de un producto deben verificarse con la información almacenada en los datos de emisión del medio (ver 2.2.1)
- El cálculo de la tarifa a aplicar con un producto debe basarse en la información almacenada en TARIFAS.xml, y TERMINAL.xml.
- Cuando el medio de pago es válido para su uso, se deben llevar a cabo las siguientes acciones para hacer uso del producto:
  - Aumentar el contador por el valor de la tarifa
  - Actualizar los datos de transacciones almacenados en la tarjeta.
- Una vez se satisface el pago de la tarifa, se debe otorgar acceso al usuario para la prestación del servicio.

4.2.2.1 Aceptación en sistemas abiertos

En un sistema abierto, los medios de pago no recargables no tienen restricción de passbacks. Por otro lado, tampoco cuentan con beneficio de transbordo. Por consiguiente, el proceso de aceptación de un medio de pago no recargable consiste únicamente en la verificación del saldo y la actualización de los campos almacenados en la estructura de datos de la tarjeta.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

El procedimiento sugerido para llevar a cabo esta transacción, se presenta a continuación:

```
Esperar por medio de pago.
Al detectar medio de pago:
(El medio de pago es precargado)
Determinar el SerialMedioPago del medio de pago precargado
Leer el valor del contador # 1
Calcular el saldo disponible del medio de pago con base en el valor del contador # 1
Calcular la tarifa a aplicar
SI saldo disponible < tarifa a aplicar ENTONCES
        El saldo del medio de pago es insuficiente para realizar el cobro
        TERMINAR
SI NO
        Leer los datos del medio de pago desde la página 0x00 hasta la página 0x0E
        Calcular Firma PSO y verificar que es igual al Firma PSO almacenada en el medio
de                                  pago no recargable
        SI Firma PSO calculado = Firma PSO almacenado ENTONCES
                DISMINUIR Saldo disponible en el monto de la tarifa calculada
                Almacenar la información de último uso en el espacio designado
                Calcular nuevamente la firma digital PSO con los nuevos datos escritos
en el           medio de pago precargado
                SOBRESCRIBIR la firma digital PSO con la nueva firma PSO calculada
                Otorgar acceso
                TERMINAR
        SI NO
                La firma PSO no es válida y no se debe otorgar acceso
        FIN SI
FIN SI
```

4.2.2.2 Aceptación en sistemas cerrados

Como se comentó en 2.1.1.2, los sistemas cerrados implementan dos transacciones de aceptación: una para entrada y otra para salida. Estas dos transacciones se describen en las siguientes secciones.

4.2.2.2.1 Aceptación para entrada en sistemas cerrados

Los sistemas cerrados buscan que cada evento de ingreso al sistema se corresponda con un evento de salida. Por tal motivo, no deben permitirse passbacks durante una ventana de tiempo determinada por el operador.

El proceso que se debe seguir un validador para realizar una aceptación para entrada en un sistema cerrado, es la que se muestra a continuación:

```
Esperar por medio de pago.
Al detectar medio de pago:
(El medio de pago es precargado)
```


www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

```
Determinar el SerialMedioPago del medio de pago precargado
SI saldo disponible < tarifa a aplicar ENTONCES
        El saldo del medio de pago es insuficiente para realizar el cobro
        TERMINAR
FIN SI
Leer los datos del medio de pago desde la página 0x00 hasta la página 0x0E
Calcular Firma PSO y verificar que es igual al Firma PSO almacenada en el medio de pago no recargable
SI Firma PSO calculado != Firma PSO almacenado ENTONCES
        (La firma PSO no es válida y no se debe otorgar acceso)
        Negar acceso
        TERMINAR
FIN SI
SI TipoEvento del medio de pago es Uso de Producto ENTONCES
        SI está en ventana de passback
                Negar acceso
                TERMINAR
        FIN SI
FIN SI

DISMINUIR Saldo disponible en el monto de la tarifa calculada
Almacenar la información de último uso en el espacio designado
Actualizar la firma digital PSO con la nueva información almacenada
Otorgar acceso
TERMINAR
```

4.2.2.2.2 Aceptación para salida en sistemas cerrados

Para salir de un sistema cerrado, es necesario presentar el medio no recargable para validar que previamente se realizó una aceptación para entrada legítima. Esta aceptación debe estar almacenado en la tarjeta como un evento de tipo Uso de Producto. En caso de encontrarse alguna irregularidad, debe negarse la salida del sistema, y el usuario deberá comunicarse con un funcionario de la estación para salir.

El proceso que se debe seguir un validador para realizar una aceptación para salida en un sistema cerrado, es la que se muestra a continuación:

```
Esperar por medio de pago.
Al detectar medio de pago:
(El medio de pago es precargado)
Determinar el SerialMedioPago del medio de pago precargado
Leer los datos del medio de pago desde la página 0x00 hasta la página 0x0E
Calcular Firma PSO y verificar que es igual al Firma PSO almacenada en el medio de pago no recargable
SI Firma PSO calculado != Firma PSO almacenado ENTONCES
        (La firma PSO no es válida y no se debe otorgar acceso)
```


www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

```
        Negar salida
        TERMINAR
FIN SI
SI TipoEvento del medio de pago es Uso de Producto ENTONCES
        Almacenar la información de último uso en el espacio designado
        Actualizar la firma digital PSO con la nueva información almacenada
        Permitir salida
SI NO
        (No hay ingreso al sistema asociado al medio de pago)
        Negar salida
        TERMINAR
FIN SI
```

4.3 Integración de una API en el SITM-Q

La autoridad de transporte de la municipalidad estará en capacidad de entregar una Interfaz de Programación de Aplicaciones (API – *Application Programming Interface*) que implemente el anterior Modelo Transaccional y realice la interpretación de los Archivos de en Terminales de Aceptación. En tal caso, dicha API tendrá que ser utilizada por los Operadores de Recaudo, Proveedores de Tecnología y/o Operadores de Transporte para la configuración y programación de todos los dispositivos que se implementen en el SITM-Q.

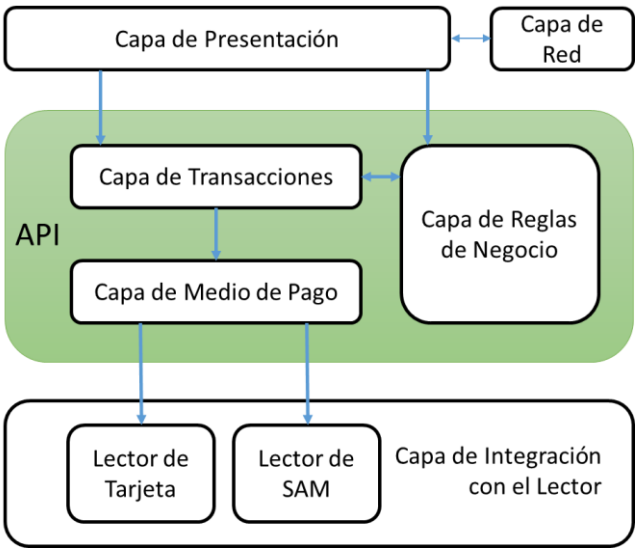
El objetivo de desarrollar una API para la implementación del Modelo Transaccional del Manual de Normatividad Técnica es garantizar que el funcionamiento de todos los posibles Operadores de Recaudo sea unificado. Así mismo, la integración de una API agilizaría la implementación de los demás requerimientos establecidos en éste documento para los Proveedores de Tecnología. Finalmente, la API facilitaría el proceso de actualización del sistema de Recaudo en caso de que cambien las reglas de negocio, las transacciones del sistema o se integren nuevos medios de pago.

4.3.1 Arquitectura de Integración de la API

La arquitectura propuesta para la integración de la API es la siguiente:

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 10. Arquitectura propuesta del API



Fuente: elaboración propia

De acuerdo al anterior esquema la API deberá implementar las siguientes capas: Capa de Transacciones, Capa de Medio de Pago y Capa de Reglas de Negocio. Así mismo, se delega a los Proveedores de Tecnología la responsabilidad del desarrollo e integración de las siguientes capas: Capa de Integración con el Lector, Capa de Presentación y Capa de Red.

4.3.1.1 Capa de Presentación

Esta capa deberá ser desarrollada por el Proveedor de Tecnología y deberá incluir funcionalidades que permitan la integración con las diferentes interfaces de usuario y los periféricos para cada dispositivo. Por ejemplo: la pantalla LCD de un validador, la interfaz para ingresar información de una máquina de venta y recarga o el torniquete de acceso de las estaciones.

4.3.1.2 Capa de Red

Esta capa deberá ser desarrollada por el Proveedor de Tecnología y deberá incluir todas las funcionalidades que requieran o implementen interfaces de comunicación con niveles superiores del sistema. Esta capa se encargará de implementar el envío de eventos al sistema central, el manejo de listas de acción y el manejo de archivos de configuración de los terminales.

4.3.1.3 Capa de Reglas de Negocio

Esta capa deberá estar incluida en la API y deberá implementar las funcionalidades necesarias para el cumplimiento de las reglas de negocio de cada subsistema. Esta capa deberá incluir funcionalidades que permitan obtener la estructura tarifaria para cada subsistema, la estructura tarifaria para transferencias y las reglas de uso de cada producto dentro de cada subsistema.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

4.3.1.4 Capa de Transacciones

Esta capa deberá estar incluida en la API y su función será implementar todas las transacciones descritas en el Manual de Normatividad Técnica. Esta capa se encargará de cumplir con todos los requerimientos de cada transacción y de implementar la función tal cual se describe en el manual. Las transacciones que deben ser implementadas en esta capa son: emisión de medios de pago, personalización de medios de pago, distribución de productos, recarga de productos, devolución de la recarga, devolución de la tarifa, uso de productos, reembolso del saldo, funciones de fiscalización, entre otras.

4.3.1.5 Capa de Medio de Pago

Esta capa también deberá hacer parte de la API y sus funciones son: implementar todos los comandos propios del estándar Calypso para medios de pago y para SAMs, realizar el manejo de sesión segura y realizar el manejo de todas las aplicaciones y archivos presentes en el medio de pago. Esta capa también debe estar en la capacidad de realizar todos los comandos propios del medio de pago MIFARE Ultralight.

4.3.1.6 Capa de Integración con el Lector

El desarrollo de esta capa es responsabilidad del Proveedor de Tecnología, su función es permitir la integración de la API con el hardware propio del dispositivo para el que se esté desarrollando el software. Específicamente esta capa deberá implementar funciones que permitan conectarse y comunicarse con el medio de pago, así como también funciones para conectarse y comunicarse con el módulo SAM.

4.3.2 Requerimientos no funcionales para integración de la API

Para garantizar que la integración de la API se pueda realizar de forma satisfactoria en todos los posibles dispositivos que se implementen en el SITM-Q se establecerán requerimientos no funcionales que se deberán tener en cuenta y se deberán cumplir tanto para el desarrollo de la API cómo para la adquisición de los equipos en los que se integrará.

Todos los dispositivos que vayan a hacer parte del SITM-Q y que requieran integrar la API para su funcionamiento deberán usar un sistema operativo Linux o Windows. Adicionalmente, se requiere que dicho dispositivos incluyan las librerías libxml (Linux) o SystemXML (Windows) debido a que la API deberá hacer uso de éstas para leer los archivos de tarifas, reglas de uso de productos y de información en terminales.

Respecto al desarrollo de la API, se establece que para la implementación del software se deberá usar el estándar ISO/IEC 9899:2011 también llamado C11 y el estándar ISO/IEC 14882:2011 conocido cómo C++11. Debido a esto, se debe garantizar que los equipos escogidos para ser usados en el sistema sean capaces de compilar con estos estándares en caso de que llegue a ser necesario.

La autoridad de transporte deberá entregar la API acompañada de un contrato que defina cada una de las funciones que se deberán implementar en la Capa de Integración con el Lector. De esta forma, se garantizará que la nomenclatura de

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

parámetros, retornos y nombres de las funciones sea la adecuada para garantizar un correcto funcionamiento de la API. Así mismo, todas las capas desarrolladas por el proveedor tecnológico también deberán cumplir con las reglas y procesos establecidos en el Manual de Normatividad Técnica.

Finalmente, la API será entregada cómo una serie de librerías pre-compiladas con sus correspondientes archivos de encabezado, los cuales definirán el nombre, parámetros y tipo de retorno de cada una de las funciones de cada librería. Adicionalmente se deberá incluir un contrato para cada función implementada.

5 Interfaces entre sistemas

5.1 Modelo interoperable de flujo de datos

En una red interoperable el flujo de información ocurre entre diferentes niveles según la estructura de la red. Esta estructura generalmente estará compuesta por los siguientes niveles:

- *Nivel 0*: medios de pago con la aplicación interoperable.
- *Nivel 1*: todos aquellos dispositivos lectores de medios de pago. Pueden ser dispositivos de aceptación de medios de pago, dispositivos de emisión de medios de pago y dispositivos de recarga de productos.
- *Nivel 2*: dispositivos concentradores de transacciones que interconectan los dispositivos de nivel 1 con un sistema central de nivel 3.
- *Nivel 3:* toda la infraestructura centralizada que administra y gestiona la información generada o destinada a los niveles inferiores. Esta es administrada por la entidad propietaria de los dispositivos de nivel 1 y 2 a los cuales está conectado, es decir el Operador de Recaudo respectivo.
- *Nivel 4:* Cámara de Compensación. Es el nivel más alto de la red interoperable. En este nivel se colecta toda la información de la red interoperable. Este nivel es supervisado por la Autoridad de Aplicación y Control.

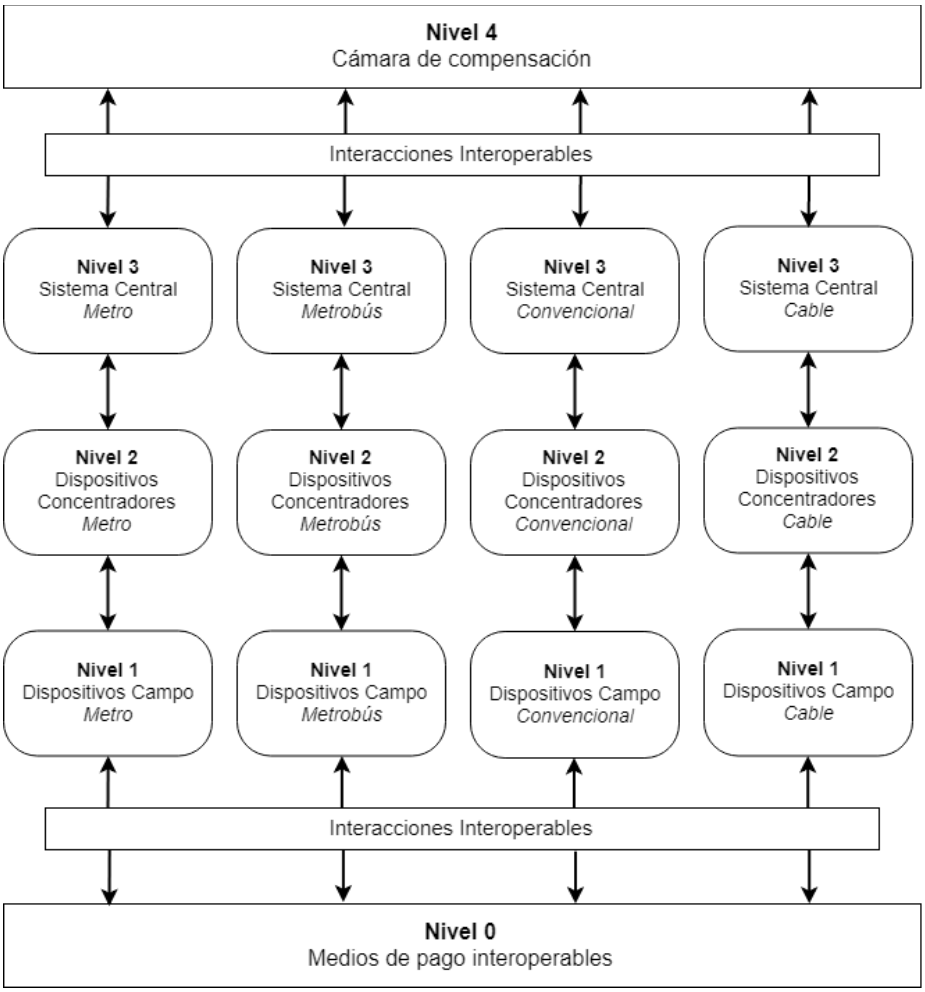
Con el fin de garantizar interoperabilidad, se debe garantizar que el flujo de información al inicio y al final de la red interoperable sea estandarizado. Es decir, la información almacenada en el nivel 0 e intercambiada con el nivel 1, así como la información intercambiada entre nivel 3 y el nivel 4, deben ser interoperables. Teniendo en cuenta que ya se ha descrito la mayor parte de la interacción entre los niveles 0 y 1, ahora se describirán las interacciones interoperables entre el nivel 3 y 4.

Es importante tener en cuenta que según el esquema planteado en la Figura 11, los actores en el nivel 3 solo pueden intercambiar información entre sí a través de la cámara de compensación. Es decir que toda la información debe centralizarse en la cámara de compensación, organizarse según actores y luego enviarse de regreso. Esto

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

es necesario para proveer la información transaccional de cada uno de los medios de pago propios de un actor para que pueda llevar a cabo su reconstrucción en caso de que sea necesario.

Figura 11 Estructura multinivel de la red interoperable



Fuente: elaboración propia

5.2 Transmisión de archivos

El Nivel 1 de la red interoperable no sólo realiza transacciones con los medios de pago del Nivel 0, sino que también compila toda la información de cada transacción que realiza en archivos. Estos archivos deberán ser transmitidos a los sistemas centrales de nivel 3, que a su vez deberán transmitir estos archivos al nivel 4 de la red interoperable. La información almacenada en estos archivos cumple con dos propósitos principales:

- Cruce de cuentas por cobrar y cuentas por pagar entre los actores por concepto de uso de productos en servicios prestados por diferentes sistemas interoperables de recaudo.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- Recolección de la actividad transaccional y no transaccional de todos los medios de pago para su seguimiento y posible reconstrucción.

Los diferentes sistemas de Nivel 3 deben trasmitir estos archivos a la Cámara de Compensación con el fin de que ésta posea toda la información necesaria para realizar un correcto proceso de compensación de los diferentes actores del sistema. La Cámara de Compensación centraliza esta información para ejercer y mantener el control sobre el SIR del SITM-Q.

La transmisión de los archivos debe realizarse mediante servicios web REST siguiendo el protocolo HTTPS. A continuación se describen los servicios que deben implementar la cámara de compensación y cada operador de recaudo.

5.2.1 Autenticación

Tanto la cámara como los operadores de recaudo deberán contar con un mecanismo de autenticación basado en tokens haciendo uso de un usuario y una contraseña. Esto implica que la cámara de compensación tendrá una lista de usuarios y contraseñas válidos de cada operador de transporte, y cada operador de transporte contará con la información del usuario y la contraseña de la cámara. Las características de la solicitud de autenticación son las siguientes:

- Método: POST
- URL: https://[Dirección del host]/auth
- Parámetros en el body (JSON):
  - Username: nombre de Usuario
  - Password: contraseña del usuario

5.2.2 Servicios web a implementar por la cámara de compensación

5.2.2.1 Endpoint de recepción de transacciones

Todos los operadores de recaudo deberán usar este Endpoint para enviar los archivos de eventos hacia la cámara. Esto incluye todas las transacciones realizadas con medios de pago (emisión, distribución, recarga, validación, confirmaciones de ejecución de listas, etc.), así como las solicitudes de ejecución de acciones sobre listas. Se recomienda que las transacciones sean enviadas con una periodicidad mínima de 24 horas (es decir, el operador de recaudo podría esperar al cierre de la operación para consolidar todas las transacciones y enviarlas a la cámara), sin embargo las solicitudes sobre listas de acción deberían enviarse al menos cada hora durante el periodo de operación diario del sistema. Las características de la solicitud para el envío de transacciones a la cámara son:

- Método: POST
- Autorización: Token
- URL: https://[Dirección del host de la cámara]/events

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- El archivo XML con los eventos debe ir en el body de la solicitud debidamente nombrado de acuerdo con la sección anterior

5.2.3 Servicios web a implementar por cada operador

5.2.3.1 Endpoint de recepción de transacciones

La cámara debe usar este Endpoint para enviar al operador de recaudo todas las transacciones realizadas con los medios de pago que este emitió, así como las difusiones de acciones sobre listas para los medios de pago de todo el sistema. Las transacciones deben enviarse tan pronto la cámara haya recibido las transacciones diarias de cada operador y esta haya creado los archivos correspondientes. Sin embargo, las difusiones sobre listas de acción deberán enviarse tan pronto como haya disponibilidad de conexión a los operadores. Debe garantizarse que el tiempo entre la recepción de la solicitud de actualización de listas y la difusión a los operadores de recaudo, sea inferior a 10 minutos. Las características de la solicitud para el envío de transacciones a cada operador son:

- Método: POST
- Autorización: Token
- URL: https://[Dirección del host del operador]/events
- El archivo XML con los eventos debe ir en el body de la solicitud debidamente nombrado de acuerdo con la sección anterior

5.3 Descripción de los archivos para transmisión de datos

Los mensajes que se vayan a intercambiar entre equipos deben estar codificados en formato XML de conformidad con el esquema XML (XSD) descrito en [16].

El nombre de los archivos intercambiados debe tener la siguiente estructura:

<XXXXYYYYNNNNNNNNN.xml>

Donde:

XXXX = Código de identificación del remitente asignado por el Registrador

YYYY = Código de identificación del destinatario asignado por el Registrador

NNNNNNNNN

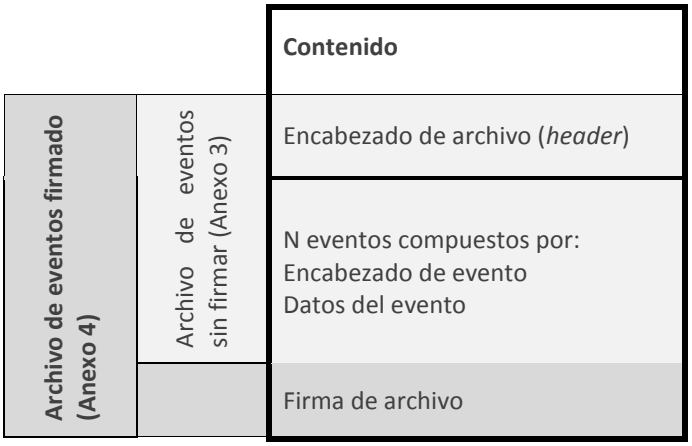
= Número consecutivo en decimal. Este número es incrementado en 1 para cada archivo enviado por el remitente. Cuando se alcanza su límite superior, este es reiniciado en 0.

Para construir este archivo se deben seguir los siguientes pasos:

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

1. Generar un archivo de eventos sin firma de conformidad con el esquema definido en [17]. Los tipos de datos presentados en [17] que terminan en 1545 corresponden a los tipos de dato que presenta el estándar BS EN 1545 [15] [18].
2. Agregar una firma al archivo de eventos de conformidad con el esquema definido en [16] y en el Capítulo 5.4.

Los archivos de eventos representan los esquemas de datos para intercambiar información transaccional y no transaccional entre Emisores y la cámara de compensación. El contenido de un archivo de eventos está compuesto por la siguiente información:



Los Anexos 3 y 4 especifican el detalle (por medio de un esquema XML) de cada evento que se puede enviar en un archivo de eventos.

La sección de encabezado de archivo se compone por los siguientes elementos:

Nombre del dato	Tipo de dato	Tamaño (bytes)	Valor inicial, comentarios
VersiónEstructura	0 .. 65535	2	Versión de la estructura usada en el archivo. La versión actual corresponde al valor 0x0001
NúmeroEventos	0 .. 4294967295	4	Número de eventos incluidos en el archivo
FechaCreaciónArchivo	0 .. 4294967295	4	Fecha de creación basada en el tiempo universal coordinado (UTC)

La sección de encabezado de evento se compone por los siguientes elementos:

Nombre del dato	Tipo de dato	Tamaño (bytes)	Valor inicial, comentarios
NúmeroSecuencial	0 .. 4294967295	4	Número que indica la posición del evento dentro del archivo. Para el primer evento del archivo este valor debe corresponder a 1 y para el último evento este valor debe corresponder a NúmeroEventos
FechaEvento	0 .. 4294967295	4	Fecha de ocurrencia basada en el tiempo universal coordinado (UTC)

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

IdSAM	0 .. 4294967295	4	Identificador del SAM que ha generado el evento.

La estructura de la sección de datos de evento depende del tipo de evento efectuado. El origen de la información aquí consignada siempre será de tres tipos: 1) el medio de pago que originó el evento, 2) las listas de acción de la red interoperable o 3) la estructura definida en el Capítulo 5.3.3 para los reportes no efectuados. Los posibles tipos de evento se muestran en la Tabla 21.

Para todos los eventos aplica que la información consignada es referente al estado del medio de pago después de haberse efectuado una transacción.

5.3.1 Archivos de eventos transaccionales

Tabla 21 Tipos de eventos transaccionales y descripciones

Tipo de evento	Nombre en esquema	Descripción
Emisión del medio de pago	E_MedioPago_Emisión	Indica que un medio de pago ha sido inicializado para ser usado en la red interoperable
Modificación de datos de usuario	E_MedioPago_ModUsuario	Indica que se ha realizado un cambio de perfil de usuario o cambio de parámetros de perfil en un medio de pago
Reembolso de saldo en monedero	E_MedioPago_Reembolso	Indica que se ha realizado un reembolso de la totalidad del saldo disponible en el monedero.
Distribución de producto	E_Producto_Distribucion	Indica que un producto ha sido distribuido en un medio de pago
Recarga de producto	E_Producto_Recarga	Indica que un producto ha sido recargado en un medio de pago
Devolución de monto recargado	E_Producto_Devolucion_Recarga	Indica que se ha hecho la devolución del monto recargado en un producto
Uso de producto	E_Producto_Uso	Indica que un producto ha sido usado en una transacción de aceptación de medio de pago
Uso de producto con transbordo	E_Transbordo_Uso	Indica que un producto ha sido usado en una transacción de aceptación de medio de pago, que clasificó como transbordo según las reglas del producto asociado
Uso de producto para salida	E_Salida_Uso	Indica que un producto ha sido usado en una transacción de aceptación para salida del sistema
Reactivación de producto	E_Producto_Reactivacion	Indica que se ha realizado la reactivación de un producto
Emisión de medio de pago precargado	E_Precargado_Emision	Indica que se ha emitido un medio de pago precargado y está disponible para ser usado en la red interoperable
Uso de medio de pago precargado	E_Precargado_Uso	Indica que un usuario ha hecho uso un medio de pago precargado para efectuar una transacción de aceptación del

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Tipo de evento	Nombre en esquema	Descripción
		medio de pago

5.3.2 Archivos de eventos no-transaccionales

Tabla 22 Tipos de eventos no transaccionales y descripciones

Tipo de evento	Nombre en esquema	Descripción
Reconstrucción de medio de pago	E_MedioPago_Reconstruccion	Indica que un emisor de medios de pago ha realizado una reconstrucción de un medio de pago previamente emitido en un nuevo medio de pago
Solicitud de acción con lista LAM	S_Accion_LAM	Indica que una entidad de la red interoperable realiza una solicitud para realizar una actualización a la lista LAM
Solicitud de acción con lista LAP_A	S_Accion_LAP_A	Indica que una entidad de la red interoperable realiza una solicitud para realizar una actualización a la lista LAP_A
Solicitud de recarga remota de producto con lista LAP_R	S_Accion_LAP_R	Indica que una entidad de la red interoperable realiza una solicitud para realizar una actualización a la lista LAP_R
Solicitud de recarga remota de producto con lista LAP_RP	S_Accion_LAP_RP	Indica que una entidad de la red interoperable realiza una solicitud para realizar una actualización a la lista LAP_R
Solicitud de inscripción a lista de recarga automática	S_Inscripcion_Automatica	Indica que un medio de pago se ha inscrito a un servicio de recarga automática
Difusión de acción con lista LAM	D_Difusion_LAM	Indica a las entidades de la red interoperable que se debe efectuar una acción de lista LAM sobre medios de pago
Difusión de acción con lista LAP_A	D_Difusion_LAP_A	Indica a las entidades de la red interoperable que se debe efectuar una acción de lista LAP_A sobre productos almacenados en medios de pago
Difusión de acción de recarga remota con lista LAP_R	D_Difusion_LAP_R	Indica a las entidades de la red interoperable que se debe efectuar una acción de lista LAP_R sobre productos almacenados en medios de pago
Difusión de acción de recarga remota con lista LAP_RP	D_Difusion_LAP_RP	Indica a las entidades de la red interoperable que se debe efectuar una acción de lista LAP_RP sobre productos almacenados en medios de pago
Confirmación de acción efectuada con lista LAM	E_Confirmacion_LAM	Indica que se ha efectuado satisfactoriamente una acción solicitada en la lista LAM
Confirmación de acción efectuada con lista LAP_A	E_Confirmacion_LAP_A	Indica que se ha efectuado satisfactoriamente una acción solicitada en la lista LAP_A
Confirmación de recarga remota de producto efectuada con lista LAP_R	E_Confirmacion_LAP_R	Indica que se ha efectuado satisfactoriamente una acción

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Tipo de evento	Nombre en esquema	Descripción
		solicitada en la lista LAP_R
Confirmación de recarga remota de producto efectuada con lista LAP_RP	E_Confirmacion_LAP_RP	Indica que se ha efectuado satisfactoriamente una acción solicitada en la lista LAP_RP
Reporte de evento no efectuado	R_Evento_No_Efectuado	Indica que se ha intentado efectuar un evento en un medio de pago, pero este no se ha podido efectuar

5.3.3 Estructura del reporte de evento no efectuado

El reporte de evento no efectuado, debe enviarse cada vez que ocurre un error no esperado a la hora de realizar una acción en la red interoperable. A diferencia del resto de posibles eventos, la información necesaria para generar el reporte de evento no efectuado no se consigna en la aplicación interoperable o en alguna de las listas de acción. Por esta razón, se definen a continuación los campos y posibles valores que debe incluir dicho evento.

Tabla 23. Datos en reporte de evento no efectuado y descripciones

Nombre de dato	Descripción	Posibles valores
SerialMedioPago	Corresponde al identificador del medio de pago sobre el cual se ha intentado efectuar un evento	
TipoEventoIntentado	Indica el evento que se intentó efectuar sobre el medio de pago	- No especificado (0) - Distribución de producto (1) - Recarga de producto (2) - Emisión del medio de pago (3) - Modificación de datos de usuario (4) - Uso de producto (5) - Uso de producto con transbordo (6) - Uso de producto para salida de sistema cerrado (7) - Devolución de recarga (8) - Devolución de tarifa (9) - Venta de medio de pago precargado (10) - Uso de medio de pago precargado (11) - Reconstrucción de medio de pago (12) - Reconstrucción de producto (13) - Confirmación de acción efectuada con lista LAM (21) - Confirmación de acción efectuada con lista LAP_A (21) - Confirmación de acción efectuada con lista LAP_R (22) - Confirmación de acción efectuada con lista LAP_RP (23)
CódigoRazónFalla	Indica la razón por la cual no se ha efectuado el evento	- No especificado (0) - Fallo de autenticación (1) - Red de origen no aceptada (2) - Versión de aplicación no aceptada (3) - Estructura de datos incompatible (4)

5.4 Seguridad en el envío de archivos

Los procesos de recolección y envío de eventos requieren del uso de firmas digitales basadas en la recomendación ITU-T X.509 [19] de Infraestructura de Llave Pública

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

(PKI). Dicha infraestructura debe permitir el cumplimiento de los siguientes requerimientos:

- Control de integridad de archivos: con lo cual es posible verificar que un archivo transmitido no ha sido modificado por un tercero durante el envío.
- Autenticación de actores: con lo cual el receptor del archivo puede verificar la autenticidad del remitente.
- No repudio: el emisor no puede negar la autenticidad de un archivo firmado digitalmente a su nombre.

5.4.1 Estructura de seguridad

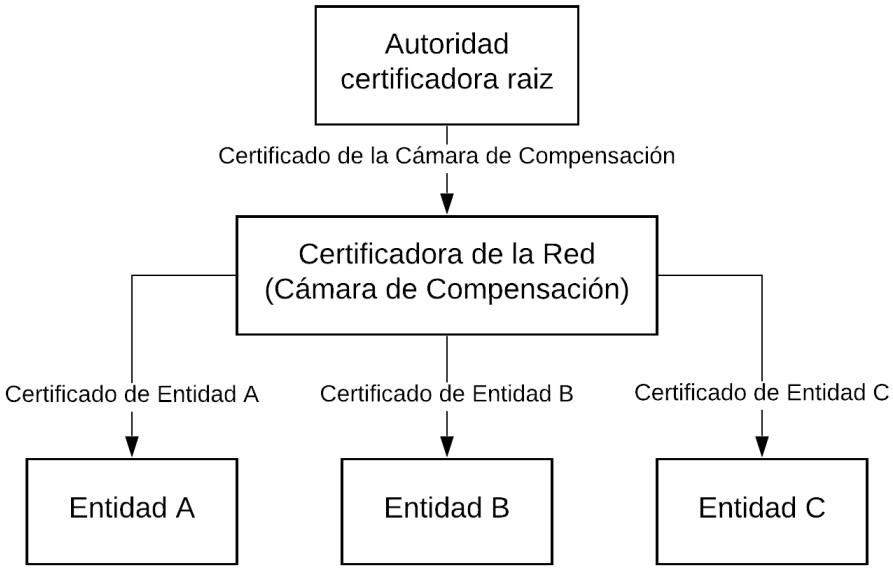
La infraestructura de llave pública está basada en pares de llave pública y privada para cada entidad. La llave privada de cada entidad debe permanecer en secreto y es usada para generar firmas digitales de archivos de eventos. La llave pública a su vez debe ser certificada por una autoridad certificadora que garantiza su autenticidad. Este proceso da como resultado el certificado digital de una entidad. Estos certificados pueden ser usados por otras entidades para verificar la validez de las firmas generadas con la respectiva llave privada de la entidad. Esto con el fin de garantizar la integridad de los archivos, autenticar a la entidad generadora de la firma y garantizar que el archivo no puede ser repudiado.

La Cámara de Compensación actúa como autoridad certificadora (CA) de la red interoperable. Por lo tanto, es esta quien tiene la responsabilidad de la generación de certificados para las entidades de la red interoperable. Por su parte, la Cámara de Compensación también debe ser certificada para que los operadoras puedan comprobar los documentos que esta envía. El certificado correspondiente a la Cámara de Compensación debe ser generado por una autoridad certificadora raíz (*Root* CA), la cual es una entidad externa especializada en dicha responsabilidad. La Autoridad de transporte, con ayuda del comité de interoperabilidad, tendrá la responsabilidad de escoger la autoridad certificadora raíz.

El proceso de generación de certificados se basa en la recomendación ITU-T X-509 [19] y debe ser llevado a cabo de acuerdo con la Figura 12. Infraestructura de llave pública en la red interoperable.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 12. Infraestructura de llave pública en la red interoperable



Fuente: elaboración propia

Con el fin de satisfacer los requerimientos de seguridad planteados siempre se debe adjuntar una firma digital a cada archivo de eventos intercambiado entre actores. Dicha firma debe satisfacer la recomendación W3C XMLDSIG [20] para archivos XML del 10 de junio de 2008 usando los siguientes parámetros:

- Método de firma (*SignatureMethod*): RSA-SHA1
- Método de canonicalización (*Canonicalization method*): Canonical XML 1.0 omitiendo comentarios (C14N)
- Algoritmo de transformación (*Transform*): Firma envuelta (*Enveloped signature*)
- Función hash (*Digest method*): SHA1

Además, los archivos generados con la firma deben seguir el esquema XSD de [16].

5.4.2 Lista de revocación de certificados (CRL)

Esta lista consiste en un archivo único al cual pueden acceder todas las entidades participantes de la red interoperable. La lista de revocación de certificados (CRL) contiene información de todos los certificados que alguna vez fueron usados en la red pero que ya no pueden ser aceptados por ninguna entidad. Debido a que solo puede existir una lista en un determinado momento en la red interoperable, las versiones anteriores del archivo deben ser removidas. Esta lista debe hacerse disponible desde la Cámara de Compensación para todas las entidades de la red interoperable.

La estructura de la lista de revocación de certificados está definida en [21]. Esta está compuesta por las siguientes secciones:

- Encabezado de archivo

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- N registros de revocación
- Firma de archivo

La sección de encabezado de archivo de la lista de revocación de certificados está compuesta por los siguientes elementos:

Nombre del campo	Descripción
Versión_CRL	Indica la versión del archivo de CRL
Emisor_CRL	Identificador de la entidad que ha generado y firmado la CRL. Asignado por el Registrador.
Fecha_Hora_CRL	Indica la fecha y hora en la cual se hace válida la lista CRL actual.

Cada registro de revocación en la lista de revocación de certificados está compuesto por los siguientes elementos:

Nombre del campo	Descripción
Núm_Serial_Certificado	Identifica el certificado que se ha revocado en la red interoperable
Fecha_Hora_Revocación	Fecha y hora en la cual el certificado ha sido revocado. El certificado no debe ser aceptado después de esta fecha.

La firma del archivo CRL debe ser calculada por la autoridad certificadora de la red interoperable; es decir, la Cámara de Compensación. La firma del archivo CRL debe satisfacer la recomendación W3C XMLDSIG [20] para archivos XML del 10 de junio de 2008 usando los siguientes parámetros:

- Método de firma (*SignatureMethod*): RSA-SHA1
- Método de canonicalización (*Canonicalization method*): Canonical XML 1.0 omitiendo comentarios (C14N)
- Algoritmo de transformación (*Transform*): Firma envuelta (*Enveloped signature*)
- Función hash (*Digest method*): SHA1

6 Modelo de seguridad de las transacciones

Todo sistema de recaudo basado en Calypso debe contar con una arquitectura de seguridad de conformidad con las especificaciones presentadas en [22]. La arquitectura de seguridad debe incluir:

- Descripción de *secret roots*
- La especificación detallada y completa de cómo se usan las *secret roots* para generar SAM maestros
- La descripción de todos los datos presentes en módulos SAM maestros, con valor detallado de todos los campos: derechos globales, identificadores de llaves, todos los atributos de llaves, cualquier restricción sobre valores de llaves (por ejemplo, llaves de diferente identificador pueden tener el mismo algoritmo y el mismo valor asociados), etc.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- Propósito y uso previsto para todos los datos presentes en SAM maestros.
- Todos los datos presentes en todos los tipos de SAM definidos, con valor detallado de todos los campos: derechos globales, identificadores de llaves, todos los atributos de llaves, cualquier restricción sobre valores llaves (por ejemplo, llaves con o sin diversificación), bloqueos y techos iniciales, etc.

En esta sección, se presenta la definición básica de la arquitectura de seguridad para el SIR del SITM-Q. Esta información debe ser utilizada por el proveedor de llaves Calypso quien lleva a cabo la ceremonia de llaves del sistema, en la cual se definen los *secret roots* y los datos específicos de configuración de módulos SAM (se extiende la definición de SAM a la de HSM, i.e., las especificaciones aplican tanto para módulos SAM como para HSM), así como documentación confidencial que solo podrá compartirse entre el propietario de las llaves y el proveedor de llaves, la cual debe contener la guía detallada para la emisión de los módulos SAM definitivos del sistema. Adicionalmente, es necesario considerar toda la documentación sobre módulos SAM de Calypso para llevar a cabo la emisión y la definición final de la funcionalidad de estos dentro de la arquitectura de seguridad. Será responsabilidad del proveedor de llaves Calypso, entidad encargada de la ceremonia de llaves, definir el documento final de la arquitectura de seguridad del sistema.

Se especifican los módulos SAM necesarios para efectuar todas las operaciones de seguridad necesarias para la manipulación de medios de pago. Definición de los tipos de SAM que serán asignados a diferentes actores dentro del SITM-Q y definición del contenido de llaves que tendrá cada SAM. También se hace una definición del entorno de emisión y administración de módulos SAM.

6.1 Modelo de seguridad de medios de pago

6.1.1 Seguridad en medios de pago recargables

Para todos los medios de pago recargables, esta norma exige el uso del esquema de cifrado por bloques TDES definido en el estándar SP 800-67 Revisión 2 [23]. Por lo tanto, la comunicación llevada a cabo entre un SAM y un medio de pago sin contacto debe hacer uso de TDES utilizando bloques de cifrado de 128 bits, siempre que sea necesario, según [2].

Adicionalmente, las llaves que se almacenan en los medios de pago recargables deben ser diversificadas para garantizar su unicidad dentro de toda la red interoperable, es decir, cada medio de pago almacenará un conjunto de llaves único, derivado de llaves determinadas en una ceremonia de llaves de conformidad con [22]. Para llevar a cabo la diversificación es necesario hacer uso de módulos SAM-C1 con funciones de diversificación de llaves. Por esta razón, es necesario fijar en los derechos de transferencia de llaves que es obligatorio hacer uso de la diversificación, como se indica en [22]. La diversificación en medios de pago Calypso depende del serial único (UID) utilizado para identificar el medio de pago.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

6.1.2 Seguridad en medios de pago no recargables

La información almacenada en medios de pago no recargables puede leerse y escribirse libremente, sin necesidad de ejecutar algoritmos de cifrado como en el caso de los medios de pago recargables. Por esta razón, con el fin de garantizar la integridad de los datos y evitar evasión del pago con medios de pago no recargables, cada vez que se efectúe una transacción que modifique los datos almacenados en la tarjeta, es necesario grabar una firma digital en ella haciendo uso de un SAM-C1 de Calypso. La firma digital debe calcularse utilizando una llave para firma de transacciones almacenada para este fin y su validez debe verificarse utilizando las funciones PSO del módulo SAM-C1, cada vez que se efectúe una transacción de aceptación del medio de pago. De esta forma, la seguridad de medios de pago no recargables recae sobre el dispositivo de aceptación de medios de pago no recargables.

Como medida adicional opcional, se sugiere la implementación de una lista de medios no recargables inválidos. Esta lista permitiría denegar el ingreso al sistema de aquellos medios de pago que presentan comportamiento fraudulento, según sea definido por el operador. De implementarse esta lista, cada operador debe notificar a la Cámara de Compensación el serial de cada medio de pago que desea invalidarse. La Cámara entonces estará encargada de mantener actualizada la lista con los seriales de los medios de pago inválidos, y distribuirla a todos los operadores. Estos a su vez, deben encargarse de distribuir la lista a los dispositivos de validación. La lista deberá ser consultada cada vez que un medio de pago no recargable se acerque al validador, y debe rechazarse cualquier medio de pago que aparezca allí reportado. También se recomienda que la lista de medios de pago no recargables inválidos se implemente como una lista ordenada, de tal manera que se reduzca el tiempo necesario para la comprobación de la misma.

6.2 Tipos de SAM

Los módulos SAM son dispositivos habilitados para almacenar llaves y efectuar operaciones de seguridad con los medios de pago. La responsabilidad de la entrega de los módulos SAM a las entidades participantes es del Proveedor de SAMs. Los módulos SAM a ser entregados deben ser usar la tecnología SAM-C1, y deben cumplir todas las especificaciones presentadas en los documentos relacionados con el estándar Calypso.

Los módulos SAM para medios de pago Calypso pueden utilizarse para:

- Gestionar la seguridad de los medios de pago
- Gestionar la seguridad de módulos SAM
- Gestionar la seguridad de información sensible

Debido a que existen múltiples llaves para efectuar diferentes operaciones sobre los medios de pago, deben existir diferentes tipos de SAM según el uso que se le busca dar. En la Tabla 24 se describen los diferentes tipos de SAM-C1 que pueden existir en la red interoperable con medios de pago Calypso, el HCM-SP se denomina HCM maestro, y el resto de SAMs se denominan SAMs de producción (los SAMs de producción son los que se utilizan en dispositivos en campo para ejecutar las transacciones del sistema).

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Todas las entidades deben tener las mismas llaves para llevar a cabo procesos de recarga, validación, carga de SAMs, distribución de productos, emisión y autenticación de medios de pago no recargables, esto con el fin de garantizar interoperabilidad en el sistema.

Tabla 24. Descripción general de módulos SAM

Tipo	Abrev.	Uso
HSM de personalización de SAMs	HSM-SP	Permite cargar llaves en módulos SAM, así como controlar el máximo número de transacciones en dichos módulos.
SAM de inicialización de la entidad X	SAM-CPP-X	Permite diversificar y cargar las llaves de la aplicación de transporte en medios de pago.
SAM de emisión de la entidad X	SAM-CP-X	Permite la inicialización de los archivos de la aplicación del medio de pago recargable o no recargable.
SAM de distribución y recarga de productos	SAM-CL	Permite la distribución de productos y la carga de saldo de transporte en la tarjeta (en el monedero o en contadores), con un número controlado de transacciones.
SAM de validación	SAM-CV	Permite validar transacciones y debitar saldo de los recargables y de los no recargables.

Ahora bien, cada uno de estos módulos SAM se asignará a distintos actores, dependiendo de los roles que desempeñen dentro de la red interoperable. A continuación, se muestran los SAMs que deben ser asignados a cada uno de estos actores:

Tabla 25. Asignación de módulos SAM

Rol	SAM
Proveedor de llaves	HSM-SP
Inicializador de medios de pago	SAM-CPP-X
Emisor de medios de pago	SAM-CP-X
Distribuidor de productos	SAM-CL
Operador de recaudo	SAM-CL y SAM-CV

El contenido de los diferentes módulos SAM se describe en el Anexo 12. Dependiendo de las llaves almacenadas por el SAM, va a ser posible realizar las diferentes operaciones sobre los archivos de la aplicación interoperable. Es decir, los permisos de cada actor están definidos por las llaves almacenadas en los tipos de SAM asignados a su rol.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

6.3 Llaves del sistema y de trabajo en módulos SAM

En los sistemas Calypso existen dos tipos de llaves, i.e., las llaves del sistema (*system keys)*, almacenadas únicamente en módulos SAM, y las llaves de trabajo (*work keys*), que pueden estar almacenadas tanto en módulos SAM como en medios de pago para poder realizar las transacciones del sistema. Tomando como referencia las especificaciones Calypso, existen cuatro llaves de sistema que pueden almacenarse en los módulos SAM-C1:

- Llave de personalización de SAMs (*Personalization key)*: permite descifrar y autorizar la escritura de parámetros en módulos SAMs y las llaves de sistema.

- Llave para escritura de SAMs (*Work file key):* permite descifrar y autorizar la escritura de llaves de trabajo.

- Llave para carga de SAMs (*Reloading key*): permite descifrar y autorizar la escritura de los valores techo de eventos registrados con contadores en módulos SAM.

- Llave para autenticación de SAMs (*Authentication key*): permite generar firmas digitales a partir de datos leídos por un módulo SAM.

En [24], se presentan las llaves del sistema que debe contener cada uno de los módulos SAM del sistema. Los parámetros de las llaves de sistema que se presentan en [24], son los que deben conservar los módulos SAM de producción, para el HSM-SP es necesario fijar condiciones de transferencia de llaves de sistema, como se especifica en [25]. También es importante considerar que no se debe utilizar un HSM-SP para cargar llaves a medios de pago, su uso debe limitarse a transferir llaves de sistema o de trabajo a cada uno de los SAM de producción.

Una vez emitidos, no debe ser posible cambiar los parámetros del HSM-SP.

Por otro lado, las llaves de trabajo se seleccionan con base en los requerimientos de seguridad transaccional de medios de pago en el SIR. Dentro de las llaves de trabajo están las llaves de trabajo que se almacenan para controlar el acceso a cada uno de los DF en medios de pago recargables. También está la llave de trabajo que controla la emisión y validación de medios de pago no recargables por medio de firmas digitales. A continuación, se resumen los tipos de llaves de trabajo que se definen para el SIR del SITM-Q:

- Llave de emisor MAESTRO: debe usarse para ejecutar comandos de Sesión # 1 dentro del DF MAESTRO.

- Llave de recarga MAESTRO: debe usarse para ejecutar comandos de Sesión # 2 dentro del DF MAESTRO.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- Llave de validación MAESTRO: debe usarse para ejecutar comandos de Sesión # 3 dentro del DF MAESTRO.

- Llave de emisor TRANSPORTE_QUITO: debe usarse para ejecutar comandos de Sesión # 1 dentro del DF TRANSPORTE_QUITO.

- Llave de recarga TRANSPORTE_QUITO: debe usarse para ejecutar comandos de Sesión # 2 dentro del DF TRANSPORTE_QUITO. Por ejemplo, para escribir un registro específico de los archivos CONTRATOS, SERVICIOS o LISTA_CONTRATOS.

- Llave de validación TRANSPORTE_QUITO: debe usarse para ejecutar comandos de Sesión # 3 dentro del DF TRANSPORTE_QUITO.

- Llave de emisor MONEDERO: debe usarse para ejecutar comandos de Sesión # 1 dentro del DF MONEDERO.

- Llave de recarga MONEDERO: debe usarse para ejecutar comandos de Sesión # 2 dentro del DF MONEDERO.

- Llave de validación MONEDERO: debe usarse para ejecutar comandos de Sesión # 3 dentro del DF MONEDERO.

- Llave de autenticación para no recargables: debe usarse para escribir y validar firmas digitales en medios de pago no recargables para efectuar transacciones de emisión y validación.

En el archivo [24] se presentan los parámetros de las llaves de trabajo que deben quedar almacenadas en los medios de pago recargables, para generar llaves de trabajo para módulos SAM es necesario grabarlas con parámetros de transferencia que permitan obtener los parámetros finales en los medios de pago como se especifica en el anexo.

Es importante tener en cuenta que el código KIF de algunas llaves puede llegar a ser el mismo, por ejemplo, en el caso de las llaves de trabajo que dan permisos de emisor a distintas entidades. Si llega a darse el caso de que el KIF de múltiples llaves es el mismo, estas deben diferenciarse por el código de versión KVC, el cual debe ser asignado por el ente Registrador.

6.4 Contadores de módulos SAM

Se deben utilizar contadores para llevar el registro del número de transacciones que se han llevado a cabo con una o varias llaves de trabajo o de sistema almacenadas en un módulo SAM. El valor de un contador asociado a una o varias llaves, se utilizará para registrar el campo ConsecutivoSAM que se envía al sistema central en cada transacción.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Un SAM-C1 de Calypso tiene 27 contadores de eventos, cada uno con 3 bytes. Es decir que para cada conjunto de llaves asociado a un contador se pueden registrar hasta 16777216 transacciones. Por seguridad, no es posible reiniciar la cuenta de los contadores, solo es posible aumentarlos y limitar su valor máximo *(Ceiling).* Por esta razón, cuando un SAM alcanza el tope máximo es necesario recargarlo usando el HSM-SP a cargo del administrador de los módulos del sistema. El HSM debe habilitarse para poder modificar los valores máximos permitidos para los contadores de cada SAM del sistema interoperable que se encuentre en campo. Las especificaciones de la conexión al servidor del HSM para realizar este proceso se describirán en la siguiente sección. Cuando el contador alcanza el valor de 16777216, el módulo SAM debe reemplazarse por uno nuevo, y debe destruirse, según las recomendaciones de [25].

La opción FreeIncrementDisableBit debe estar habilitada para que siempre se pueda usar la función *increment* para todos los contadores, es decir, debe ser igual a cero. La función *increment* del SAM-C1 se debe utilizar para aumentar la cuenta de un contador asociado a una transacción específica con un módulo SAM.

6.5 Aumento de límite de recargas de SAMs mediante HSM

Los contadores anteriormente mencionados poseen valores máximos llamados *Ceilings*, estos son usados para limitar el número de recargas que puede realizar un módulo SAM. Esto se hace con el fin de mejorar la seguridad del sistema, ya así se previene la posibilidad de realizar numerosas recargas fraudulentas en caso de hurto de un módulo SAM. Este mecanismo también facilita el control de las recargas disponibles en los puntos de red externa de forma remota.

Por lo anterior, es necesario administrar el valor máximo para el contador de recarga de todos los módulos SAM del sistema y aumentarlos progresivamente de acuerdo a las solicitudes que realice cada uno de los equipos de recarga. Estas solicitudes deberán emitirse automáticamente cuando un equipo detecte que el contador de recarga del módulo SAM posee menos de 50 recargas disponibles, para el caso de equipos en estaciones de Metro o BRT. Para equipos de la red externa, esta solicitud debe hacerse cada vez que se reinicie el equipo.

Para la administración de los módulos SAM del sistema se debe implementar una base de datos que contenga toda la información relevante para realizar una detallada administración y auditoría de las recargas disponibles en el sistema. Dicha base de datos deberá incluir al menos la siguiente información: serial del SAM, aumento disponible para el contador de recargas y si el módulo SAM se encuentra habilitado para el aumento de límite de recargas.

El uso de ésta base de datos permitirá administrar las recargas adquiridas para módulos SAM de la red externa de recargas y para bloquear los módulos SAM que se han reportado cómo hurtados. De esta forma, cada vez que se reciba una solicitud será necesario revisar si el módulo SAM para el que se está emitiendo la solicitud es apto para el aumento del valor máximo del contador de recargas.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Vale la pena aclarar que los puntos de red externa deberán adquirir sus recargas mediante un operador de recaudo, el cual se comunicará con la entidad administradora del HSM para que esta actualice en su base de datos el límite de recargas que cada SAM va a tener.

6.5.1 Transacción de aumento de valor máximo de contador de recargas

De forma general esta transacción debe dividirse en dos partes: solicitud hecha por el equipo de recarga y respuesta enviada por el HSM. La conexión entre los equipos de recarga y el HSM se hará mediante el protocolo TCP-IP. El HSM del sistema deberá poseer una dirección IP pública hacia la cual deberán conectarse todos los equipos que posean módulo(s) SAM de recarga para emitir sus respectivas solicitudes.

Vale la pena agregar que todos los comandos ejecutados en este proceso deberán usar cifrado dinámico [11], no sólo porque es la forma más segura, sino operativamente también la forma más sencilla de implementar esta transacción.

2.1.1.3. Solicitud de aumento de límite de recargas

Para realizar la solicitud de aumento de límite del contador de recargas se debe realizar una solicitud al HSM por medio de una conexión TCP-IP. En dicha solicitud se incluirá toda la información necesaria para el aumento del límite del contador de recargas y ser enviada a través de la conexión TCP-IP con el HSM.

Para crear la solicitud se deberá ejecutar el comando ***Get Challenge*** *(descrito en* [11]*)* en el SAM a recargar y guardar la respuesta *(Challenge)*. Posteriormente, se debe ensamblar un datagrama TCP estándar siguiendo el siguiente esquema de datos:

Formato de Cabecera TCP estándar (20 Bytes) Datos (12 Bytes)

El Formato de cabecera TCP estándar, estará compuesto por la siguiente información:

Puerto de origen (2 Bytes) Puerto de destino (2 Bytes)

Número de secuencia (4 Bytes)

Número de confirmación (4 Bytes)

Offset (4 bits) RFU (3 bits) Banderas (9 bits) Tamaño de ventana (2 Bytes)

Suma de comprobación (2 Bytes) Apuntador de urgencia (2 Bytes)

De la misma manera se definieron los datos de la solicitud de la siguiente forma:

DATO	LONGITUD	VALOR
ID transacción	1 Byte	“AC”

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Serial SAM	4 Bytes	Serial del SAM a recargar
Número Contador	1 Byte	00h → 1Ah (valores entre 0 y 26)
Valor actual contador	3 Bytes	-
Límite actual contador	3 Bytes	-
Challenge	8 Bytes	Respuesta del comando *Get Challenge.*

2.1.1.4. Respuesta del HSM

Cuándo el HSM reciba la solicitud de aumento de valor máximo para el contador de recargas y se deberá seguir el siguiente proceso:

1. Verificar que la solicitud corresponde a un módulo SAM que no está reportado cómo hurtado y en caso de ser un módulo SAM de la red externa de recargas se deberá verificar que hay un aumento del límite de recargas disponible para dicho módulo SAM.

2. Ejecutar el comando ***Select Diversifier*** *(descrito en* [11]*)* en el HSM. Usando el serial del SAM objetivo incluido en la solicitud cómo *Diversificador*.

3. Ejecutar el comando ***Give Random*** *(descrito en* [11]*)* en el HSM usando la respuesta de *Get Challenge* incluida en la solicitud.

4. Ejecutar el comando ***Cipher Ceiling*** *(descrito en* [11]*)* en el HSM, usando la información de la solicitud y de la base de datos para construir el comando y guardar la respuesta.

5. Construir el comando ***Write Ceiling*** *(descrito en* [11]*)* para ser ejecutado en el SAM objetivo, usando la respuesta de *Cipher Ceiling* como mensaje encriptado.

6. Enviar la respuesta al equipo siguiendo este formato:

Formato de Cabecera TCP estándar (20 Bytes)	Comando *Write Ceiling* (53 Bytes)

7 Datos Asignados por el Registrador

A lo largo del presente documento se han mencionado diferentes campos y valores que deben ser asignados por el Registrador. Esta sección presenta un resumen de dichos valores y el momento en que deben ser asignados. Adicionalmente se realiza una discriminación de los datos según la relevancia de estos.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

7.1 Datos relevantes para la red interoperable

Nombre del dato	Momento de asignación
Identificador de la red interoperable	Antes de la constitución de la red interoperable
Identificador de la entidad propietaria de la aplicación interoperable	

7.2 Datos relevantes para la aplicación interoperable

Nombre del dato	Momento de asignación
Versión de la aplicación interoperable	Cada vez que se realice una modificación a la estructura de datos de la aplicación interoperable
Identificador de la versión de llaves almacenadas en la aplicación interoperable	Cada vez que se realice una actualización de una o más llaves de la red interoperable

7.3 Datos relevantes para productos

Nombre del dato	Momento de asignación
Identificador del producto	Antes de la constitución de la red interoperable o cada vez que el Registrador considere adecuado modificar un valor
Prioridad del producto	
Tiempo de *passback*	
Tiempo de transbordo	
Tiempo máximo de viaje	
Transbordos permitidos dentro del tiempo de transbordo	
Passbacks permitidos dentro del tiempo de passback	
Mínimo valor que puede almacenar cada producto (puede ser negativo)	
Máximo valor que puede almacenar cada producto (debe ser mayor o igual a cero)	
Número máximo de viajes por días de la semana	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Número máximo de viajes por mes	

7.4 Datos relevantes para empresas emisoras de medios de pago

Nombre del dato	Momento de asignación
Identificador de la entidad emisora de medios de pago	Durante el ingreso a la red interoperable
Identificador de cada dispositivo de emisión de la red interoperable	
Versión de la llave de emisión para cada emisor de medios de pago en un SAM de emisión de la entidad X	

7.5 Datos relevantes para empresas distribuidoras de medios de pago

Nombre del dato	Momento de asignación
Red a la que pertenece el distribuidor de productos	Durante el ingreso a la red interoperable
Identificador del distribuidor de productos	
Identificador de cada dispositivo de distribución y recarga de la red interoperable	
Versión de las llaves para distribución de productos de los SAMs de distribución de productos Y, para un emisor de medios de pago	

7.6 Datos relevantes para empresas aceptadoras de medios de pago

Nombre del dato	Momento de asignación
Identificador de la red a la cual pertenece la entidad aceptadora	Durante el ingreso a la red interoperable
Identificador de la empresa aceptadora de medios de pago	
Identificador de cada dispositivo de aceptación de medios de pago de la red interoperable	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

8 Casos de uso de medios de pago

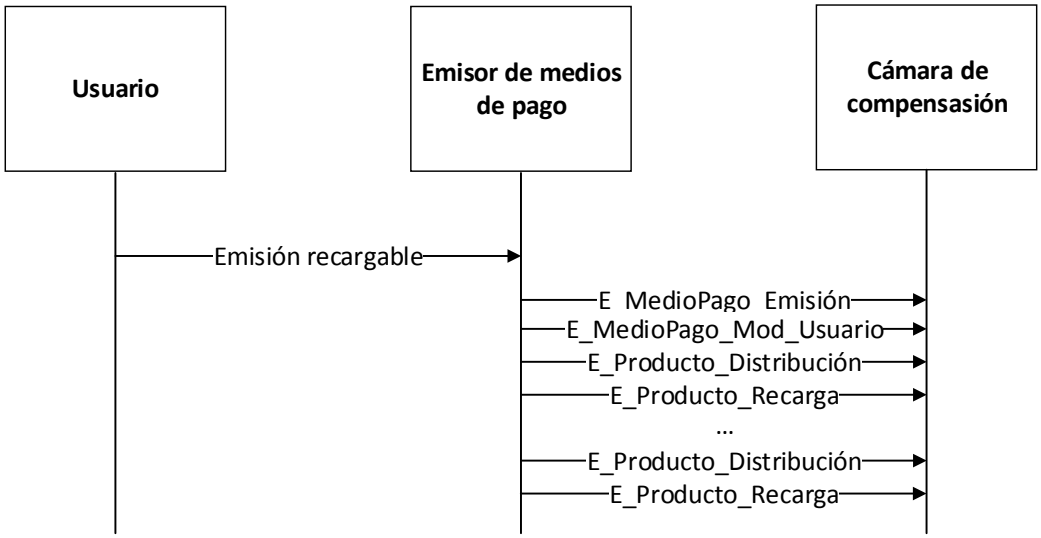
Los casos de uso de medios de pago describen las posibles interacciones que se pueden dar en el SIR y en las cuales es necesaria la comunicación entre las Empresas Operadoras de Recaudo y la Cámara de Compensación. Dicha comunicación está compuesta por un intercambio de mensajes elementales que representan cada uno un evento. A continuación, se describen los casos de uso para todos los posibles eventos de uso de un medio de pago.

8.1 Emisión de medio de pago recargable

Nombre del caso de uso	**Emisión de medio de pago recargable**
Resumen	Un usuario adquiere un medio de pago con producto general como mínimo y un saldo inicial.
Prerrequisitos	Medio de pago inicializado
Accionado por	Usuario
Actores	Usuario Emisores de medios de pago Cámara de Compensación
Descripción del caso de uso	Un medio de pago con la aplicación interoperable es entregado a un usuario por parte del emisor del medio de pago a través de un dispositivo de emisión de medios de pago. El dispositivo de emisión de medios de pago efectúa: ▪ Emisión del medio de pago a través de la escritura de la aplicación interoperable ▪ (Opcional) Modificación de datos de usuario. ▪ Distribución y recarga inicial del producto general (esto es obligatorio antes de darle la tarjeta por primera vez al usuario). ▪ (Opcional) Distribuir otros productos asociados al perfil de usuario. ▪ Creación de nuevas entradas en el archivo EVENTOS del medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 13. Eventos enviados en la emisión de un medio de pago recargable



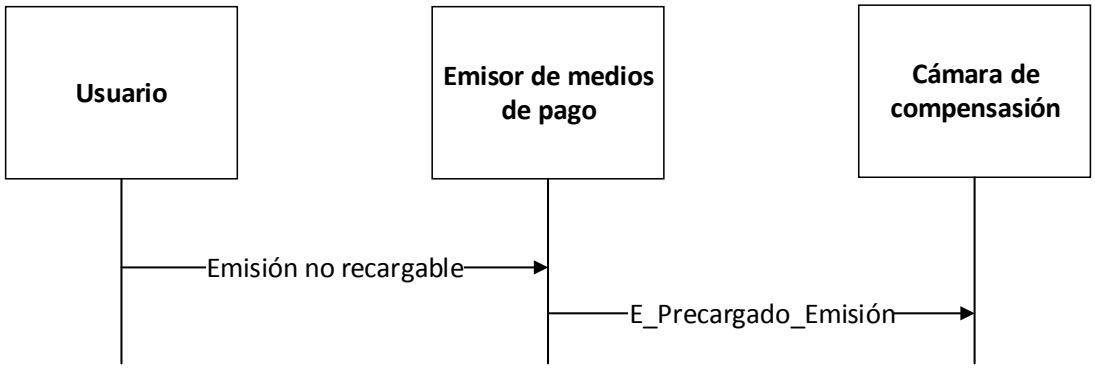
Fuente: elaboración propia

8.2 Emisión de medio de pago no recargable

Nombre del caso de uso	Emisión de medio de pago no recargable
Resumen	Un emisor de medios de pago emite medios de pago no recargables para ser usados en la red interoperable.
Prerrequisitos	Ninguno
Accionado por	Usuario
Actores	Usuario Emisores de medios de pago no recargables Cámara de Compensación
Descripción del caso de uso	El emisor de medios de pago no recargables emite un medio de pago no recargable y se lo entrega al usuario. A través de un dispositivo de emisión de medios de pago no recargables se realiza: ▪ Almacenamiento de los datos de emisión del medio de pago, incluyendo saldo inicial, datos de entorno y evento de emisión. ▪ Envío de la información de emisión a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 14. Eventos enviados en la emisión de un medio de pago no recargable



Fuente: elaboración propia

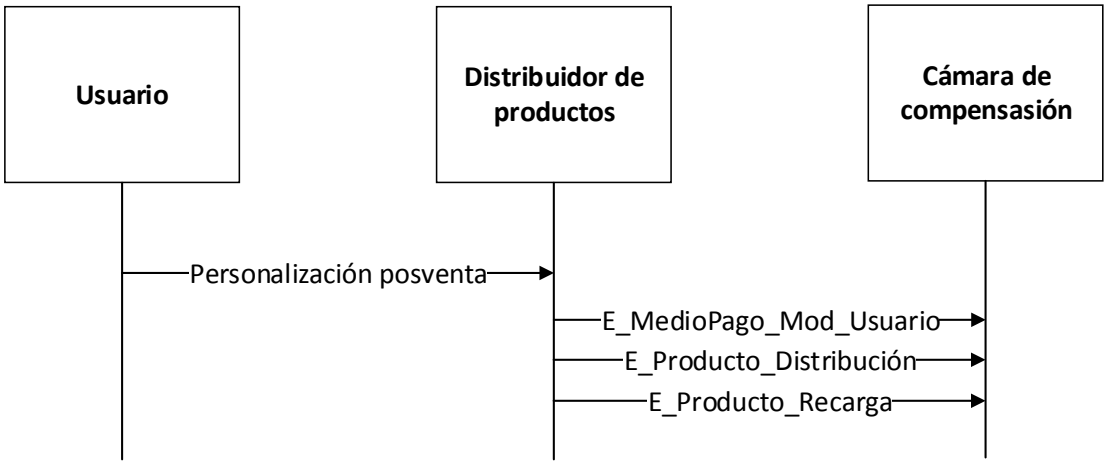
8.3 Personalización posventa del medio de pago recargable

Nombre del caso de uso	Personalización del medio de pago anónimo
Resumen	Un usuario con un medio de pago anónimo entregado por un emisor de medios de pago solicita la personalización del mismo.
Prerrequisitos	Emisión de medio de pago con perfil general
Accionado por	Usuario
Actores	Usuario Distribuidor de producto Cámara de Compensación
Descripción del caso de uso	Dado un medio de pago anónimo emitido por una entidad, un usuario solicita a dicha entidad personalizar este medio de pago. A través de un dispositivo de emisión de medios de pago, este emisor realiza: ▪ Personalización del medio de pago almacenando los datos necesarios en el archivo USUARIO del medio de pago. ▪ Si el perfil requiere distribución de producto, modificar los archivos LISTA CONTRATOS, CONTRATOS y SERVICIOS según sea necesario. ▪ Si el perfil requiere la distribución de un producto, se debe crear el evento de distribución de producto, así como la recarga del archivo de valor asociado a este producto. ▪ Si el perfil requiere la suspensión de un producto, se debe realizar este proceso y enviar un evento de confirmación LAP_A.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	▪ Envío de la información de eventos a la Cámara de Compensación.

Figura 15. Eventos enviados durante la personalización posventa de un medio de pago recargable



Fuente: elaboración propia

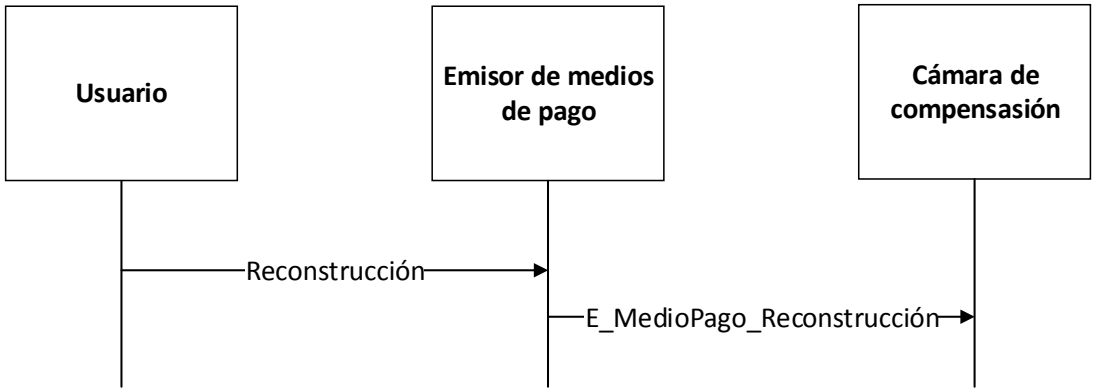
8.4 Reconstrucción del medio de pago

Nombre del caso de uso	**Reemplazo del medio de pago**
Resumen	Un usuario solicita un nuevo medio de pago debido a que lo ha extraviado o averiado.
Prerrequisitos	Emisión de medio de pago personalizado
Accionado por	Usuario
Actores	Usuario Emisor de medios de pago Cámara de Compensación
Descripción del caso de uso	Un usuario solicita al emisor con el cual ha adquirido un medio de pago la reconstrucción del mismo. El emisor de medios de pago debe reconstruir el medio de pago usando la información recolectada de los eventos ocurridos en dicho medio de pago. Para este nuevo medio de pago se deben efectuar las siguientes acciones: ▪ Emisión del nuevo medio de pago. ▪ Personalización posventa del medio de pago en el caso en que el medio de pago anterior almacenara un perfil de

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	usuario. ▪ Distribución de los productos almacenados en el medio de pago a reconstruir. ▪ Recarga de archivos de valor almacenados en el medio de pago a reconstruir. ▪ Envío de la información del evento de reconstrucción a la Cámara de Compensación.

Figura 16. Eventos enviados para la reconstrucción de un medio de pago

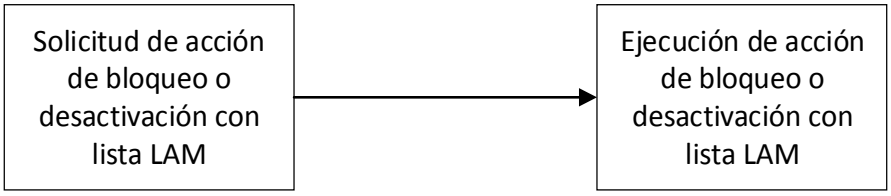


Fuente: elaboración propia

8.5 Bloqueo o desactivación del medio de pago

Las acciones de bloqueo o desactivación de medios de pago están compuestas por la siguiente secuencia de casos de uso que deben efectuar múltiples actores de la red interoperable.

Figura 17. Secuencia de casos de uso necesarios para el bloqueo o desactivación del medio de pago



Fuente: elaboración propia

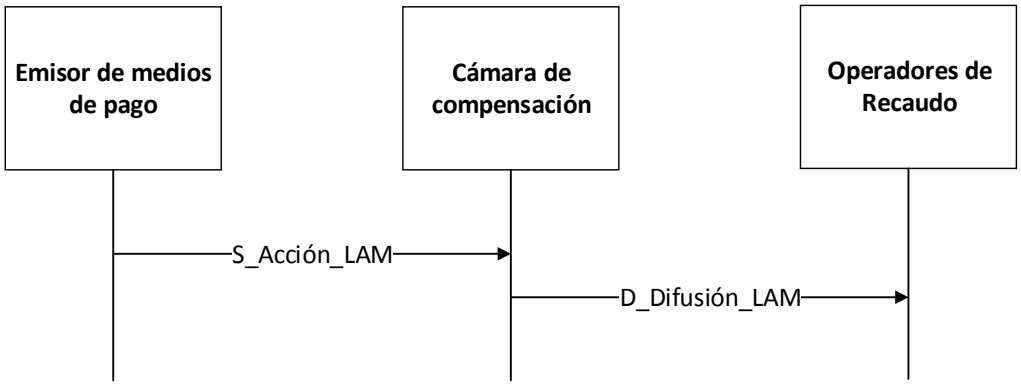
A continuación, se describen los dos casos de uso que se deben efectuar para lograr el bloqueo o desactivación de un medio de pago.

Nombre del caso de uso	**Solicitud de acción de bloqueo o desactivación con lista LAM**
Resumen	Un emisor de medios de pago adquiere un motivo por el cual es necesario el bloqueo o desactivación de un medio de pago que ha emitido.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Prerrequisitos	Emisión de medio de pago con perfil anónimo o Emisión de medio de pago personalizado
Accionado por	Emisor de medios de pago
Actores	Emisores de medios de pago Cámara de Compensación Operador de recaudo
Descripción del caso de uso	El emisor de medios de pago envía a la Cámara de Compensación un mensaje donde solicita la actualización de la lista LAM con una operación de bloqueo o desactivación sobre un medio de pago. La Cámara de Compensación reenvía la solicitud a todos los demás emisores del sistema. Todos los emisores deberán ejecutar la solicitud y actualizar la lista LAM en sus dispositivos de aceptación de medios de pago y de venta y recarga de medios de pago.

Figura 18. Evento enviado durante la solicitud de acción de bloqueo o desactivación con lista LAM



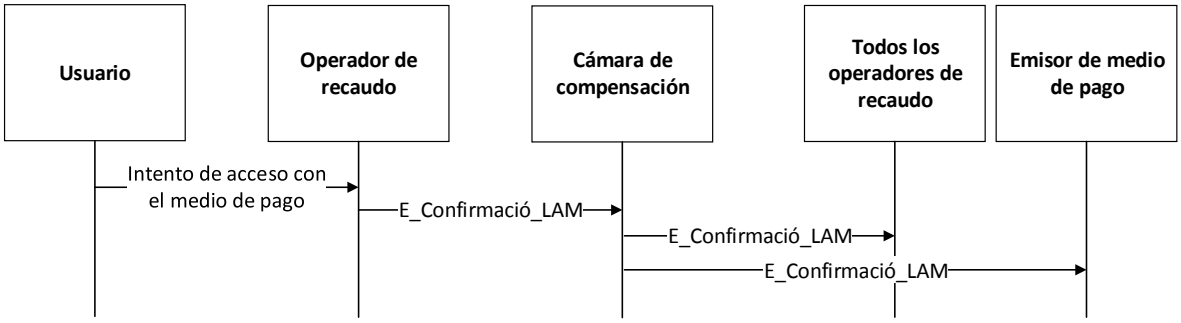
Fuente: elaboración propia

Nombre del caso de uso	**Ejecución de acción de bloqueo o desactivación con lista LAM**
Resumen	Un usuario intenta acceder a un servicio de transporte con un medio de pago al cual se le debe aplicar una acción de bloqueo o desactivación de lista LAM
Prerrequisitos	Solicitud de acción de bloqueo o desactivación con lista

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	LAM
Accionado por	Usuario
Actores	Empresas Operadoras de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario intenta usar su medio de pago para acceder a un servicio de la red interoperable acercándolo a un dispositivo de aceptación de medios de pago. El operador de recaudo al cual se le solicita el acceso realiza las siguientes acciones con dicho dispositivo: ▪ Verificación de la existencia de una acción disponible para el medio de pago presentado en lista LAM. ▪ Ejecución de la acción en el medio de pago mediante escritura de datos. ▪ Almacenamiento del evento de ejecución de la acción con lista LAM ▪ Envío de una confirmación del evento efectuado a la Cámara de Compensación. Todas las empresas operadoras de recaudo deben actualizar la lista LAM con esta nueva información.

Figura 19. Eventos enviados durante la ejecución de acción de bloqueo o desactivación con lista LAM



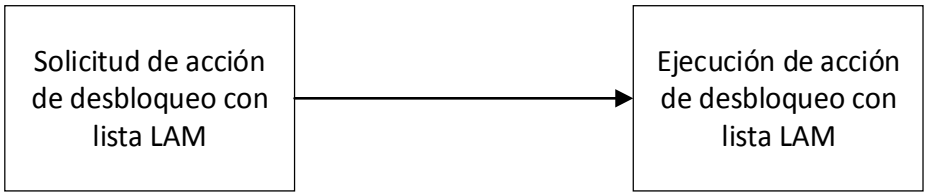
Fuente: elaboración propia

8.6 Desbloqueo del medio de pago

La acción de desbloqueo de medios de pago está compuesta por la siguiente secuencia de casos de uso que deben efectuar múltiples actores de la red interoperable.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 20. Secuencia de casos de uso necesarios para el desbloqueo del medio de pago



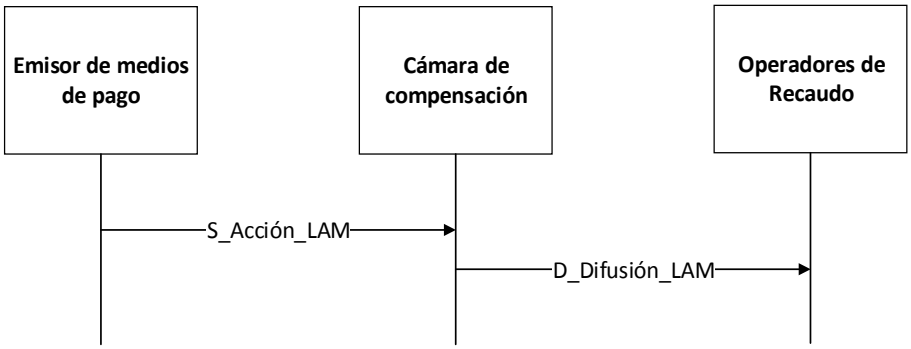
Fuente: elaboración propia

A continuación, se describen los dos casos de uso que se deben efectuar para lograr el desbloqueo de un medio de pago.

Nombre del caso de uso	**Solicitud de acción de desbloqueo con lista LAM**
Resumen	Un emisor de medios de pago adquiere un motivo por el cual es necesario el desbloqueo de un medio de pago que ha sido bloqueado previamente.
Prerrequisitos	Ejecución de acción de bloqueo con lista LAM
Accionado por	Emisor de medios de pago
Actores	Emisores de medios de pago Cámara de Compensación Operadores de recaudo
Descripción del caso de uso	El emisor de medios de pago envía a la Cámara de Compensación un mensaje donde solicita la actualización de la lista LAM con una operación de bloqueo o desactivación sobre un medio de pago. La Cámara de Compensación reenvía la solicitud a todos los demás emisores del sistema. Todos los emisores deberán ejecutar la solicitud y actualizar la lista LAM en sus dispositivos de aceptación de medios de pago y de venta y recarga de medios de pago.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 21. Eventos enviados durante la solicitud de acción de desbloqueo con lista LAM

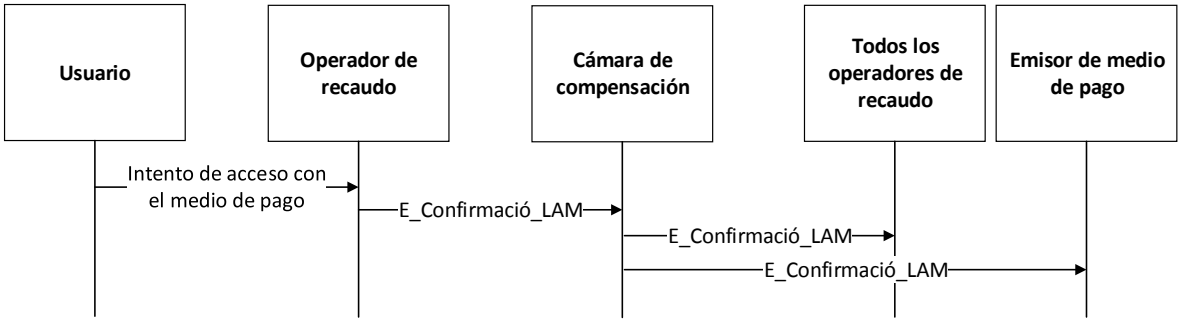


Fuente: elaboración propia

Nombre del caso de uso	Ejecución de acción de desbloqueo con lista LAM
Resumen	Un usuario intenta acceder a un servicio con un medio de pago al cual se le debe aplicar una acción de desbloqueo con la lista LAM
Prerrequisitos	Solicitud de acción de desbloqueo con lista LAM
Accionado por	Usuario
Actores	Operadoras de Recaudo Cámara de Compensación Emisor de medios de pago Usuario
Descripción del caso de uso	Un usuario intenta usar su medio de pago para acceder a un servicio de la red interoperable acercándolo a un dispositivo de aceptación de medios de pago. El operador de recaudo al cual se le solicita el acceso realiza las siguientes acciones con dicho dispositivo: ▪ Verificación de la existencia de una acción disponible para el medio de pago presentado en lista LAM. ▪ Ejecución de la acción en el medio de pago mediante escritura de datos. ▪ Almacenamiento del evento de ejecución de la acción con lista LAM ▪ Envío de una confirmación del evento efectuado a la Cámara de Compensación. Todas las empresas operadoras de recaudo deben actualizar la lista LAM con esta nueva información.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 22. Eventos enviados durante la ejecución de acción de desbloqueo con lista LAM



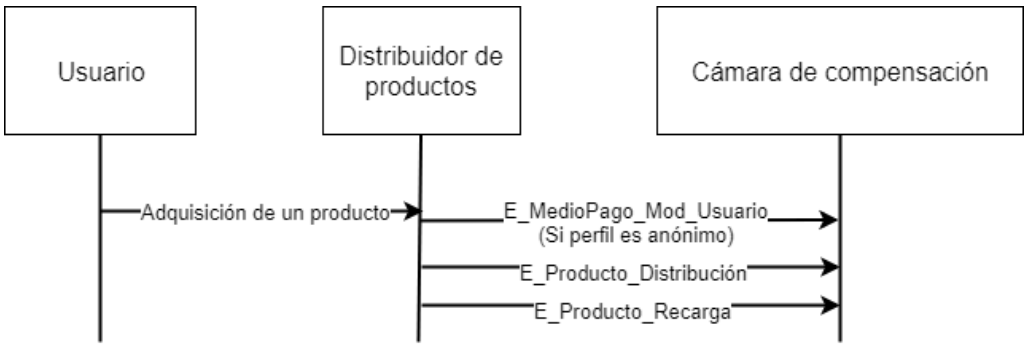
Fuente: elaboración propia

8.7 Adquisición de un producto posventa

Nombre del caso de uso	Adquisición de un producto
Resumen	Un usuario solicita un producto que aún no está activado en su medio de pago
Prerrequisitos	Emisión de medio de pago con perfil anónimo o Emisión de medio de pago personalizado
Accionado por	Usuario
Actores	Distribuidores de productos Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario solicita a un distribuidor de productos la distribución de un producto que no posee. A través de un dispositivo lector de medios de pago, este emisor realiza: ▪ Personalización del medio de pago si este es anónimo. ▪ Autorización, distribución, y recarga del producto solicitado, siempre y cuando corresponda al perfil de usuario almacenado en el medio de pago (según la información en el archivo USUARIO) ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 23. Eventos enviados durante la distribución de un producto posventa



Fuente: elaboración propia

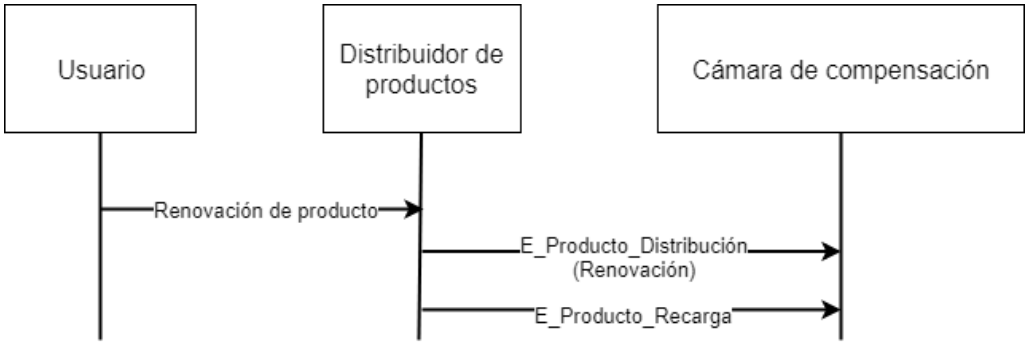
8.8 Renovación de un producto

Nombre del caso de uso	**Renovación de un producto**
Resumen	Un usuario solicita a un distribuidor de productos la renovación del contrato de un producto previamente distribuido en su medio de pago para extender su validez.
Prerrequisitos	Emisión de medio de pago de perfil general o Emisión de medio de pago personalizado o Adquisición de un producto
Accionado por	Usuario
Actores	Distribuidores de productos Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario solicita a un distribuidor de productos la renovación de un producto distribuido por dicho distribuidor. Este proceso equivale a una nueva distribución de producto en la que se sobrescriben los parámetros del producto. A través de un dispositivo lector de medios de pago, este distribuidor realiza: ▪ Autorización y renovación de los parámetros del producto solicitado. ▪ Opcionalmente, recarga del producto solicitado. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	Compensación.

Figura 24. Eventos enviados durante la renovación de un producto



Fuente: elaboración propia

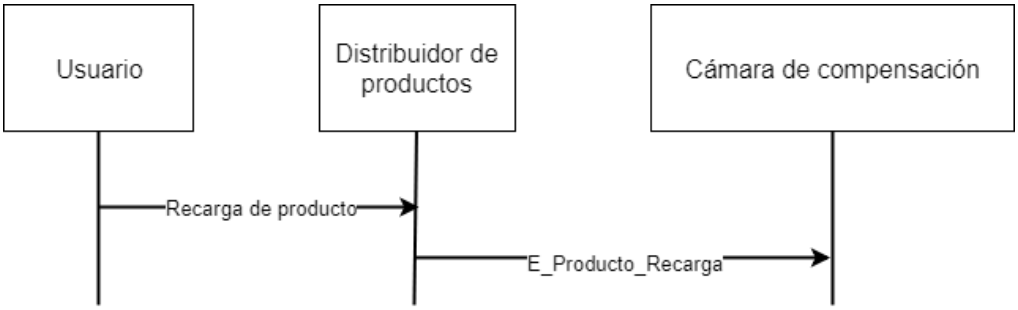
8.9 Recarga de un producto

Nombre del caso de uso	**Recarga de un producto**
Resumen	Un usuario solicita la recarga de valor de un producto almacenado en su medio de pago a un distribuidor de productos apropiado.
Prerrequisitos	Emisión de medio de pago con perfil anónimo o Emisión de medio de pago personalizado con producto por recargar asociado a **MONEDERO** o Emisión de medio de pago personalizado con producto por recargar asociado a contador Adquisición de un producto
Accionado por	Usuario
Actores	Operadores de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario solicita, a operador de recaudo autorizado, la recarga de un producto almacenado en su medio de pago. A través de un dispositivo de lector de medios de pago, este operador realiza: ▪ Recarga de valor del producto solicitado y generación del registro del evento en el medio de pago. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	Compensación.

Figura 25. Eventos enviados durante la recarga de un producto



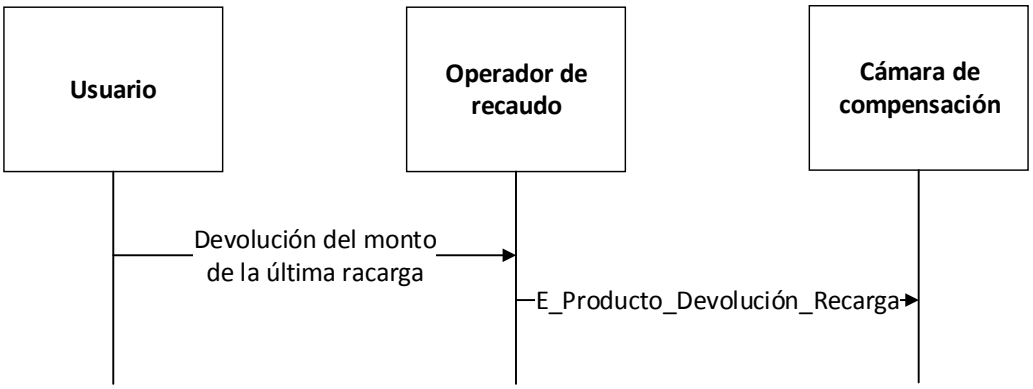
Fuente: elaboración propia

8.10 Devolución del monto de la última recarga

Nombre del caso de uso	**Devolución del monto de la última recarga**
Resumen	Un usuario u operador solicita la devolución del monto de la última recarga hecha en el medio de pago. Esta recarga debió haber sido hecha por el mismo distribuidor de productos que va a hacer la devolución.
Prerrequisitos	Recarga de un producto
Accionado por	Usuario u Operador de recaudo
Actores	Operadores de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario u operador solicita la devolución del monto de la última recarga hecha en el medio de pago. A través de un dispositivo de lector de medios de pago, este operador realiza: ▪ Devolución del monto de la última recarga. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 26. Eventos enviados durante la devolución del monto de la última recarga

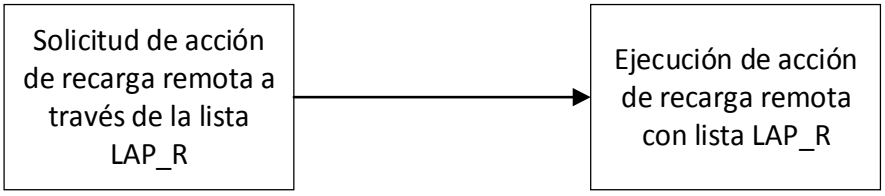


Fuente: elaboración propia

8.11 Recarga remota de productos a través de la lista LAP_R

La acción de recarga remota de productos está compuesta por la siguiente secuencia de casos de uso que deben efectuar múltiples actores de la red interoperable.

Figura 27. Secuencia de casos de uso necesarios para la recarga remota de productos



Fuente: elaboración propia

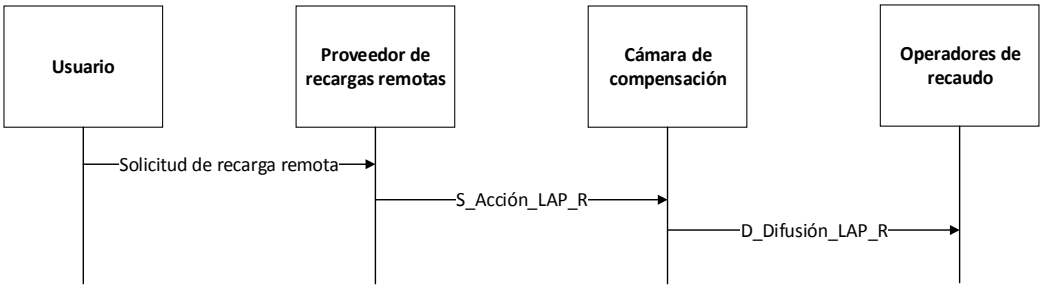
A continuación, se describen diferentes casos de uso que pueden llevarse a cabo para recargar productos en diferentes condiciones.

Nombre del caso de uso	**Solicitud de acción de recarga remota a través de la lista LAP_R**
Resumen	Un usuario solicita a un proveedor de recargas remotas, la recarga remota de un producto almacenado en su medio de pago.
Prerrequisitos	Emisión de medio de pago con perfil general o Emisión de medio de pago personalizado
Accionado por	Usuario
Actores	Proveedor de recargas remotas

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	Cámara de Compensación Operadores de recaudo Usuario
Descripción del caso de uso	El usuario solicita y paga a un proveedor la recarga remota de un producto almacenado en su medio de pago. Esta solicitud la realiza a través de un medio de comunicación no presencial. El proveedor de recargas remotas hace la solicitud de la recarga remota a la Cámara de Compensación y esta lo redistribuye a los demás operadores. Luego de recibir la solicitud, todos los distribuidores de productos deben actualizar la lista LAP_R en los dispositivos de recarga.

Figura 28. Eventos enviados durante la solicitud de acción de recarga remota a través de la lista LAP_R



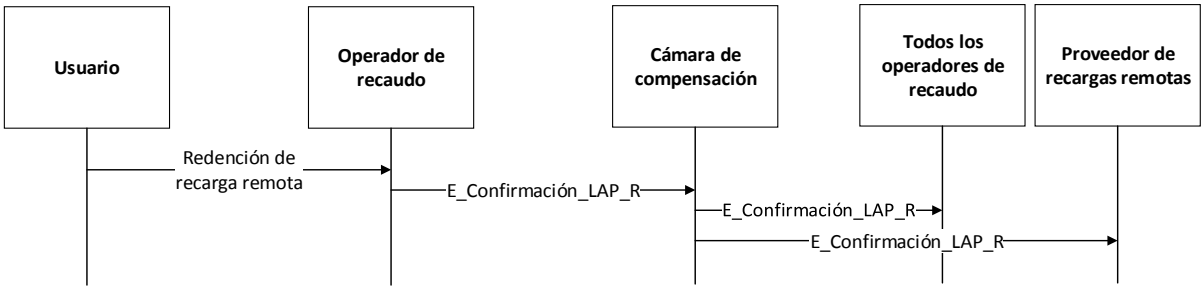
Fuente: elaboración propia

Nombre del caso de uso	**Ejecución de acción de recarga remota de producto general o especial con lista LAP_R**
Resumen	Un usuario lleva su medio de pago para redimir una recarga remota que ha realizado previamente.
Prerrequisitos	Solicitud de acción de recarga remota a través de la lista LAP_R
Accionado por	Usuario
Actores	Proveedor de recargas remotas

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	Operadores de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago en un dispositivo de recarga, por lo cual su recarga debe hacerse efectiva. El distribuidor de productos realiza las siguientes acciones con dicho dispositivo: ▪ Verificación de la existencia de una acción de recarga remota disponible para el medio de pago y el producto presentado. ▪ Ejecución de la acción de recarga del producto general o especial en el medio de pago mediante escritura de datos. ▪ Almacenamiento del evento de ejecución de la acción con lista LAP_R ▪ Envío de una confirmación del evento efectuado a la Cámara de Compensación.

Figura 29. Eventos enviados durante la ejecución de acción de recarga remota de producto general o especial con lista LAP_R



Fuente: elaboración propia

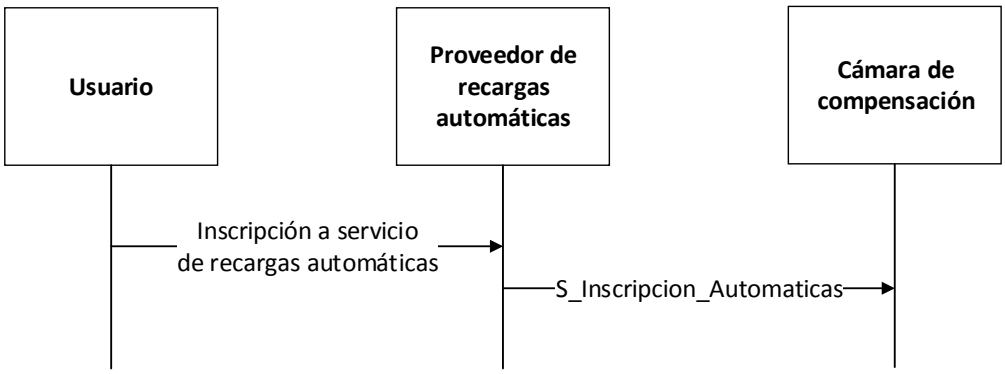
8.12 Inscripción a servicio de recarga automática

Nombre del caso de uso	**Inscripción a servicio de recarga automática**
Resumen	Un usuario se suscribe a un servicio de recarga automática ofrecido por un proveedor. Este proveedor inscribe la tarjeta personalizada del usuario ante la Cámara de Compensación.
Prerrequisitos	Emisión de medio de pago personalizado
Accionado por	Usuario

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Actores	Proveedor de recargas automáticas Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario se suscribe a un servicio de recarga automática ofrecido por un proveedor. El proveedor de recargas automáticas realiza las siguientes operaciones: ▪ Verificación que la identidad del usuario concuerda con la almacenada en el medio de pago personalizado. ▪ Registrar en su base de datos el monto de recarga y el umbral definido por el usuario. ▪ Enviar un evento de S_Inscripcion_Automatica a la cámara de Compensación para suscribir la tarjeta al servicio.

Figura 30. Secuencia de casos de uso necesarios para la inscripción a recargas automáticas

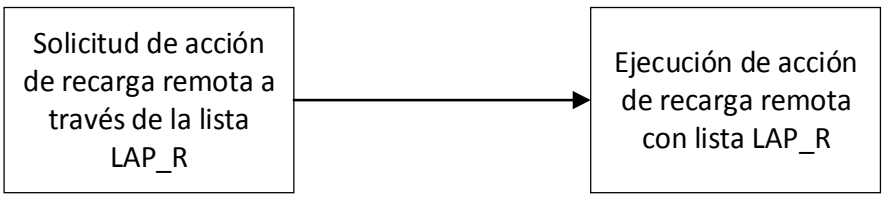


Fuente: elaboración propia

8.13 Renovación remota de productos a través de la lista LAP_RP

La acción de renovación remota de productos está compuesta por la siguiente secuencia de casos de uso que deben efectuar múltiples actores de la red interoperable.

Figura 31. Secuencia de casos de uso necesarios para la renovación remota de productos



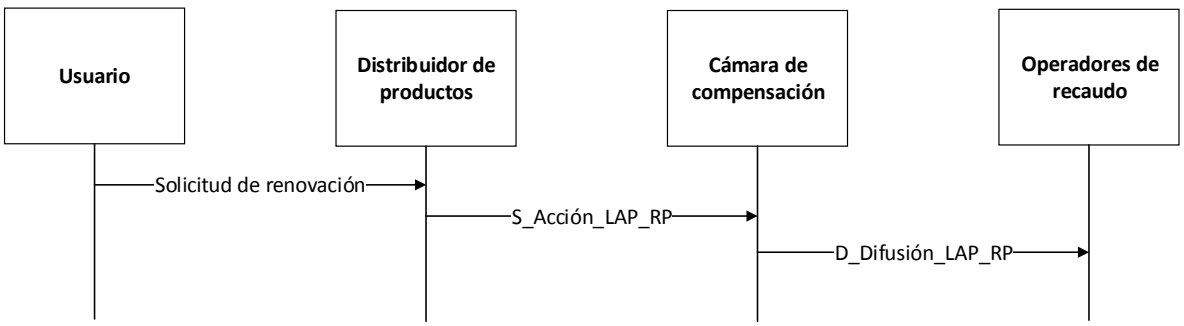
Fuente: elaboración propia

A continuación, se describen diferentes casos de uso que pueden llevarse a cabo para recargar productos en diferentes condiciones.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Nombre del caso de uso	Solicitud de acción de renovación remota a través de la lista LAP_RP
Resumen	Una entidad solicita a su distribuidor de productos la renovación remota de un producto almacenado en el medio de pago de sus estudiantes, empleados o beneficiarios
Prerrequisitos	Emisión de medio de pago con perfil general o Emisión de medio de pago personalizado
Accionado por	Distribuidores de productos especiales
Actores	Distribuidores de productos Operadores de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Una entidad solicita a un distribuidor de productos la renovación remota de un producto almacenado en un medio de pago. Esta solicitud la realiza a través de un medio de comunicación no presencial. El distribuidor de productos hace la solicitud de la renovación remota a la Cámara de Compensación y esta lo redistribuye a los demás operadores. Luego de recibir la solicitud, todos los distribuidores de productos deben actualizar la lista LAP_RP en los dispositivos de recarga.

Figura 32. Eventos enviados durante la solicitud de acción de renovación remota a través de la lista LAP_RP



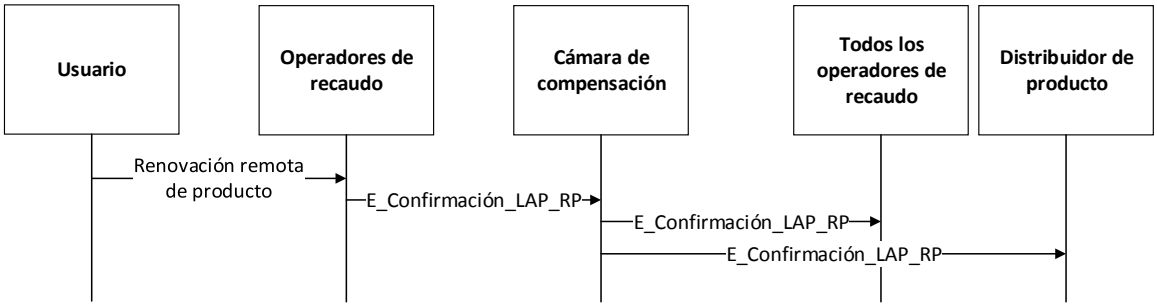
Fuente: elaboración propia

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Nombre del caso de uso	Ejecución de acción de renovación remota de producto general o especial con lista LAP_RP
Resumen	Un usuario lleva su medio de pago para redimir una renovación remota que una entidad ha registrado previamente.
Prerrequisitos	Solicitud de acción de renovación remota a través de la lista LAP_RP
Accionado por	Usuario
Actores	Distribuidores de productos Operadores de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago en un dispositivo de recarga y solicita la redención de su renovación. El distribuidor de productos realiza las siguientes acciones con dicho dispositivo: ▪ Verificación de la existencia de una acción de renovación remota disponible para el medio de pago y el producto presentado. ▪ Ejecución de la acción de renovación del producto general o especial en el medio de pago mediante escritura de datos. ▪ Almacenamiento del evento de ejecución de la acción con lista LAP_RP ▪ Envío de una confirmación del evento efectuado a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 33. Eventos enviados durante la ejecución de acción de renovación remota de producto general o especial con lista LAP_RP

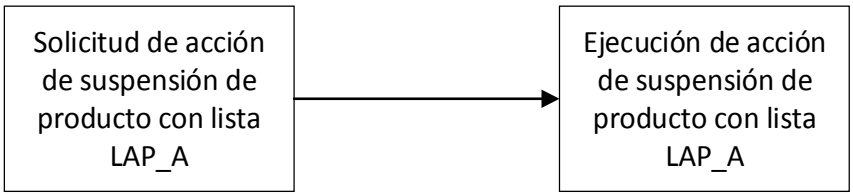


Fuente: elaboración propia

8.14 Suspensión de productos

La acción de suspensión de productos está compuesta por la siguiente secuencia de casos de uso que deben efectuar múltiples actores de la red interoperable.

Figura 34. Secuencia de casos de uso necesarios para la suspensión de productos



Fuente: elaboración propia

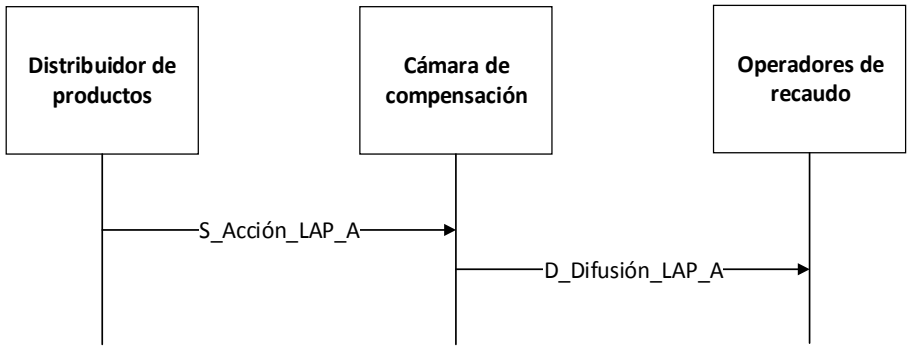
A continuación, se describen los dos casos de uso que se deben efectuar para lograr la suspensión de un producto.

Nombre del caso de uso	**Solicitud de acción de suspensión de producto con lista LAP_A**
Resumen	Un distribuidor de productos adquiere un motivo por el cual es necesaria la suspensión de un producto almacenado en un medio de pago
Prerrequisitos	Emisión de medio de pago con perfil anónimo o Emisión de medio de pago personalizado o Emisión de medio de pago personalizado con producto especial o Adquisición de un producto
Accionado por	Distribuidor de productos
Actores	Distribuidores de productos

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	Cámara de Compensación Operadores de recaudo
Descripción del caso de uso	El distribuidor de productos envía a los demás distribuidores y a la Cámara de Compensación un mensaje donde solicita la actualización de la lista LAP_A con una operación de suspensión de un producto almacenado en un medio de pago. Los operadores de recarga deben actualizar la lista LAP_A con este nuevo registro en todos los equipos de aceptación de medios de pago.

Figura 35. Eventos enviados durante la solicitud de acción de suspensión de producto con lista LAP_A



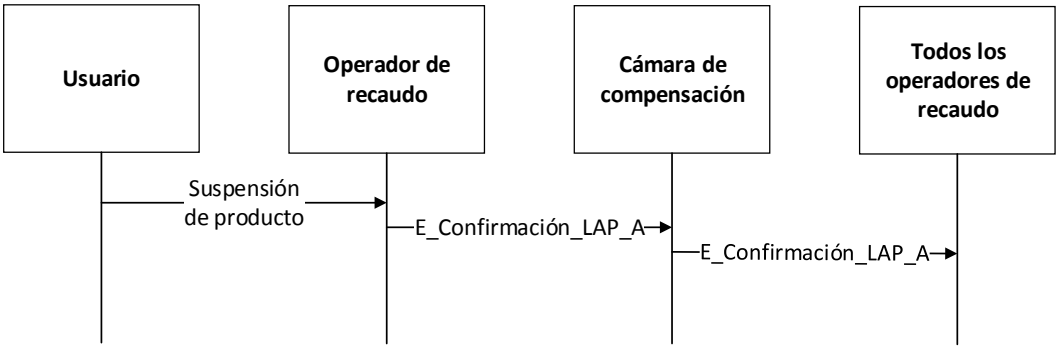
Fuente: elaboración propia

Nombre del caso de uso	**Ejecución de acción de suspensión de producto con lista LAP_A**
Resumen	Un usuario intenta acceder al sistema de transporte con un medio de pago al cual se le debe aplicar una acción de suspensión con la lista LAP_A
Prerrequisitos	Solicitud de acción de suspensión de producto con lista LAP_A
Accionado por	Usuario
Actores	Empresas Operadoras de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario intenta usar su medio de pago para acceder a la red interoperable acercándolo a un dispositivo de

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	aceptación de medios de pago. El Operador de recaudo del servicio al cual se le solicita el acceso realiza las siguientes acciones con dicho dispositivo: ▪ Verificación de la existencia de una acción disponible para el medio de pago presentado. ▪ Ejecución de la acción en el medio de pago mediante escritura de datos. ▪ Almacenamiento del evento de ejecución de la acción con lista LAP_A ▪ Envío de una confirmación del evento efectuado a la Cámara de Compensación. Todas las Empresas Prestadoras deben actualizar la lista LAP_A en los equipos de aceptación de medios de pago.

Figura 36. Eventos enviados durante la ejecución de acción de suspensión de producto con lista LAP_A



Fuente: elaboración propia

8.15 Reactivación de productos

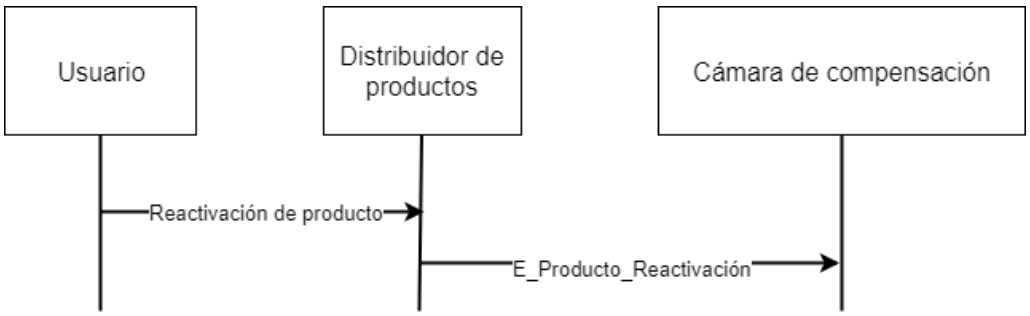
Dado un producto suspendido en un medio de pago, solo el distribuidor de productos que ha solicitado la suspensión está autorizado para reactivarlo. Este distribuidor de productos es responsable de definir los procesos necesarios para lograr la reactivación de un producto. Esto implica la toma de la decisión acerca de cuándo reactivarlo, informar al usuario la posibilidad de la reactivación e indicarle al usuario la fecha y la ubicación en donde puede reactivar el producto.

Nombre del caso de uso	**Reactivación de producto**
Resumen	Un producto que ha sido previamente suspendido por solicitud de un distribuidor de productos es reactivado por dicho distribuidor de productos.
Prerrequisitos	Ejecución de acción de suspensión de producto con lista LAP_A

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Accionado por	Usuario
Actores	Distribuidores de productos Cámara de Compensación Usuario
Descripción del caso de uso	El distribuidor de productos que ha suspendido un producto decide que se debe reactivar un producto que ha sido suspendido. El usuario propietario del medio de pago al cual se desea reactivar el producto se presenta ante el distribuidor de productos. El distribuidor de productos realiza las siguientes operaciones a través de un dispositivo de lector de medios de pago: ▪ Escritura de la información necesaria en el medio de pago para reactivar el producto. ▪ Almacenamiento de la información del evento en el dispositivo. ▪ Envío de la información del evento a la Cámara de Compensación.

Figura 37. Eventos enviados durante la reactivación de un producto



Fuente: elaboración propia

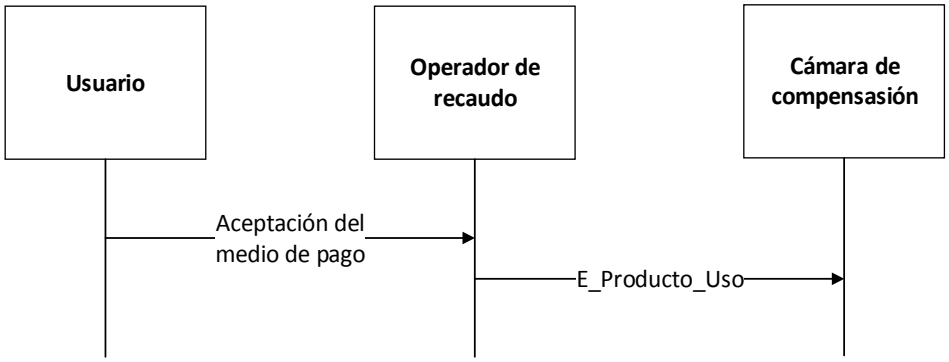
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

8.16 Aceptación del medio de pago recargable

Nombre del caso de uso	**Aceptación del medio de pago usando un producto**
Resumen	Un usuario acerca su medio de pago a un dispositivo de aceptación del medio de pago para acceder a un servicio de la red interoperable. Su medio de pago almacena uno o varios productos y este, o uno de estos, está disponible para uso. Dependiendo del perfil que tenga asociado el medio de pago, el producto especial debe tener un saldo mayor que cero.
Prerrequisitos	Emisión de medio de pago personalizado o Emisión de medio de pago anónimo o Adquisición de un producto
Accionado por	Usuario
Actores	Empresas Operadoras de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago con el producto disponible. El Operador de recaudo realiza las siguientes operaciones a través de un dispositivo de aceptación de medios de pago: ▪ Verificación de la validez del medio de pago y del producto disponible ▪ Cálculo de la tarifa y uso del producto ▪ Generación del registro de evento en el medio de pago. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 38. Eventos enviados durante la transacción de aceptación del medio de pago usando producto



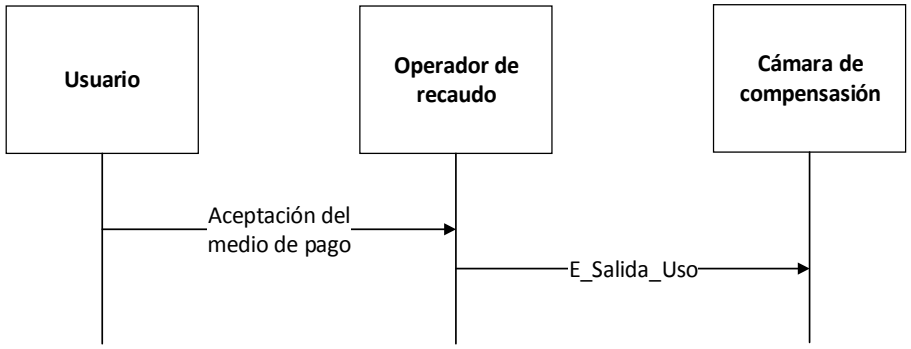
Fuente: elaboración propia

8.17 Aceptación de salida del medio de pago recargable

Nombre del caso de uso	Aceptación del medio de pago usando un producto
Resumen	Un usuario acerca su medio de pago a un dispositivo de aceptación del medio de pago para salir de las instalaciones de la red interoperable. Se verifica que el usuario entró legítimamente al sistema verificando la información almacenada en el medio
Prerrequisitos	Emisión de medio de pago personalizado o Emisión de medio de pago anónimo o Adquisición de un producto
Accionado por	Usuario
Actores	Operadores de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago con el que ingreso al sistema. El Operador de recaudo realiza las siguientes operaciones a través de un dispositivo de aceptación de medios de pago: ▪ Verificación de la validez del medio de pago y del procedimiento de entrada ▪ Generación del registro de evento en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 39. Eventos enviados durante la transacción de aceptación del medio de pago usando producto



Fuente: elaboración propia

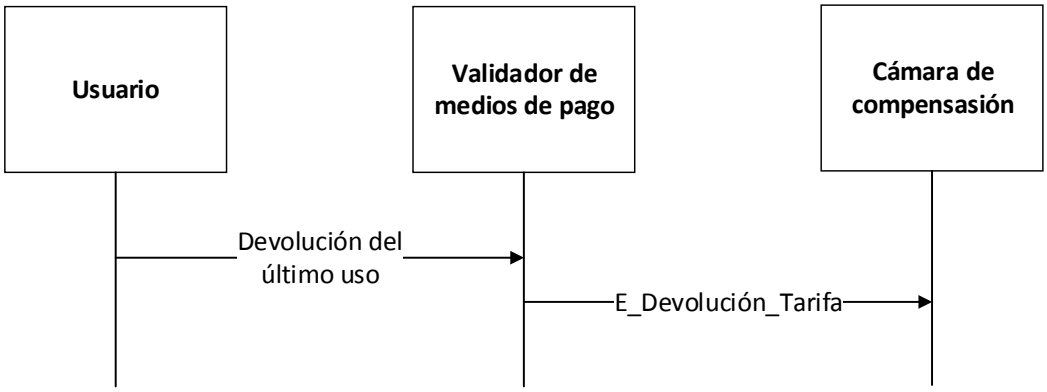
8.18 Devolución de la tarifa de la última transacción de aceptación del medio de pago recargable

Nombre del caso de uso	**Devolución de la tarifa de la última transacción de aceptación del medio de pago**
Resumen	Un usuario solicita la devolución de valor del último producto usado en una transacción de aceptación del medio de pago debido a que no fue posible la prestación del servicio.
Prerrequisitos	Aceptación del medio de pago usando el producto general exclusivamente o Aceptación del medio de pago usando un producto especial
Accionado por	Usuario
Actores	Operadoras de recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un Operador de recaudo realiza la devolución de la tarifa que ha pagado un usuario por medio del uso de uno o más productos en su medio de pago. El Operador de recaudo realiza las siguientes operaciones a través de un dispositivo lector de medios de pago autorizado para la devolución de valor: ▪ Verificación de la existencia previa de uno o varios eventos de uso de productos.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	▪ Generación de uno o más registros de los eventos de devolución en el medio de pago. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Figura 40. Eventos enviados durante la devolución de la tarifa



Fuente: elaboración propia

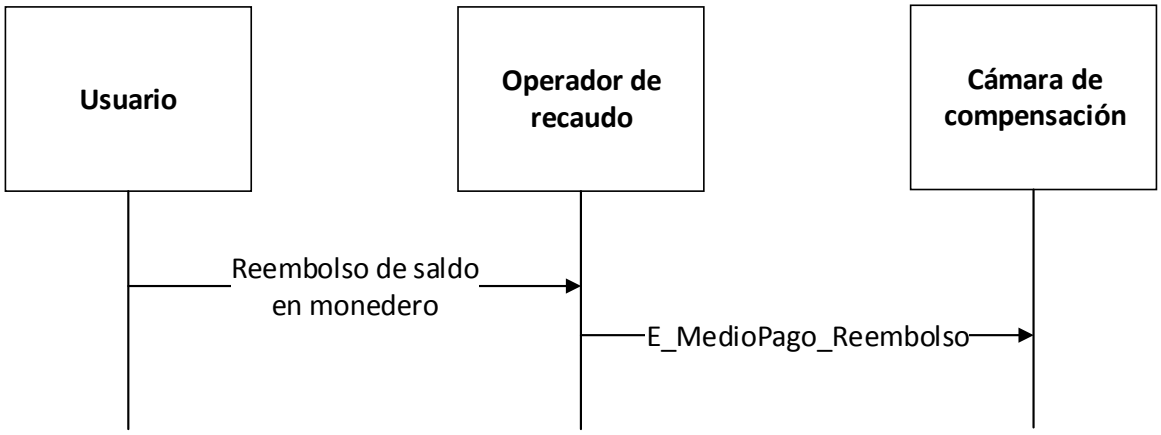
8.19 Reembolso de saldo en medio de pago recargable

Nombre del caso de uso	**Reembolso del saldo de un medio de pago recargable**
Resumen	Un usuario solicita el reembolso del saldo disponible en un medio de pago anónimo o personalizado.
Prerrequisitos	Emisión de un medio de pago anónimo o personalizado.
Accionado por	Usuario
Actores	Empresas Operadoras de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago recargable y solicita la devolución del saldo disponible. El Operador de recaudo realiza las siguientes operaciones a través de un dispositivo lector de medios de pago ▪ Débito de la totalidad del saldo en la aplicación monedero. ▪ Para medios de pago anónimos se deben borrar todos los eventos en el medio de pago y los contadores del archivo SERVICIOS. ▪ En caso de ser un medio de pago personalizado se debe escribir un evento de tipo reembolso en el medio de pago.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	▪ Envío de la información de eventos a la Cámara de Compensación.

Figura 41. Eventos enviados durante el uso de un medio de pago precargado



Fuente: elaboración propia

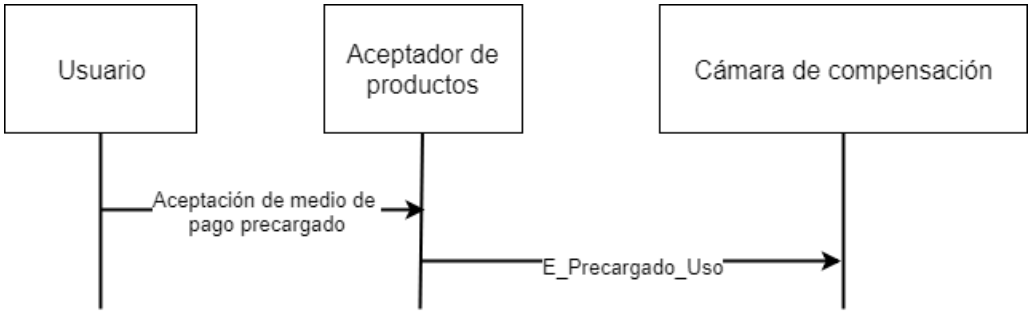
8.20 Aceptación del medio de pago no recargable

Nombre del caso de uso	**Uso de medio de pago precargado**
Resumen	Un usuario acerca su medio de pago precargado a un dispositivo de aceptación de medios de pago para acceder a un servicio de la red interoperable. El medio de pago precargado almacena suficiente saldo para pagar la tarifa.
Prerrequisitos	Emisión de medio de pago precargado
Accionado por	Usuario
Actores	Empresas Operadoras de Recaudo Cámara de Compensación Usuario
Descripción del caso de uso	Un usuario presenta su medio de pago precargado. El Operador de Recaudo realiza las siguientes operaciones a través de un dispositivo de aceptación ▪ Verificación de la validez del medio de pago. ▪ Cálculo de la tarifa y uso del medio de pago mediante la deducción del saldo equivalente a la tarifa.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	▪ Generación de los datos de evento en el medio de pago. ▪ Almacenamiento de la nueva información generada en el medio de pago. ▪ Envío de la información de eventos a la Cámara de Compensación.

Figura 42. Eventos enviados durante el uso de un medio de pago precargado



Fuente: elaboración propia

9 Protocolo de pruebas y certificación de equipos y sistemas

9.1 Introducción

A continuación, se describe el protocolo de pruebas y certificación de la especificación técnica. Su principal objetivo es establecer un proceso de certificación para las entidades participantes de la red interoperable. De esta forma, se busca garantizar la seguridad y escalabilidad de la norma técnica, de modo que cada uno de sus componentes permita la interoperabilidad. Para tal fin, es necesario contemplar la naturaleza jerárquica del sistema. Por este motivo, inicialmente se describe el alcance del protocolo de pruebas de acuerdo con los diferentes niveles de la red. Posteriormente se presentan cada uno de los requerimientos para la ejecución de las pruebas. Desde los ambientes por los que deben efectuarse cada uno de los escenarios de prueba, hasta los equipos que se deben utilizar y los informes que se deben generar antes y durante la ejecución. Enseguida, se procede a explicar en su totalidad el procedimiento que se debe efectuar por las entidades objeto de prueba. Después, se presenta una descripción general de la planeación y ejecución de las pruebas, previo a la presentación de los escenarios por actores. Finalmente, con el objetivo de guiar al ejecutor de las pruebas y demás lectores del presente documento, se describen una serie de instrucciones que permiten hacer un correcto uso de los escenarios de prueba y sus anexos. En esta sección se habla de una entidad certificadora. Esta entidad puede ser la Autoridad de Aplicación y Control o cualquier otro organismo que esta designe.

9.2 Alcance

En una red interoperable de transporte existen diversas interacciones entre los actores y elementos que lo componen. Sin embargo, solo algunas de estas son relevantes en el proceso de pruebas y certificación. El presente protocolo de pruebas se divide en tres

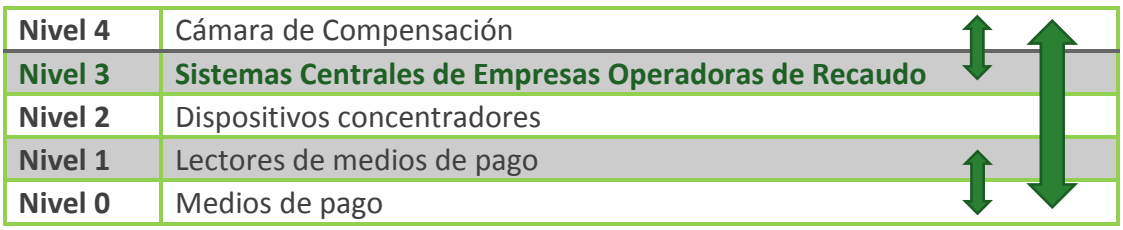
www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

subprocesos cada uno de los cuales está enfocado en interacciones entre dos diferentes niveles de la red.

- Subproceso 1: corresponde a las interacciones entre los primeros niveles de la red interoperable (0-1)
- Subproceso 2: corresponde a las interacciones entre los últimos niveles de la red interoperable (3-4)
- Subproceso 3: concierne al flujo de información entre los niveles 0 y 4.

El siguiente diagrama representa más claramente el alcance del protocolo:

Figura 43. Alcance del protocolo de pruebas



Fuente: elaboración propia

Para efectos de claridad, a continuación, se describen los tres subprocesos en mayor detalle.

9.2.1 Subproceso 1: medios de pago

En primera instancia, se deben garantizar las funcionalidades de los dispositivos de cada uno de los Operadores de Recaudo. Sin embargo, son limitadas las transacciones interoperables que pueden llevarse a cabo en las pruebas internas realizadas para cada entidad. Se requiere que el sistema esté ensamblado en su totalidad para poder efectuar acciones de *solicitud*. No obstante, existen casos de uso de medio de pago que deben probarse durante este subproceso. Por lo tanto, es imperativo que la información de acciones sobre medios de pago requerida sea creada y guardada localmente desde el sistema de respaldo de cada entidad, y no de forma interoperable. De esta forma es posible efectuar todos los casos de uso probables y evitar inconsistencias en el sistema.

Las pruebas que contemplan estas situaciones son presentadas en el Capítulo 9.5.1 del presente documento. Cabe aclarar que deberán ser certificadas aquellas que involucren exclusivamente los niveles 0 y 1 de la red. Por tal motivo, otro tipo de pruebas no serán contempladas en esta sección. Es decir que se debe verificar que las interacciones con los medios de pago se efectúen correctamente para cada uno de los actores de la red interoperable.

9.2.2 Subproceso 2: Comunicación entre actores

Es imperativo garantizar el flujo de información entre los últimos niveles de la red interoperable. Es decir que los actores deben validar la recepción y el envío de información desde y hacia la Cámara de Compensación. Estas entidades deben comunicarse por medio de intercambio de archivos generados por cada una. Así

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

mismo, la información debe ser creada y guardada en los sistemas de respaldo de cada entidad.

Este subproceso no requiere de interacción directa del medio de pago. Sin embargo, la información transferida debe ser consistente con los casos de uso del medio y por lo tanto debe ser de conformidad con lo establecido en la presente especificación técnica.

Las pruebas que contemplan la comunicación directa entre actores se encuentran en el Capítulo 9.5.2. Adicionalmente, cabe aclarar que estas pruebas son planteadas entre los niveles 3 y 4 de la red interoperable. Es decir, se contempla el envío de archivos desde un Operador de recaudo del Servicio hacia la Cámara de Compensación y desde la Cámara hacia las demás Empresas Operadoras de Recaudo.

9.2.3 Subproceso 3: Operación integral de la red interoperable

Finalmente, se debe asegurar una correcta operación del sistema integrado en su totalidad. Esto con la participación de todos los actores, incluyendo a los usuarios de medios de pago. Sin embargo, este subproceso debe ejecutarse posterior a la exitosa ejecución de los anteriores subprocesos. Una vez se tengan las garantías necesarias de que los otros niveles de la red funcionan de acuerdo con lo establecido en este documento es posible poner en marcha el sistema.

Con el propósito de reducir la complejidad durante el proceso se verificarán exclusivamente las transacciones llevadas a cabo en los niveles 0 y 4 (interacción con medio de pago y transferencia de archivos entre Empresas Operadoras de Recaudo y Cámara de Compensación). El Capítulo 9.5.3 presenta en detalle las pruebas para la operación total del sistema.

Adicional a estos subprocesos que delimitan el alcance por niveles de la red es necesario identificar a los actores objeto de certificación.

9.2.4 Roles del proceso de certificación

El presente protocolo de pruebas busca certificar exclusivamente a los encargados de: emitir medios de pago, distribuir y recargar productos y aceptar medios de pago. Para el caso particular del SIR del SITM-Q, estos tres roles son ejecutados por las Empresas Operadoras de Recaudo, por lo que el conjunto de pruebas expuesto aquí será usado para la certificación de estas Empresas.

Todos los aspectos presentados a lo largo de este documento, a excepción de los escenarios de prueba, deben ser tenidos en cuenta para la certificación de todas las entidades que participen en el SITM-Q. Una explicación más detallada de la asignación de casos de pruebas para las Empresas Operadoras de Recaudo se presenta en el Capítulo 9.6.1.

Una vez definidos los subprocesos y las entidades participantes del proceso de pruebas, la entidad certificadora debe tener en cuenta los requerimientos para la ejecución de las mismas. De esta forma se reduce el margen de error durante la implementación. A continuación, se describen cada uno de los requerimientos.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

9.3 Requerimientos de pruebas

9.3.1 Ambientes de prueba

El proceso de pruebas y certificación debe pasar por diferentes estados con el fin de garantizar la calidad, no exclusivamente de la red interoperable, sino también de las mismas pruebas. Enseguida se describen los ambientes de prueba en el orden en el que deben ser implementados. Cabe aclarar que los ambientes de prueba son secuenciales. Es decir que únicamente serán iniciadas las pruebas en el siguiente ambiente si todas las pruebas del anterior se han ejecutado y cumplido de acuerdo con los resultados esperados.

2.1.1.5. Pruebas en ambiente de prueba controlado

Un ambiente controlado se define como aquel que implementa el mismo software y hardware que se espera implementar en producción. Por esta razón, los equipos que se usen para estas pruebas deberán ser los mismos que se vayan a implementar en producción y la versión del software deberá ser la misma que se espera desplegar en producción. El objetivo de realizar pruebas sobre un ambiente de prueba controlado es la detección temprana de fallos y la verificación de la integración de hardware y software. Durante esta fase la entidad certificadora realizará las pruebas para cada entidad participante.

Durante el desarrollo de pruebas de los escenarios en el ambiente de prueba, no se usará la red de comunicación para *solicitud* de actualización de listas de acción. En este caso las entidades acordaran el uso de un sistema para el envío de los datos (portal web, correos electrónicos, otros), de forma que se garantice una transmisión controlada de la información.

Las pruebas de niveles 0 y 1 se efectuarán con medios de pago que cumplan con las características de la red interoperable. Igualmente, los equipos lectores de medios estarán completamente configurados. Como en esta etapa no es necesaria la interconexión entre actores, solo se probarán los subprocesos 1 y 2.

2.1.1.6. Pruebas de QA

El siguiente ambiente corresponde al de pruebas de Garantía de calidad (QA por sus siglas en inglés Quality Assurance), y tiene la principal característica de que los datos no se manejan de forma controlada. Es decir que busca garantizar las actualizaciones de los datos, el software y el hardware utilizado de manera que cumplan con las expectativas de la red interoperable. Esto bajo un ambiente con condiciones similares a las de la operación final del sistema integrado.

Las pruebas de los últimos niveles, se llevan a cabo durante esta fase del proceso de pruebas usando una red de comunicación con garantía de calidad. De forma que se asegure el flujo de información entre los últimos actores de la red interoperable. De lo contrario una inconsistencia en las pruebas podría deberse a fallas en la red, situación que afectaría directamente el proceso de certificación de las entidades. La

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

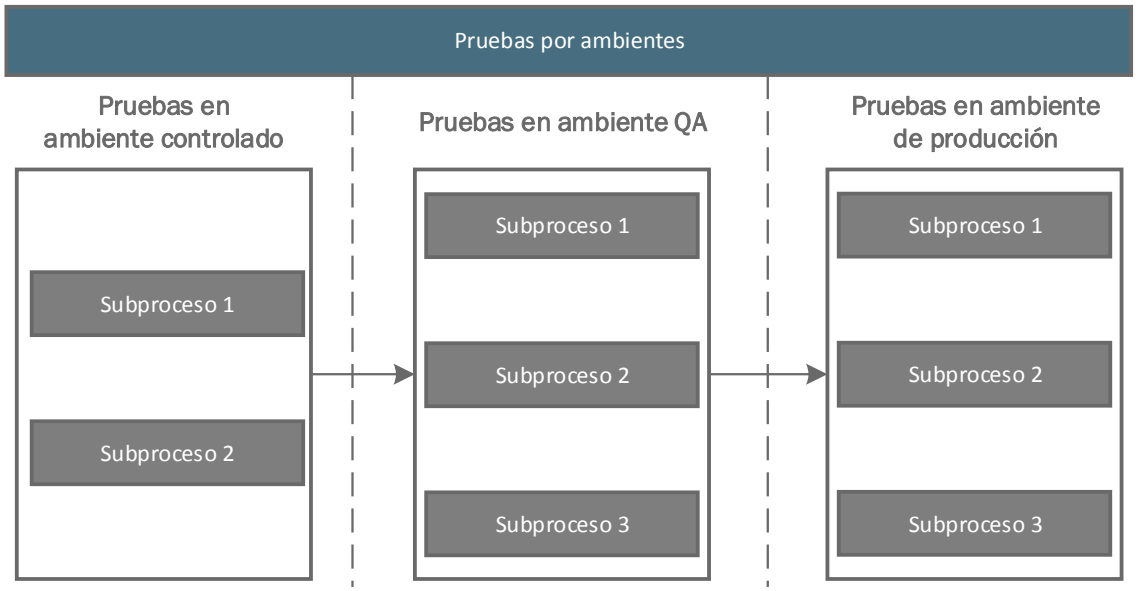
configuración de la red, así como su proceso de certificación no hacen parte del alcance del presente protocolo.

2.1.1.7. Pruebas en ambiente de producción

Una vez se ratifiquen las pruebas en los anteriores ambientes, se procede a realizar nuevamente todos los escenarios en un ambiente de producción. Este ambiente no difiere en gran medida del anterior. Los cambios radican en la configuración especial de los equipos, así como los permisos de acceso como llaves de entidades. Durante esta fase de prueba el sistema debe probarse con las modificaciones finales que serán utilizadas durante su implementación definitiva. Por lo tanto, para la ejecución de las pruebas durante este ambiente se requiere efectuar una ceremonia para la creación y definición de las llaves de producción, así como identificadores de dispositivos y entidades. Esta etapa de pruebas corresponde a un piloto que se debe realizar durante un periodo de tiempo previo a la salida masiva a producción.

La Figura 44 resume la relación entre los ambientes de prueba con cada uno de los tipos de escenarios planteados en el presente documento.

Figura 44. Escenarios de pruebas por ambientes



Fuente: elaboración propia

9.3.2 Equipos de prueba

El proceso de certificación requiere que las entidades de la red hagan uso de equipos con las características requeridas para el sistema, es decir los equipos deberán ser los mismos que se implementen en producción. El software de dichos equipos tuvo que haber sido previamente desarrollado y los equipos configurados por el proveedor de tecnología o el Operador de Recaudo a certificar. La fase de pruebas durante el desarrollo de software será responsabilidad de cada entidad y no será contemplada en el presente protocolo.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

2.1.1.8. Equipos de prueba para ambiente de prueba controlado:

- Medios de pago recargables
- Medios de pago no recargables
- Lectores de medios de pago
- SAMs de prueba (Usar TEST-SAM-F5 de Calypso)
- Dispositivos de venta, recarga y aceptación de medios de pago
- Equipos de respaldo de información
- Datos de prueba (ver Capítulo 9.6.2)
- Elementos para efectuar pagos (dinero en efectivo)

2.1.1.9. Equipos de prueba para ambiente QA

- Medios de pago recargables
- Medios de pago no recargables
- Lectores de medios de pago
- SAMs de prueba (Usar TEST-SAM-F5 de Calypso)
- Dispositivos de venta, recarga y aceptación de medios de pago
- Equipos de respaldo de información
- Red de comunicación configurada con garantía de calidad para el soporte de listas de acción y flujo de información (Red de comunicación entre Empresas Operadoras de Recaudo y la Cámara de Compensación)
- Datos de prueba (ver Capítulo 9.6.2)
- Elementos para efectuar pagos (dinero en efectivo)

2.1.1.10. Equipos de prueba en ambiente de producción

- Medios de pago recargables
- Medios de pago no recargables
- Lectores de medios de pago
- SAMs de producción (SAM Maestro y SAMs de producción con llaves de producción)
- Dispositivos de venta, recarga y aceptación de medios de pago
- Equipos de respaldo de información
- Red de comunicación configurada con garantía de calidad para el soporte de listas de acción y flujo de información (Red de comunicación entre Empresas Operadoras de Recaudo y la Cámara de Compensación)
- Datos definitivos de producción (ver Capítulo 9.6.2)
- Elementos para efectuar pagos (dinero en efectivo)

9.3.3 Informes de prueba

2.1.1.11. Plan de pruebas

Previo a la realización de los casos de prueba, se deberá documentar un plan de pruebas. En dicho plan se describen el alcance, las características, el cronograma de actividades, entre otros. Deberá existir uno por cada ambiente de pruebas y subprocesos. Este será un prerrequisito fundamental para la ejecución del protocolo. A continuación, se presenta un modelo de la tabla de contenido del documento:

Contenido	Comentarios
Identificador del plan de pruebas	Identificador único del plan
Introducción	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Elementos del test	Hardware y software
Características de la red interoperable a ser probadas	Descripción de objetivos de pruebas. Identificar subproceso a ejecutar
Características de la red interoperable que no serán probadas	En caso de ser necesario
Actividades de prueba	Actividades a efectuar durante ejecución
Ambiente de prueba	Descripción detallada de los requerimientos y el montaje del ambiente de pruebas
Responsabilidades	
Personal requerido	Adicionar necesidades de entrenamiento en caso de ser necesario
Cronograma de ejecución de pruebas	
Riesgos y contingencias	Situaciones críticas a tener en cuenta
Aprobaciones	Firmas

2.1.1.12. Reporte de casos de pruebas en ambientes

Se debe generar un plan de ejecución de las pruebas para cada uno de los ambientes que deberán ser probados. Igualmente, se debe crear un reporte por ambiente. Al final de la ejecución de todos los subprocesos se obtendrá un reporte final que contendrá toda la información relevante de todos los casos de prueba. A continuación, se presentan los requerimientos que debe tener el reporte de pruebas.

- Identificadores de los escenarios a ejecutar
- Descripción de los escenarios
- Versiones de documentos de pruebas y actualización de equipos
- Resultados obtenidos durante la ejecución de casos de pruebas
- Discrepancias con los resultados esperados
- Contenido esperado y obtenido del medio de pago antes y después de prueba (exclusivamente para escenarios de prueba del subproceso 1 y del 2)
- Contenido esperado y obtenido de archivos enviados y recibidos entre entidades (exclusivamente para escenarios subproceso 2 y del 3)
- Firmas de aprobación

2.1.1.13. Reporte de fallas

Todos los problemas y comportamientos no esperados durante la ejecución deben ser reportados en documentos diferentes al plan y reporte de pruebas. Con el objetivo de identificar correctamente la fuente del problema, es necesario que el reporte sea bastante detallado y específico con respecto a los diferentes factores que pueden

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

influir en el comportamiento de los equipos. Enseguida se presenta un modelo del contenido del reporte de fallas:

Campo	Descripción
Componente	Dispositivo en el que ocurre la falla
Versión	Versión de actualización de equipos y protocolo de pruebas
Severidad	Importancia de la falla
Estado Inicial	Descripción del procedimiento previo a la realización de la falla
Asignado a	Responsable del dispositivo donde ocurre la falla
Funcionalidad	Debe indiciarse en caso de ser posible la funcionalidad a la que concierne la falla
Resumen	Descripción corta de la falla
Descripción	Descripción detallada con toda la información asociada al evento de falla. Debe incluir escenario de prueba específico, pasos ejecutados, productos usados, dispositivos utilizados, contenidos inesperados en el medio de pago, entre otros

9.4 Proceso de certificación

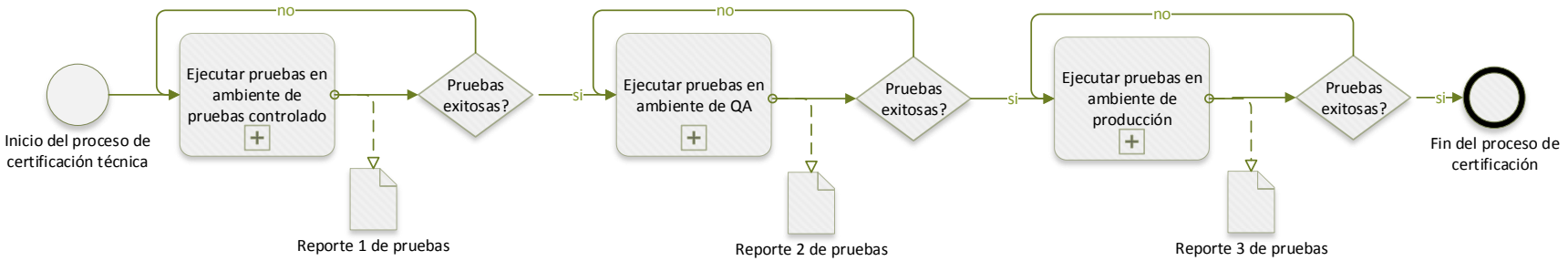
El proceso de certificación técnica que debe seguir cada Operador de Recaudo con el fin de autorizar su participación en la red interoperable es presentado en las gráficas de la presente sección.

La Figura 45 presenta el proceso de certificación técnica en el cual las Empresas Operadoras de Recaudo deben ejecutar pruebas en: Ambiente Controlado, Ambiente de QA y Ambiente de Producción. Si se presentan errores en las pruebas al ejecutar una etapa, el proceso debe reiniciarse, esto con el fin de garantizar que se manejen versiones homogéneas de hardware y software en todas las pruebas realizadas en un mismo ambiente. De igual manera, en cada ambiente deben ejecutarse las pruebas de los subprocesos que correspondan.

El proceso para la ejecución de pruebas en cada ambiente se muestra en la Figura 46. De acuerdo a esta, las pruebas de los subprocesos 1 y 2 se pueden hacer de forma simultánea. Si es necesario el despliegue de una nueva versión de software o hardware debido a un cambio que se hizo para corregir un error en algún caso de prueba, se deben repetir todas las pruebas para un subproceso. Así mismo, solo se podrá avanzar a las pruebas del subproceso 3 si las pruebas del subproceso 1 y 2 fueron exitosas en su totalidad. Una prueba de un subproceso es exitosa si y solo si todos los escenarios de prueba se ejecutaron de manera adecuada y arrojaron los resultados esperados.

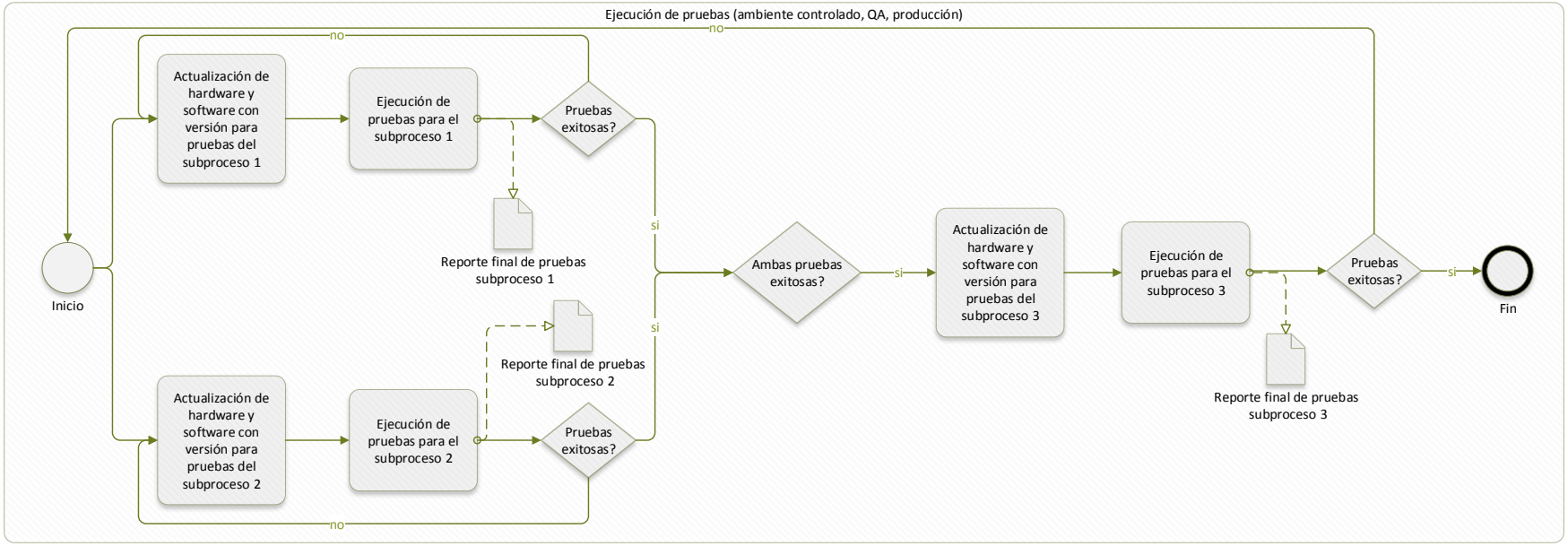
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 45. Proceso de certificación de actores en la red interoperable



Fuente: elaboración propia

Figura 46. Expansión de cada etapa de pruebas (ambiente de pruebas controlado, QA y producción)



Fuente: elaboración propia

9.4.1 Instrucciones

Para cada fase, las Empresas Operadoras de Recaudo deberán seguir las instrucciones presentadas a continuación:

1. Comprobar las pruebas de calidad de fábrica (FAT por sus siglas en inglés Factory Acceptance Test) y de sitio (SAT por sus siglas en inglés Site Acceptance Test) ejecutadas por los proveedores de equipos.
2. Proveer los equipos necesarios a la entidad certificadora
3. Generar un plan para el desarrollo de las pruebas (ver Capítulo 9.3.1)
4. Implementar el respectivo ambiente de prueba

Por otra parte, el Registrador deberá entregar a la entidad certificadora los datos necesarios para la ejecución de las pruebas (ver Capítulo 9.6.2). Con esta información la entidad certificadora procederá a seguir las siguientes instrucciones en el orden en el que son presentadas:

1. Configurar equipos de acuerdo con el ambiente de prueba y a los datos recibidos por el Registrador, con el soporte del Operador de Recaudo.
2. Ejecutar los casos de prueba
3. Documentar en reportes todos los datos de la prueba
4. Para casos de prueba del subproceso 1, donde se ejecuten transacciones y por tanto exista flujo de información, documentar el mapa del medio de pago antes y después de la prueba. De igual forma, documentar la información enviada y recibida en el dispositivo lector de medios de pago (venta, recarga, aceptación de medios de pago). Un dispositivo propiedad de la entidad certificadora, será el encargado de verificar los datos.
5. Aprobar pruebas y certificar con firma de analista en caso de que se obtengan todos los resultados esperados.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

9.5 Pruebas de certificación por subprocesos

Los escenarios de pruebas del presente protocolo se plantean basándose en los subprocesos presentados en el Capítulo 9.2. Esto teniendo en cuenta que corresponden a interacciones entre diferentes niveles de la red. Por lo tanto, requieren de hardware y software diferentes. Adicionalmente, dichos escenarios son genéricos y aplican a diferentes combinaciones de equipos. Esta sección tiene como propósito explicar los objetivos de cada uno de los tipos de escenarios, la forma en la que fueron planteados y sus implicaciones, así como los detalles a tener en cuenta en el momento de ejecutarlos.

9.5.1 Pruebas de subproceso 1

Las pruebas de niveles 0 y 1 tienen el objetivo de garantizar una correcta interacción entre los medios de pago interoperables y los dispositivos lectores. Por tal motivo, tanto la experiencia del usuario del sistema interoperable, como la información recibida por los dispositivos con los cuales interactúa el medio dentro de la red resultan ser fundamentales. Es así como cada prueba se contempla dentro de un modo de uso del medio de pago, a partir del cual se evalúan las situaciones que se derivan del mismo. Todos los cambios en el medio de pago son enviados y guardados en los dispositivos de aceptación de medios.

Enseguida se presenta una asignación entre el tipo de evento llevado a cabo durante la ejecución de un caso de uso del medio de pago y los archivos que cambian en el mismo. Por lo tanto, aplica para todos los casos de uso de los niveles 0 y 1.

Los archivos o campos que cambian de acuerdo con la siguiente tabla, deberán ser verificados por la entidad certificadora con el fin de garantizar que no existen errores durante la ejecución de los casos. Algunos escenarios planteados generan varios eventos. Por este motivo en los Capítulos 10.1.1, 10.2.1 y 10.3 se presentan los cambios teniendo en cuenta todos los eventos ocurridos.

NO	Evento	Cambios en medio de pago
1	E_MedioPago_Emisión	ENTORNO
		ESTADO_APLICACION
		EVENTOS
2	E_MedioPago_ModUsuario	USUARIO / FUNCIONARIO
3	E_Producto_Distribución(Producto)	LISTA_CONTRATOS
		EVENTOS
		SERVICIOS(Producto)
		CONTRATOS(Producto)
4	E_Producto_Recarga	EVENTO

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

NO	Evento	Cambios en medio de pago
		Valor(Producto)
5	E_Producto_Devolución_Recarga	EVENTO
		Valor(Producto)
6	E_Producto_Uso	EVENTOS
		SERVICIOS(Producto)
		Valor(Producto)
7	E_Producto_Devolución_Tarifa	EVENTOS
		SERVICIOS(Producto)
8	E_Precargado_Emisión	IdEmisor
		FechaEmisiónTarjeta
		FechaFinValidezTarjeta
		VersiónAplicación
		IdRed
9	E_Precargado_Uso	IdEntidad
		FechaHoraEvento
		TipoEvento
		MontoEvento
		IdSAM
		ConsecutivoSAM
		IdDispositivo
		IdRuta
		IdRutaEstación
10	E_MedioPago_Reconstrucción	ENTORNO
		USUARIO
		ESTADO_APLICACION
		LISTA_CONTRATOS
		EVENTOS
		CONTRATOS(Todos los Productos)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

NO	Evento	Cambios en medio de pago
		SERVICIOS(Todos los Productos)
		Valor(Todos los Productos)
11	E_Confirmación_LAM	ESTADO_APLICACION
12	E_Confirmación_LAP_A	EVENTOS
		SERVICIOS(Todos los Productos)
13	E_Confirmación_LAP_R	EVENTOS
		Valor(Producto)
14	R_Evento_No_Efectuado	---

9.5.2 Pruebas de subproceso 2

Como se mostró en la sección 5.15.1, existe un flujo de información entre el nivel 3 y 4 de la red interoperable. Las pruebas del subproceso 2 tienen el objetivo de comprobar el formato y contenido de los archivos que deben enviar las Empresas Operadoras de Recaudo cuando se generan eventos en los medios de pago, es decir, los casos de uso mostrados en el capítulo 8.

La información es enviada entre entidades en concordancia con el anexo [26] y deberá ser verificada con el fin de garantizar la interoperabilidad del sistema. El intercambio de información entre entidades o Empresas Prestadoras de Servicio se hace por medio del nivel 4, que es donde se centraliza la información de la red interoperable.

El objetivo de estas pruebas es garantizar una correcta generación de los archivos y una verificación de estos cuando son recibidos por el destino final. Un archivo contiene la información correspondiente a todos los casos de usos del medio de pago efectuados en los sistemas centrales. A cada caso de uso se le asocia uno o más eventos dependiendo del tipo al que pertenezca. Dada la información proveída por el Registrador se procede a efectuar las pruebas correspondientes. El objetivo es generar los archivos XML en concordancia con la información suministrada.

Un Operador de Recaudo envía información a la Cámara de Compensación, quien, de ser necesario, distribuye la información a los demás operadores de recargo. La información está asociada a los tres roles que desempeña el Operador de Recaudo: emisión, distribución y aceptación de medios de pago. A continuación, se presenta una asignación entre los casos de uso y los tipos de eventos que se generan, los cuales siempre son enviados desde un Operador de Recaudo hacia la Cámara de Compensación y a las demás Empresas Operadoras de Recaudo.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Caso de uso	Eventos
Emisión de medio de pago recargable	E_MedioPago_Emisión E_Producto_Distribución (para cada producto distribuido) E_Producto_Recarga (para cada producto distribuido)
Emisión de medio de pago no recargable	E_Precargado_Emisión
Personalización posventa del medio de pago recargable	E_MedioPago_Mod_Usuario E_Producto_Distribución (Opcional) E_Producto_Recarga (Opcional) E_Confirmación_LAP_A (Suspensión) (Opcional)
Reconstrucción del medio de pago	E_MedioPago_Reconstrucción
Bloqueo o desactivación del medio de pago (Solicitud)	S_Acción_LAM
Bloqueo o desactivación del medio de pago (Ejecución)	E_Confirmación_LAM (Bloqueo o desactivación)
Desbloqueo del medio de pago (Solicitud)	S_Acción_LAM
Desbloqueo del medio de pago (Ejecución)	E_Confirmación_LAM (Desbloqueo)
Adquisición de un producto posventa	E_Producto_Distribución
Renovación de un producto	E_Producto_Distribución (Renovación)
Recarga de un producto	E_Producto_Recarga
Devolución del monto de la última recarga	E_Producto_Devolución_Recarga

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Recarga remota de productos a través de la lista LAP_R (Solicitud)	S_Acción_LAP_R
Recarga remota de productos a través de la lista LAP_R (Ejecución)	E_Confirmación_LAP_R E_Producto_Recarga
Suspensión de productos (Solicitud)	S_Acción_LAP_A
Suspensión de productos (Ejecución)	E_Confirmación_LAP_A
Reactivación de productos	E_Producto_Reactivación
Aceptación del medio de pago recargable	E_Producto_Uso
Devolución de la tarifa de la última transacción de aceptación del medio de pago	E_Producto_Devolución_Tarifa
Aceptación del medio de pago precargado	E_Precargado_Uso

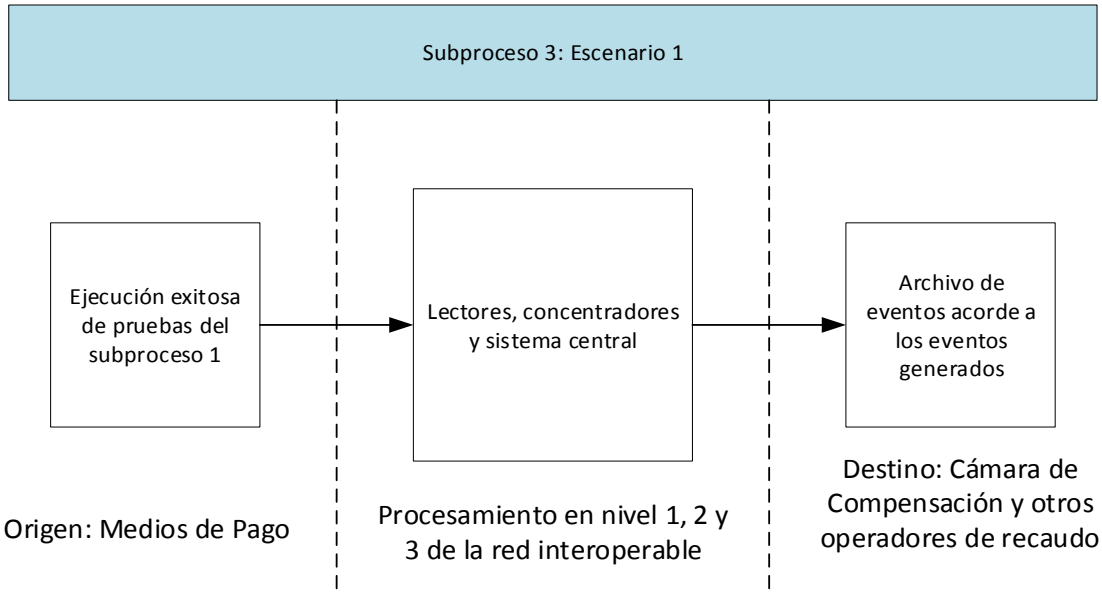
9.5.3 Pruebas del subproceso 3

Posterior a la realización de las anteriores pruebas se procede a probar el sistema en su totalidad. Cabe aclarar, que esto debe ocurrir siempre y cuando se hayan obtenido todos los resultados esperados durante todos los escenarios probados. De esta forma, el flujo de información entre dos de los puntos críticos de la red se encuentra verificado.

Las siguientes figuras indican cómo fueron planteados los dos escenarios que un Operador de Recaudo debe aprobar. Como se mencionó anteriormente en el presente documento estos escenarios no requieren de verificación de información en puntos intermedios de la red. Es decir que la información se verifica directamente en los puntos destino del flujo de información.

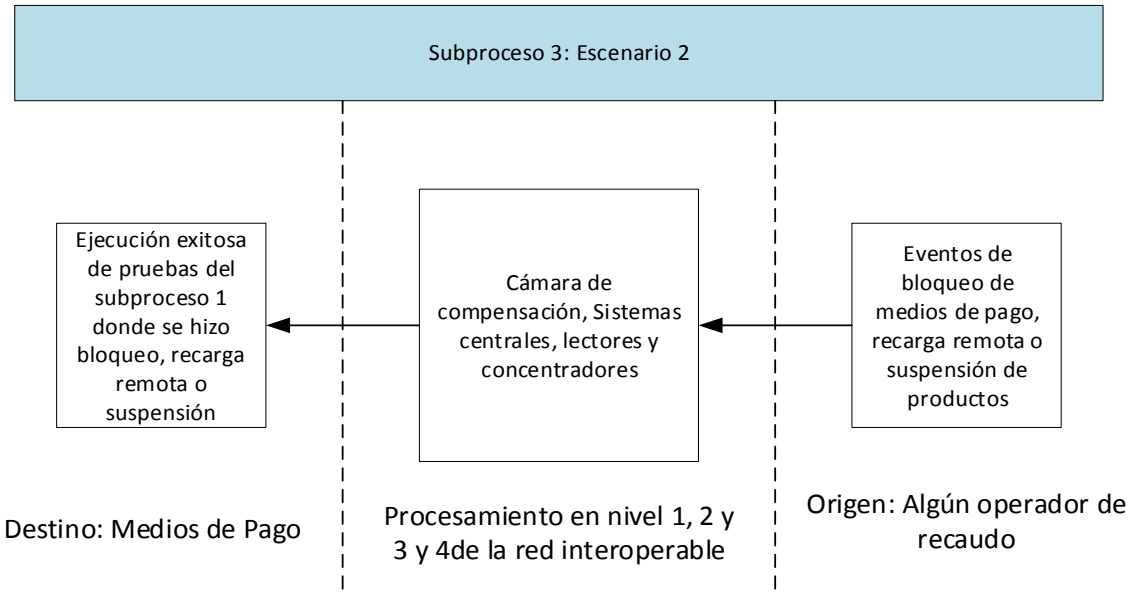
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Figura 47. Escenario 1 para pruebas de subproceso 3



Fuente: elaboración propia

Figura 48. Escenario 2 para pruebas de subproceso 3



Fuente: elaboración propia

Adicionalmente, es necesario garantizar la correcta validación de los módulos SAM de los dispositivos lectores con el módulo HSM de cada sistema central, así como verificar el aumento efectivo de los valores máximos de los contadores de los módulos SAM de recarga, según se describe en la sección 6.4 de este documento.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

9.6 Instrucciones de uso de los escenarios de prueba y sus anexos

El protocolo de pruebas contiene tres anexos que tienen como objetivo principal ejemplificar algunas situaciones planteadas, así como presentar información relevante para el proceso de certificación. Es así como el anexo 6 [27] por ejemplo, contiene tablas para ejecución de pruebas y formatos que las entidades deben completar. Esta sección pretende guiar al certificador en la ejecución de los casos de prueba, de manera que este pueda hacer un correcto uso de los anexos. Es decir, que esta sección está enfocada exclusivamente en los escenarios de pruebas presentados en los próximos capítulos.

Cada uno de los escenarios de prueba planteados utiliza el siguiente formato sin importar el tipo de subproceso al que pertenezca:

ID_Prueba	Identificador único de la prueba
Propósito	Motivación para la realización de la prueba
Configuración	Elementos necesarios para realizar ejecutar el caso de prueba
Condiciones previas	Condiciones que debe tener el sistema antes de la realización de las pruebas
Acciones del test	Pasos a seguir para realizar la prueba
Resultados	Resultados esperados
Observaciones	Comentarios adicionales de relevancia para el entendimiento y aplicación de la prueba.

9.6.1 Asignación de escenarios de prueba

Los operadores de recaudo deberán ser certificados teniendo en cuenta los 3 roles que cumplen: emisión, distribución y aceptación de medios de pago. Es por este motivo que los escenarios de prueba se encuentran divididos en estas categorías.

La siguiente tabla presenta una asignación de los escenarios de prueba del subproceso 1 de acuerdo con el rol ejecutado por el Operador de Recaudo. Todos los casos del subproceso 1 tienen un identificador único de prueba que inicia en 1. Con el objetivo de facilitar la compresión de la asignación de los casos, el siguiente número del identificador corresponde con la numeración en la tabla. Por ejemplo, todos los identificadores de los casos de emisión de medios de pago inician en 1.1. Por otra parte, los identificadores de los casos de aceptación de medios de pago inician en 1.15. Adicionalmente, se definen casos y situaciones particulares de prueba para cada escenario de prueba. Se utiliza un identificador ordenado tanto para los casos como

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

para las pruebas. Por ejemplo, los identificadores del caso emisión de medios de pago personalizados inicia con 1.1.2, y la situación 2 para el mismo caso tiene identificador 1.1.2.2.

Rol	Tipo de escenario de prueba
Emisor de medios de pago	1. Emisión de medio de pago recargable
	2. Emisión de medio de pago no recargable
	3. Personalización posventa
	4. Reconstrucción del medio de pago
	5. Bloqueo o desactivación del medio de pago
	6. Desactivación del medio de pago
	7. Desbloqueo del medio de pago
	8. Adquisición de un producto posventa
	9. Renovación de un producto
	10. Recarga de un producto
Distribuidor de productos	11. Devolución del monto de la última recarga
	12. Recarga remota de productos a través de la lista LAP_R
	13. Suspensión de productos
	14. Reactivación de productos
	15. Aceptación del medio de pago recargable
	16. Devolución de la tarifa
Aceptador de medios de pago	17. Suspensión de productos (Ejecución)
	18. Bloqueo del medio de pago (Ejecución)
	19. Desbloqueo del medio de pago (Ejecución)
	20. Desactivación del medio de pago (Ejecución)

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Los identificadores de prueba del subproceso 2 inician en 2. Teniendo en cuenta que se tiene un máximo de dos casos de prueba por rol para el subproceso 2 del protocolo, se establece que el siguiente número del identificador corresponda con el rol. Es decir que los escenarios del subproceso 2 para emisión de medios de pago inician en 2.1, para distribución de productos en 2.2 y para aceptación de medios de pago en 2.3. Esta misma situación aplica con los escenarios del subproceso 3, con la diferencia de que el identificador inicia en 3. Es decir 3.1, 3.2 y 3.3 para emisión, distribución y aceptación de medios de pago respectivamente.

9.6.2 Manual de uso del documento de formatos para ejecución de pruebas

Previo a la ejecución de los casos de prueba para los ambientes de prueba y QA, la entidad certificadora debe tener acceso a la información de prueba del Registrador. Igualmente, para la ejecución en ambientes de producción es requerida la información de producción. La sección 7 de estas especificaciones expone en detalle cada uno de los datos relevantes en la red interoperable. En el anexo 6 [27] hoja ***Formatos Registrador*** se presenta un formato más detallado que debe entregar el Registrador a la entidad certificadora. Para el caso de identificador de dispositivos se debe utilizar un formato como el que se presenta en el mismo anexo hoja ***Formatos Registrador-dispositivos***. Esta información permite constatar que los datos guardados tanto en los medios de pago, como en los dispositivos aceptadores y en los archivos que serán enviados entre entidades; corresponden con las acciones efectuadas con el medio de pago.

Adicional a esta información, la entidad certificadora debe considerar los datos dependientes del entorno, tales como fechas exactas de creación de eventos. Teniendo en consideración estos dos tipos de datos es posible comparar el mapa del medio de pago antes y después de la generación de los eventos. Como se mencionó anteriormente, la entidad certificadora deberá contar con su propio dispositivo que comprobará los cambios en los archivos del medio.

Por otra parte, para las pruebas que se lleven a cabo en un ambiente de prueba controlado o en el ambiente de QA, se deben utilizar llaves de prueba del SAM-TEST-F5 v6 de Calypso, se deben utilizar las llaves de prueba descritas en el anexo 6 [27] en la hoja ***Llaves de prueba***. Para las pruebas en ambiente de producción se deben haber emitido todos los tipos de SAM de la red en una ceremonia de llaves según las especificaciones Calypso, i.e., se deben utilizar llaves de producción.

9.6.3 Manual de uso del documento de estructura de archivos del medio de pago interoperable durante ejecución de pruebas del subproceso 1

Los escenarios de prueba de los primeros niveles de la red serán descritos a partir de la sección 10. Sin embargo, una descripción detallada de estos se encuentra en el anexo

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

7 [28] En él se podrán identificar ejemplos de uso de cada uno de los casos de prueba, en donde se podrá visualizar con claridad los cambios en los archivos de la aplicación de acuerdo con el tipo de prueba aplicada. A continuación, se presenta una serie de aclaraciones sobre el mismo:

- El anexo se compone de 3 documentos de hojas de cálculo. Cada documento corresponde a uno de los roles anteriormente definidos: emisión, distribución y recarga, y aceptación.
- Cada uno de los archivos consiste en una serie de hojas en las cuales se ejemplifican los escenarios de prueba. Las hojas están identificadas con el ID del escenario de prueba que representan.
- Cada una de las hojas muestra la estructura de datos de la aplicación interoperable concerniente. En esta estructura se muestran los valores relevantes para el caso de prueba representado. Igualmente, se muestran los cambios que deben ocurrir dentro del medio de pago, ejemplificando los valores iniciales y finales de cada dato relevante.
- Cada hoja muestra en una tabla separada, la información relevante del archivo de eventos. En dicha tabla se muestra la información que debe ser consignada en todos los eventos creados durante la ejecución del escenario, y, cuando sea necesario, la información que debe estar almacenada en eventos previos.

9.6.4 Manual de uso del documento de formatos genéricos para ejecución de pruebas de los suprocesos 2 y 3

En los escenarios de prueba de los subprocesos 2 y 3, se hace referencia al anexo 8 [29] del presente documento. Este anexo describe los eventos que deben ser enviados entre los actores en cada escenario de prueba. Cada archivo intercambiado entre entidades contiene toda la información almacenada por diversos usos del medio de pago en un periodo de tiempo. Por este motivo, este anexo busca exponer de forma genérica la información que se debe garantizar dependiendo del rol a certificar. De esta manera para las pruebas del subproceso 2, cada entidad está en la obligación de recrear la información que debería recibir, dados los escenarios de uso del subproceso 1. Enseguida se presentan las aclaraciones pertinentes sobre el documento:

- El anexo se compone de una serie de hojas en las cuales se presenta la información relevante para efectuar las pruebas. Adicionalmente se encuentran dos hojas que presentan nuevamente las tablas expuestas en la sección 9.5.2. Para las pruebas del subproceso 2, las hojas principales están nombradas de acuerdo al rol asociado al caso de prueba.
- La estructura de cada una de las hojas:
  - En primer lugar, se presenta la numeración de los escenarios de prueba para los cuales se va a recrear la información.
  - La siguiente columna indica el nombre del escenario. Es acá donde son relevantes las hojas de ***Eventos por casos***, ***Cambios en medio de pago*** y ***Acciones adicionales***. Dado el nombre del escenario es posible en ***Eventos por casos*** identificar los eventos que deben ser enviados. En ***Cambios en medio de pago*** a cada evento se le asocian los cambios que se deben efectuar en el medio de pago. En ***Acciones adicionales*** se identifica la información a enviar dadas las acciones de *solicitud*. De esta forma es posible comparar si la información enviada es la correcta.
  - La tercera columna corresponde al número del medio de pago que debe ser usado para recrear la información dado el caso de uso en específico.
  - La cuarta columna indica las características generales del medio de pago. Cabe aclarar que dependiendo del caso y dado que estos se basan en los del subproceso 1, es conveniente

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

revisar la configuración y condiciones previas del equivalente de la prueba de los primeros niveles.

- Finalmente, la última columna corresponde a un formato de encabezado de eventos, se deja explícito que el ejecutor de las pruebas debe identificar la fecha de generación del evento, así como el SAM usado para efectuarlo. Esta información debe ser comparada al llegar al destinatario del archivo. Adicional a estos campos se encuentra el número secuencial. Esta numeración se presenta teniendo en cuenta que cada escenario en la segunda columna puede generar varios eventos. Es así como en algunos casos se presenta, por ejemplo, *Número secuencial = 1-3* con el objetivo de indicar que deben ser 3 eventos diferentes los que se deben enviar, a pesar de que el SAM y la fecha deben ser los mismos.

10 Escenarios de Prueba

10.1 Escenarios de pruebas para entidades emisoras de medios de pago

10.1.1 Escenarios de pruebas del subproceso 1

10.1.1.1 Inicialización

ID_Prueba	1.0
Propósito	Garantizar que el proceso de inicialización del medio de pago se efectúe correctamente. Es decir, verificar la creación de la aplicación y sus directorios
Configuración	
Condiciones previas	
Acciones del test	Acercar el medio de pago a un dispositivo de inicialización del medio de pago
Resultados	▪ Se crean todos los DF de la aplicación interoperable ▪ Se cargan con éxito cada una de las llaves ▪ Se crean todos los archivos dentro de la aplicación conforme a las especificaciones de este documento. ▪ Se escriben los datos de los archivos ICC. ▪ Se asigna SerialMedioPago para cada una de las aplicaciones (DF) del medio de pago ▪ Se fija el estado de la aplicación como inicializado

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.1.1.2 Emisión de medio de pago recargable

10.1.1.2.1 Emisión de medio de pago anónimo

ID_Prueba	1.1.1
Propósito	Garantizar que un usuario anónimo con perfil general adquiera un medio de pago con las condiciones establecidas. Adicionalmente, asegurar que esté en la capacidad de utilizar cada uno de sus productos en la red interoperable.
Configuración	
Condiciones previas	El medio de pago fue inicializado
Acciones del test	Acercar el medio de pago a un dispositivo de emisión de medios de pago
Resultados	▪ Se completan todos los datos en el archivo de ENTORNO ▪ Se distribuye el producto general y pasa a estado activado (SERVICIOS(General).EstadoProducto = 1) ▪ Se escribe en un sector libre del archivo LISTA_CONTRATOS la información correspondiente al producto general ▪ Se efectúa la recarga del producto general. Se incrementa el valor de este producto en el ingresado al sistema. ▪ Se generan nuevos eventos en el archivo EVENTOS (Un evento de tipo emisión de medio de pago (6), un evento de distribución de producto (1) y un evento de recarga de producto general (3))
Observaciones	

10.1.1.2.2 Emisión de medio de pago personalizado

SITUACIÓN 1 – PRODUCTO GENERAL

ID_Prueba	1.1.2.1
Propósito	Garantizar que un usuario con perfil general reciba su medio de pago personalizado bajo las condiciones establecidas. Adicionalmente, asegurar que esté en la capacidad de utilizar el producto general.
Configuración	
Condiciones previas	El medio de pago fue inicializado

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Acciones del test	Acercar el medio de pago a un dispositivo de emisión de medios de pago
Resultados	▪ Se completan cada uno de los datos en ENTORNO ▪ Se escribe toda la información del usuario en USUARIO ▪ Se distribuye el producto general y pasa a estado activado (SERVICIOS(General)**.**EstadoProducto = 1) ▪ Se escribe en los correspondientes sectores del archivo LISTA_CONTRATOS la información correspondiente a cada producto emitido ▪ Se efectúa la recarga del producto general (**MONEDERO)**. Se incrementa el valor de este producto en el ingresado al sistema. ▪ Se generan nuevos eventos en el archivo EVENTOS (Un evento de tipo emisión de medio de pago (6), un evento de modificación de datos de usuario (7), un evento de distribución de producto (1) y un evento de recarga de producto general (3))
Observaciones	

SITUACIÓN 2 – PRODUCTO ESPECIAL ASOCIADO A MONEDERO

ID_Prueba	1.1.2.2
Propósito	Asegurar que el usuario de un segmento especial adquiera un medio de pago personalizado con un producto especial asociado al **MONEDERO**. Las recargas del producto se harán en el **MONEDERO,** las reglas de validez y los beneficios tarifarios se definirán al tomar información del archivo de parámetros en terminales de aceptación.
Configuración	Se requiere de un mínimo de seis medios de pago para probar emisión de medio de pago personalizado con producto general, productos especiales (estudiante, adulto mayor, invidente, discapacitado), y no recargable.
Condiciones previas	El medio de pago fue inicializado
Acciones del test	Acercar el medio de pago al dispositivo de emisión
Resultados	▪ Se completan cada uno de los datos en ENTORNO ▪ Se escribe la información del usuario en USUARIO ▪ Se distribuye el producto especial asociado al **MONEDERO** y pasa a estado activado (SERVICIOS(Especial)**.**EstadoProducto = 1) ▪ Se escribe en los correspondientes sectores del archivo LISTA_CONTRATOS la información correspondiente a cada producto emitido. ▪ Se efectúa la recarga del producto especial (**MONEDERO)**. Se incrementa el valor de este producto de acuerdo con lo establecido por

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

el distribuidor. Esta recarga no se hace si el perfil es de invidente.
- Se generan nuevos eventos en el archivo EVENTOS (un evento de tipo emisión de medio de pago (6), un evento de modificación de datos de usuario (7), un evento de distribución de producto especial (1) y un evento de recarga de producto especial (3) (no se hace para producto de invidente)).

Observaciones

SITUACIÓN 3 – PRODUCTO ESPECIAL ASOCIADO A CONTADOR

Para esta prueba es necesario crear un producto ficticio.

ID_Prueba	1.1.2.3
Propósito	Asegurar que el usuario de un segmento especial adquiera un medio de pago personalizado con un producto especial asociado a un contador (e.g. producto con número de viajes limitado para un periodo de tiempo determinado, pero que debe renovarse periódicamente). Las recargas del producto se harán en el contador, sus reglas de validez y los beneficios tarifarios se definirán al tomar información del archivo de parámetros en terminales de aceptación.
Configuración	
Condiciones previas	El medio de pago fue inicializado
Acciones del test	Acercar el medio de pago al dispositivo de emisión
Resultados	- Se completan cada uno de los datos en ENTORNO - Se escribe la información del usuario en USUARIO - Se distribuye el producto especial asociado al contador de valor variable en CONTADORES y pasa a estado activado (SERVICIOS(Especial).EstadoProducto = 1) - Se escribe en los correspondientes sectores del archivo LISTA_CONTRATOS la información correspondiente al producto especial emitido. - Se efectúa la recarga del producto especial (CONTADORES). Se incrementa el valor de este producto de acuerdo con lo establecido por el distribuidor. Esta recarga no se hace si el perfil es de invidente. - Se generan nuevos eventos en el archivo EVENTOS (un evento de tipo emisión de medio de pago (6), un evento de modificación de datos de usuario (7), un evento de distribución de producto especial (1) y un evento de recarga de producto especial (3) (no se hace para producto de invidente)).

Observaciones

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

10.1.1.3 Emisión medio de pago no recargable

ID_Prueba	1.2
Propósito	Garantizar que el usuario de medio de pago no recargable adquiera un medio de pago con un saldo establecido
Configuración	
Condiciones previas	
Acciones del test	Acercar el medio de pago a un dispositivo de emisión de medios de pago
Resultados	▪ Los dos últimos bytes de la página 0x02 (Lock Bytes) se establecen en 0xF800 ▪ Se escriben todos los datos de emisión en las páginas 0x00 a 0x06 ▪ Se incrementa el saldo del Contador #1 al valor designado para el medio de pago ▪ Se escriben todos los datos asociados al evento de emisión en las páginas 0x07 a 0x0D. ▪ Se genera un evento de emisión de medio de pago no recargable. ▪ Se calcula MACEstado cuyos datos de diversificación corresponden a los datos de las páginas 0x00 a 0x0D junto con el valor del Contador #1
Observaciones	

10.1.1.4 Personalización posventa del medio de pago recargable

ID_Prueba	1.3
Propósito	Garantizar que un usuario perteneciente a un segmento especial esté en la capacidad de personalizar su medio de pago previamente emitido y recibido
Configuración	
Condiciones previas	▪ El medio de pago tuvo que haber sido previamente inicializado y emitido ▪ El medio de pago se encuentra activo ▪ El medio de pago se ha emitido con el perfil anónimo y este se encuentra activo.
Acciones del test	Acercar el medio de pago a un dispositivo de emisión de medios de pago
Resultados	▪ Se escribe la información del usuario en USUARIO ▪ Se debe cambiar el perfil del usuario ▪ Se debe distribuir el producto relacionado con el perfil. ▪ Se debe recargar el valor del archivo de valor, bien sea un contador o el

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	MONEDERO. ▪ Se deben enviar 3 eventos, uno por la modificación de los datos de usuario (4), uno por la distribución del producto (1), uno por la recarga del producto (2).
Observaciones	

10.1.1.5 Reconstrucción del medio de pago

ID_Prueba	1.4
Propósito	Garantizar que el usuario pueda remplazar su medio de pago en caso de pérdida o avería
Configuración	
Condiciones previas	▪ El medio que se desea remplazar tuvo que haber sido previamente inicializado y emitido. ▪ El medio de pago se ha emitido con el perfil general personalizado. ▪ El emisor de medios de pago tiene la información completa y actualizada relacionada con el medio de pago
Acciones del test	Acercar el medio de pago nuevo a un dispositivo de emisión de medios de pago
Resultados	▪ Se inicializa el medio de pago y se cumple con la prueba de ID 1.0 ▪ Se emiten los productos que tenía el medio de pago y se cumple con las pruebas de ID 1.1.2., dependiendo del tipo de medio de pago. Esto incluye la escritura de la última información registrada en los archivos CONTRATOS, SERVICIOS, LISTA_CONTRATOS, Valor (Producto) para cada producto, USUARIO, DEVOLUCIONES, y FUNCIONARIO (si es el medio de pago de un funcionario).
Observaciones	

10.1.1.6 Bloqueo del medio de pago

ID_Prueba	1.5
Propósito	Bloquear el medio de pago siguiendo las instrucciones del caso de uso presentado en este documento
Configuración	
Condiciones previas	▪ El medio tuvo que haber sido previamente inicializado y emitido ▪ El medio de pago debe contener la aplicación que se quiere bloquear y esta debe estar en estado activado
Acciones del test	Acercar el medio de pago nuevo a un dispositivo de emisión de medios de pago

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Resultados	▪ Se actualiza el archivo ESTADO_APLICACIÓN(Producto).EstadoAplicación = 3 ▪ La aplicación queda en estado bloqueado ▪ No se puede hacer uso de los productos almacenados en la aplicación bloqueada ▪ La aplicación se puede desbloquear
Observaciones	

10.1.1.7 Desactivación del medio de pago

ID_Prueba	1.6
Propósito	Desactivar el medio de pago siguiendo las instrucciones del caso de uso presentado en este documento
Configuración	
Condiciones previas	▪ El medio tuvo que haber sido previamente inicializado y emitido con el perfil estudiantil ▪ El medio de pago debe contener la aplicación que se quiere desactivar y esta debe estar en estado activado
Acciones del test	Acercar el medio de pago nuevo a un dispositivo de emisión de medios de pago
Resultados	▪ Se actualiza el archivo ESTADO_APLICACIÓN(Producto).EstadoAplicación = 2 ▪ La aplicación queda en estado desactivado ▪ No se puede hacer uso de los productos almacenados en la aplicación desactivada ▪ No se puede volver a activar la aplicación
Observaciones	

10.1.1.8 Desbloqueo del medio de pago

ID_Prueba	1.7
Propósito	Desbloquear una aplicación del medio de pago que ha sido previamente bloqueada. Una vez desbloqueada el usuario puede volver a utilizarla para acceder al sistema de transporte.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Configuración	
Condiciones previas	▪ El medio tuvo que haber sido previamente bloqueado ▪ El medio de pago debe contener la aplicación que se quiere desbloquear y esta debe estar en estado bloqueado
Acciones del test	Acercar el medio de pago nuevo a un dispositivo de emisión de medios de pago
Resultados	▪ Se actualiza el archivo ESTADO_APLICACIÓN(Producto).EstadoAplicación = 1 ▪ La aplicación queda en estado activado ▪ Se puede volver a hacer uso de los productos almacenados en la aplicación desbloqueada ▪ La aplicación puede volver al estado bloqueado o pasar al estado desactivado
Observaciones	

10.1.2 Escenarios de pruebas del subproceso 2

10.1.2.1 Intercambio de archivos entre niveles 3 y 4

ID_Prueba	2.1.1
Propósito	Garantizar que la Cámara de Compensación reciba correctamente la información proveniente del emisor de medios de pago, dados los eventos recreados por este último actor.
Configuración	Se requiere simular un mínimo de seis medios de pago para probar emisión de medio de pago personalizado con producto general, productos especiales (estudiante, adulto mayor, invidente, discapacitado), y no recargable.
Condiciones previas	Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago
Acciones del test	1. La entidad emisora debe recrear la información que debería recibir dados los tipos de casos de uso a probar (Ver hoja ***Emisión*** de anexo 8 [29]). Posteriormente, debe generar el archivo XML y enviarlo a la Cámara de Compensación. 2. La Cámara de compensación debe entonces verificar la validez de las firmas generadas con la respectiva llave privada de la entidad
Resultados	Debe verificarse que el archivo cumpla con lo siguiente: ▪ Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento. ▪ El número de eventos corresponde con la cantidad enviada y con lo establecido en la hoja ***Emisión*** del anexo 8 [29]

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- El encabezado de los eventos debe corresponder con lo siguiente:
  - Fecha exacta de supuesta ocurrencia del evento
  - IdSAM otorgado por el Registrador
  - Número secuencial dependiendo del orden de ocurrencia del evento.
- Firma válida generada por el emisor de medios de pago

Observaciones

10.1.3 Escenarios de pruebas del subproceso 3

10.1.3.1 Integración de pruebas de subprocesos 1 y 2

ID_Prueba	3.1
Propósito	Garantizar que la información de los eventos de emisión generados por la interacción con los medios de pago sea remitida con éxito a la Cámara de Compensación. Además, asegurar que los archivos del medio de pago cambien conforme a las mismas acciones
Configuración	
Condiciones previas	Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago
Acciones del test	1. Se ejecutan todas las pruebas de nivel 0-1 para emisores de medios de pago, de conformidad con la hoja ***Emisión*** del anexo 8 [29]. 2. Se generan todos los archivos XML asociados a la información generada por transacciones entre nivel 0-1, se almacenan en el nivel 3. 3. Se envían los archivos de nivel 3 a nivel 4. 4. Verificar la validez de las firmas de los archivos recibidos.
Resultados	1. El archivo enviado por la entidad emisora debe cumplir con lo siguiente: ▪ Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento. ▪ El número de eventos corresponde con la cantidad enviada y con lo establecido en la hoja ***Emisión*** ▪ El encabezado de los eventos debe corresponder con lo siguiente: – Fecha exacta de ocurrencia del evento – IdSAM otorgado por el Registrador – Número secuencial dependiendo del orden de ocurrencia del evento ▪ Firma válida generada por los actores de la red 2. El medio de pago cambia de acuerdo con los resultados esperados de las pruebas de subproceso 1 que se presentan en la hoja ***Emisión***
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.2 Escenarios de prueba de distribución y recarga de productos

10.2.1 Escenarios de pruebas del subproceso 1

10.2.1.1 Adquisición de un producto especial posventa

10.2.1.1.1 Adquisición de un producto asociado al MONEDERO

ID_Prueba	1.8.1
Propósito	Garantizar que un usuario con un perfil específico esté en la capacidad de adquirir un producto especial, con archivo de valor **MONEDERO**, si este aún no se encuentra almacenado en su medio de pago.
Configuración	
Condiciones previas	▪ El medio de pago tuvo que haber sido previamente inicializado y emitido ▪ El medio de pago es anónimo ▪ El medio de pago cuenta con el producto general ▪ El medio de pago se encuentra activo
Acciones del test	Acercar el medio de pago a un dispositivo de distribución y recarga
Resultados	▪ Se escribe la información del usuario en USUARIO ▪ Se crea el registro CONTRATOS(Producto) y se escribe la información requerida en el mismo ▪ El producto especial distribuido pasa a estado activado ▪ Se escribe en los correspondientes sectores del archivo LISTA_CONTRATOS la información correspondiente al producto emitido ▪ Se efectúa la recarga del producto especial. Se incrementa el valor de este producto de acuerdo con lo establecido para el distribuidor. ▪ Se generan nuevos eventos en el archivo EVENTOS (Un evento de modificación de datos de usuario (7), un evento de distribución de producto (1) y un evento de recarga de producto (3))
Observaciones	

10.2.1.1.2 Adquisición de un producto asociado a contador

ID_Prueba	1.8.3
Propósito	Garantizar que un usuario con un perfil específico esté en la capacidad de adquirir un producto especial, con valor asociado a contador, si este aún no se encuentra almacenado en su medio de pago.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Configuración	
Condiciones previas	▪ El medio de pago tuvo que haber sido previamente inicializado y emitido ▪ El medio de pago es anónimo ▪ El medio de pago cuenta con el producto general ▪ El medio de pago se encuentra activo
Acciones del test	Acercar el medio de pago a un dispositivo de distribución y recarga
Resultados	▪ Se escribe la información del usuario en USUARIO ▪ Se crea el registro CONTRATOS(Producto) y se escribe la información requerida en el mismo ▪ El producto especial distribuido pasa a estado activado ▪ Se escribe en los correspondientes sectores del archivo LISTA_CONTRATOS la información correspondiente al producto emitido ▪ Se efectúa la recarga del producto especial. Se fija el valor de este producto de acuerdo con lo establecido para el distribuidor. ▪ Se generan nuevos eventos en el archivo EVENTOS (Un evento de modificación de datos de usuario (7), un evento de distribución de producto (1) y un evento de recarga de producto (3))
Observaciones	

10.2.1.2 Renovación de un producto

ID_Prueba	1.9
Propósito	Garantizar que la renovación de un producto efectivamente permite su uso en el sistema interoperable
Configuración	
Condiciones previas	▪ El medio de pago tuvo que haber sido previamente inicializado y emitido ▪ El medio de pago se encuentra activo
Acciones del test	Acercar el medio de pago a un dispositivo de distribución y recarga
Resultados	▪ Se sobrescriben los archivos CONTRATOS(Producto) y SERVICIOS(Producto) ▪ En caso de recarga esta se efectúa y se incrementa el valor de este producto Valor(Producto) en el ingresado al sistema ▪ En caso de recarga se generan dos eventos, un evento de distribución de producto (1) y un evento de recarga de producto (3) en el archivo EVENTOS
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.2.1.3 Recarga de productos

Todas las pruebas relacionadas con la acción de recarga tienen las siguientes condiciones previas adicionales a las presentadas en cada uno de los casos de prueba.

- El medio de pago tuvo que haber sido previamente inicializado y emitido
- El medio de pago se encuentra activo
- El producto que se desea recargar se encuentra almacenado en un medio de pago perteneciente a la red interoperable
- Los productos del medio de pago no han vencido (El campo FinValidezProducto indicado en CONTRATOS(Producto) es mayor a la fecha actual)
- En caso de productos vencidos no se debe permitir la recarga
- Los productos pueden encontrarse en estado activado o suspendido

10.2.1.3.1 Recarga de producto asociado al MONEDERO

SITUACIÓN 1 – SALDO DESPUÉS DE RECARGA MENOR A TARIFA MÁXIMA APLICABLE

ID_Prueba	1.10.1.1
Propósito	Garantizar que el usuario pueda efectuar correctamente la recarga de un producto dada la presente configuración
Configuración	Se cuenta con un medio de pago con producto asociado a MONEDERO y se estima que el valor después de la recarga será mayor o igual a la tarifa máxima aplicable al producto por recargar.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de recarga
Resultados	▪ No debe ser posible la recarga del producto ▪ No se generan eventos
Observaciones	

SITUACIÓN 2 – SALDO DESPUÉS DE RECARGA MAYOR O IGUAL A TARIFA MÁXIMA APLICABLE

ID_Prueba	1.10.1.2
Propósito	Garantizar que el usuario pueda efectuar correctamente la recarga de un producto dada la presente configuración
Configuración	Se cuenta con un medio de pago con producto asociado al

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	MONEDERO, se estima que el valor después de la recarga será mayor o igual a la tarifa máxima aplicable al producto por recargar.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de recarga
Resultados	▪ Se efectúa la recarga del producto. Se incrementa el valor de este producto en el ingresado al sistema ▪ Se genera un nuevo evento de recarga (3) en el archivo EVENTOS La recarga se efectúa instantáneamente
Observaciones	

10.2.1.3.2 Recarga de producto asociado a contador

ID_Prueba	1.10.2
Propósito	Garantizar que el usuario pueda efectuar correctamente la recarga de un producto dada la presente configuración
Configuración	Se cuenta con un medio de pago con producto asociado a un contador variable y se estima que el valor después de la recarga será mayor o igual a la tarifa máxima aplicable al producto por recargar.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de recarga
Resultados	▪ Se efectúa la recarga del producto. Se incrementa el valor de este producto en el ingresado al sistema ▪ Se genera un nuevo evento de recarga (3) en el archivo EVENTOS ▪ La recarga se efectúa instantáneamente
Observaciones	

10.2.1.4 Devolución del monto de la última recarga

ID_Prueba	1.11
Propósito	Garantizar que se pueda hacer la devolución del monto de la última recarga

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Configuración	
Condiciones previas	Son necesarios 2 medios de pago emitidos y con producto General activo: Uno cuyo último evento registrado NO sea una recarga Uno cuyo último evento registrado sea una recarga
Acciones del test	Acercar el dispositivo a un equipo de recarga
Resultados	▪ Para el primer medio de pago, la devolución no se ejecuta. ▪ Para el segundo medio de pago, se hace la devolución de todo el monto recargado, es decir se modifica Valor(Producto), se genera un evento nuevo en EVENTOS de tipo Devolución de recarga (8) y ESTADO_APLICACIÓN.NúmeroAcciónAplicada incrementa en 1.
Observaciones	

10.2.1.5 Recarga remota de productos

ID_Prueba	1.12
Propósito	Garantizar que se pueda recargar un producto de forma remota
Configuración	▪ Actualizar lista LAP_R con la información del medio de pago a recargar ▪ NúmeroAcciónProducto es mayor que CONTRATOS(Producto).NúmeroAcciónAplicadaProducto
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializado y emitido
Acciones del test	Acercar el medio de pago al dispositivo de distribución y recarga
Resultados	▪ NúmeroAcciónAplicadaProducto del archivo CONTRATOS(Producto) se incrementa en 1 ▪ Se efectúa la recarga del producto. Se incrementa el valor de este producto en el ingresado al sistema ▪ Se crea un evento de recarga en el archivo EVENTOS
Observaciones	Solo se puede recargar el producto si el monto pagado en la recarga remota es mayor o igual a la suma de la deuda más la máxima tarifa aplicable. Se deben satisfacer las restricciones para recarga descritas en la sección 4.1.5.

10.2.1.6 Suspensión de productos

ID_Prueba	1.13

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Propósito	Garantizar que la suspensión de cada uno de los productos se dé correctamente
Configuración	
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializado y emitido, con uno o varios productos activos
Acciones del test	Acercar el medio de pago al dispositivo de distribución y recarga
Resultados	▪ Se suspenden uno o varios productos almacenados en el medio de pago ▪ Para cada producto suspendido, se actualiza el valor de SERVICIOS(Producto).EstadoProducto = 2 (suspendido) ▪ No es posible hacer uso de los productos suspendidos ▪ Los productos pueden reactivarse
Observaciones	Para garantizar que es efectivamente no es posible usar los productos del medio de pago se deben realizar las pruebas de recarga y no debe ser posible efectuar el procedimiento. Además, se debe poder garantizar la no sea posible aceptación de dicho medio de pago. Es decir que se deben efectuar las pruebas de aceptación para dicho medio de pago y este no debe ser aceptado.

10.2.1.7 Reactivación de productos

ID_Prueba	1.14
Propósito	Garantizar que la reactivación de cada uno de los productos se dé correctamente
Configuración	
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializado y emitido, con uno o varios productos suspendidos
Acciones del test	Acercar el medio de pago al dispositivo de distribución y recarga
Resultados	▪ Es posible utilizar cada uno de los productos reactivados del medio de pago ▪ Se generan cambios en CONTRATOS(Producto) (CONTRATOS(Producto).NúmeroReactivaciónProducto se incrementa en 1) ▪ Se modifica el estado del producto a activo
Observaciones	Para garantizar que es efectivamente posible usar los productos del medio de pago se deben realizar las pruebas de recarga.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Además, se debe poder garantizar la aceptación de dicho medio de pago. Es decir que se deben efectuar las pruebas de aceptación para dicho medio de pago

10.2.1.8 Reembolso de saldo en el medio de pago

REEMBOLSO DE SALDO DE MEDIO DE PAGO ANÓNIMO

ID_Prueba	1.15.1
Propósito	Garantizar que el reembolso del saldo de un medio de pago anónimo se realiza satisfactoriamente
Configuración	
Condiciones previas	El medio de pago fue previamente inicializado, emitido con perfil anónimo y recargado.
Acciones del test	Acercar el medio de pago a un dispositivo de recarga.
Resultados	▪ Débito de la totalidad del saldo en la aplicación monedero. ▪ Borrar todos los eventos del medio de pago.
Observaciones	

REEMBOLSO DE SALDO DE MEDIO DE PAGO PERSONALIZADO

ID_Prueba	1.15.2
Propósito	Garantizar que el reembolso del saldo de un medio de pago personalizado se realiza satisfactoriamente
Configuración	
Condiciones previas	El medio de pago fue previamente inicializado, emitido, personalizado y recargado.
Acciones del test	Acercar el medio de pago a un dispositivo de recarga.
Resultados	▪ Débito de la totalidad del saldo en la aplicación monedero. ▪ Escribir un evento de tipo reembolso en el medio de pago.
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.2.2 Escenarios de pruebas del subproceso 2

10.2.2.1 Intercambio de archivos entre niveles 3 y 4

ID_Prueba	2.2.1
Propósito	Garantizar que la Cámara de Compensación y las otras Empresas Operadoras de Recaudo reciban correctamente la información proveniente de los distribuidores de medios de pago, dados los eventos recreados por este último actor.
Configuración	Se requiere simular un mínimo de ocho medios de pago para probar los casos con medios de pago con perfil anónimo, personalizados y con producto especial
Condiciones previas	Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago
Acciones del test	1. La entidad debe recrear la información que debería recibir dados los tipos de casos de uso a probar (Ver hoja ***Distribución y Recarga*** del anexo [30]). 2. Posteriormente, debe generar el archivo XML y enviarlo a la cámara de compensación. 3. En caso de que una acción de lista esté involucrada en el proceso, la cámara debe enviar la difusión o confirmación a los demás actores interesados. 4. Verificar la validez de las firmas generadas con la respectiva llave privada de la entidad receptora
Resultados	Los destinatarios reciben el archivo de la siguiente forma: ▪ Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento. ▪ El número de eventos corresponde con la cantidad enviada y con lo establecido en la hoja ***Distribuidor*** ▪ El encabezado de los eventos debe corresponder con lo siguiente: – Fecha exacta de supuesta ocurrencia del evento – IdSAM otorgado por el Registrador – Número secuencial dependiendo del orden de ocurrencia del evento. ▪ Firma válida generada por el distribuidor de productos
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.2.3 Escenarios de pruebas del subproceso 3

10.2.3.1 Integración de pruebas de subprocesos 1 y 2

ID_Prueba	3.2.1
Propósito	Garantizar que la información de los eventos de distribución, generados por la interacción con los medios de pago, sea remitida con éxito a la Cámara de Compensación y a las demás Empresas Operadoras de Recaudo. Además, asegurar que los archivos del medio de pago cambien conforme a las mismas acciones
Configuración	
Condiciones previas	Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago
Acciones del test	1. Se ejecutan todas las pruebas del subproceso 1 en concordancia con el modelo genérico presentado en la hoja ***Distribución y Recarga*** del anexo [30]. 2. Verificar la validez de las firmas de los archivos enviados por el Operador de Recaudo.
Resultados	1. Todos los destinatarios reciben un archivo por la entidad emisora, el cual llega de la siguiente forma: ▪ Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento. ▪ El número de eventos corresponde con la cantidad enviada y con lo establecido en la hoja ***Distribución y Recarga*** ▪ El encabezado de los eventos debe corresponder con lo siguiente: • Fecha exacta de ocurrencia del evento • IdSAM otorgado por el Registrador • Número secuencial dependiendo del orden de ocurrencia del evento ▪ Firma válida generada por los actores de la red 2. El medio de pago cambia de acuerdo con los resultados esperados de las pruebas del subproceso 1 que se presentan en la hoja ***Distribución y Recarga***
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

10.3 Escenarios de prueba de aceptación de medios de pago

10.3.1 Escenarios de pruebas del subproceso 1

10.3.1.1 Aceptación del medio de pago recargable

Las pruebas 1.15.1.1, 1.15.1.2, 1.15.1.3 relacionadas con la transacción de aceptación de un medio de pago tienen las siguientes condiciones previas adicionales a las presentadas en cada uno de los casos de prueba.

- El medio de pago tuvo que haber sido previamente inicializado, emitido y personalizado en caso de ser necesario.
- El medio de pago se encuentra activo.
- El producto con el cual se desea ingresar al sistema se encuentra almacenado en un medio de pago perteneciente a la red interoperable.
- Los productos dentro del medio de pago que van a ser usados no han vencido (El dato FinValidezProducto indicado en CONTRATOS(Producto) es mayor a la fecha actual).
- Se cumplen todas las restricciones del producto en CONTRATO(Producto) y SERVICIOS(Producto).

10.3.1.1.1 Aceptación de producto asociado a MONEDERO

Las situaciones que se presentan a continuación deben probarse para todos los productos asociados al **MONEDERO**.

SITUACIÓN 1 – SALDO SUFICIENTE

ID_Prueba	1.15.1.1
Propósito	Garantizar que el medio de pago sea aceptado para acceder al servicio de transporte en caso de contar con un producto asociado al **MONEDERO**.
Configuración	El medio de pago debe contar con saldo suficiente para un viaje con el producto asociado al **MONEDERO**.
Condiciones previas	Medio de pago inicializado
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Si es necesario, se reduce el saldo del **MONEDERO** ▪ Se escribe la información de la transacción de aceptación en SERVICIOS(Producto) ▪ Se genera un nuevo evento de uso (4) con el producto asociado al **MONEDERO** en el archivo EVENTOS. El dispositivo debe mostrar información del nuevo saldo
Observaciones	Se deben registrar resultados para 5 medios de pago:

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

- 1 medio de pago con producto general válido
- 1 medio de pago con producto especial de estudiante válido
- 1 medio de pago con producto especial de adulto mayor válido
- 1 medio de pago con producto especial de discapacitado válido
- 1 medio de pago con producto especial de invidente válido

SITUACIÓN 2 – SALDO INSUFICIENTE SIN CRÉDITO SIN OTRO PRODUCTO VÁLIDO DISPONIBLE

ID_Prueba	1.15.1.2
Propósito	Garantizar que el usuario con un medio de pago no pueda acceder al servicio de transporte en caso de no contar con saldo disponible ni tampoco con la facilidad de viaje a crédito, ya sea porque el valor mínimo del producto no permite viaje a crédito, o porque el saldo del **MONEDERO** es negativo
Configuración	El medio de pago no debe tener saldo suficiente para un viaje con el producto asociado al **MONEDERO.** Deben hacerse pruebas con dos medios de pago: i) Medio de pago con producto con restricción de valor mínimo que impide viaje a crédito ii) Medio de pago con saldo negativo en el **MONEDERO**
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario del tipo de problema que ha ocurrido con el pago
Observaciones	Se deben registrar resultados para 5 medios de pago: - 1 medio de pago con producto general sin saldo - 1 medio de pago con producto especial de estudiante sin saldo y producto general sin saldo - 1 medio de pago con producto especial de adulto mayor sin saldo y producto general sin saldo

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

- 1 medio de pago con producto especial de discapacitado sin saldo y producto general sin saldo

- 1 medio de pago con producto especial de invidente sin saldo y producto general sin saldo

SITUACIÓN 3 – SALDO INSUFICIENTE CON CRÉDITO

ID_Prueba	1.15.1.4
Propósito	Garantizar que el usuario con un medio de pago pueda acceder al servicio de transporte en caso de no contar con saldo disponible, haciendo uso del viaje a crédito.
Configuración	El medio de pago debe contar con saldo insuficiente para un viaje con el producto asociado al **MONEDERO**, el producto debe ser válido y debe contar con saldo a crédito suficiente para completar la tarifa y darle acceso al usuario
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se reduce el saldo del **MONEDERO** ▪ El saldo del **MONEDERO** es negativo ▪ Se escribe la información de la transacción de aceptación en **SERVICIOS(Producto)** ▪ Se genera un nuevo evento de uso (4) con el producto asociado al **MONEDERO** en el archivo EVENTOS ▪ El dispositivo debe mostrar información del nuevo saldo
Observaciones	

SITUACIÓN 4 – PRODUCTO EXPIRADO

ID_Prueba	1.15.1.5
Propósito	Garantizar que el usuario con un medio de pago no pueda acceder al servicio de transporte en caso de que el producto ha expirado.
Configuración	El medio de pago debe contar con uno o varios productos asociados al **MONEDERO** cuya fecha de vencimiento es menor a

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	la fecha actual.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario que el producto ha expirado
Observaciones	

10.3.1.1.2 Aceptación de producto asociado a contador

Considerando que no se han definido productos de este tipo para los subsistemas de transporte del SITM-Q, es necesario hacer las pruebas de esta sección con un producto ficticio que utilice contador de valor fijo como archivo de valor.

Se deben hacer pruebas para un producto asociado a contador fijo y para un producto asociado a un contador de valor variable.

SITUACIÓN 1 – SALDO SUFICIENTE

ID_Prueba	1.15.2.1
Propósito	Garantizar que el usuario con un medio de pago pueda acceder al servicio de transporte en caso de que cuente con un producto válido asociado a un contador con saldo suficiente para un viaje.
Configuración	Debe utilizarse un medios de pago con un producto asociado a contador de valor variable
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se reduce el saldo del contador ▪ Se escribe la información de la transacción de aceptación en **SERVICIOS(Producto)** ▪ Se genera un nuevo evento de uso (4) con el producto asociado al contador en el archivo EVENTOS
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

SITUACIÓN 2 – SALDO INSUFICIENTE CON OTRO PRODUCTO VÁLIDO DISPONIBLE

ID_Prueba	1.15.2.2
Propósito	Garantizar que el usuario con un medio de pago pueda acceder al servicio de transporte en caso de que su producto especial asociado a un contador de valor fijo no tenga saldo suficiente o haya expirado, mediante el uso de un producto válido de menor prioridad asociado al **MONEDERO**.
Configuración	El medio de pago debe contar con el producto general válido y con saldo suficiente y debe contar con un producto asociado a un contador de valor fijo sin saldo disponible.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se reduce el saldo del producto General ▪ Se escribe la información de la transacción de aceptación en **SERVICIOS(Producto)** ▪ Se genera un nuevo evento de uso (4) con el producto asociado al **MONEDERO** en el archivo EVENTOS
Observaciones	

SITUACIÓN 3 – SALDO INSUFICIENTE SIN OTRO PRODUCTO VÁLIDO DISPONIBLE

ID_Prueba	1.15.2.3
Propósito	Garantizar que el usuario con un medio de pago no pueda acceder al servicio de transporte en caso de que su producto especial asociado a un contador de valor fijo no tenga saldo suficiente o haya expirado, y tampoco cuenta con otros productos válidos.
Configuración	El medio de pago debe contar con uno o varios productos asociados al **MONEDERO** y con al menos un producto asociado a un contador de valor fijo. Ninguno de los productos tiene saldo suficiente para que el usuario viaje.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario
Observaciones	

SITUACIÓN 4 – PRODUCTO EXPIRADO

ID_Prueba	1.15.2.4
Propósito	Garantizar que el usuario con un medio de pago no pueda acceder al servicio de transporte en caso de que el producto ha expirado.
Configuración	El medio de pago debe contar con un producto asociado al **Contador** cuya fecha de vencimiento es menor a la fecha actual. El producto general no tiene saldo suficiente.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario que el producto ha expirado
Observaciones	

10.3.1.1.3 Aceptación del medio de pago con un producto suspendido

Todas las pruebas relacionadas con la aceptación de un medio de pago con productos suspendidos cumplen con la condición previa de que el producto se encuentra en la lista LAP_A.

SITUACIÓN 1 – ACEPTACIÓN DE PRODUCTO SUSPENDIDO SIN OTRO PRODUCTO

ID_Prueba	1.15.3.1
Propósito	Garantizar que el usuario de medio de pago recargable no esté

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	en la capacidad de usar el producto General, dado que se encuentra en estado suspendido y se cumple la presente configuración.
Configuración	El medio de pago debe contar con dos productos asociados al **MODENERO,** uno suspendido y el otro sin saldo suficiente.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario
Observaciones	

SITUACIÓN 2 – ACEPTACIÓN DE PRODUCTO SUSPENDIDO: ESPECIAL SUSPENDIDO Y GENERAL ACTIVO

ID_Prueba	1.15.3.2
Propósito	Garantizar que un medio de pago con perfil especial pueda acceder al servicio si el producto especial está suspendido y el producto general está activo.
Configuración	El medio de pago debe contar con saldo disponible en el producto general.
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se escribe la información de la transacción de aceptación en ***SERVICIOS(Producto)*** ▪ Se genera un nuevo evento de tipo uso (4) en el archivo ***EVENTOS***
Observaciones	Debe probarse para todos los productos especiales

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

SITUACIÓN 3 – ACEPTACIÓN DE PRODUCTO SUSPENDIDO: ESPECIAL Y GENERAL SUSPENDIDO

ID_Prueba	1.15.3.3
Propósito	Garantizar que el usuario de medio de pago recargable no esté en la capacidad de usar el producto Especial dado que se encuentra en estado suspendido y se cumple la presente configuración
Configuración	El medio de pago debe contar con (i) saldo negativo para realizar la transacción en el producto General
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario
Observaciones	Debe probarse para todos los productos especiales

SITUACIÓN 4 – ACEPTACIÓN DE PRODUCTO SUSPENDIDO: ESPECIAL SUSPENDIDO Y GENERAL CON CRÉDITO

ID_Prueba	1.15.3.4
Propósito	Garantizar que el usuario de medio de pago recargable no esté en la capacidad de usar el producto Especial dado que se encuentra en estado suspendido y se cumple la presente configuración
Configuración	El medio de pago debe contar con (i) saldo insuficiente para hacer la transacción en el producto General, pero cuenta con saldo a crédito
Condiciones previas	
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se actualiza el valor del producto general otorgado por viaje a crédito

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	▪ Se escribe la información de la transacción en SERVICIOS
Observaciones	Debe probarse para todos los productos especiales

10.3.1.1.4 Aceptación de medios de pago cuando hay transbordos

Este conjunto de pruebas solo debe ejecutarse en caso de decidir implementar transbordos en el servicio del SIR. Las situaciones planteadas parten del último producto usado en la última transacción de aceptación del medio de pago.

SITUACIÓN 1 – ACEPTACIÓN DE MEDIOS DE PAGO CON TRANSBORDO: TRANSBORDO PERDIDO

ID_Prueba	1.15.4.1
Propósito	Garantizar que el usuario de medio de pago recargable no esté en la capacidad de usar el descuento por transbordo si el tiempo límite del mismo ha finalizado
Configuración	Algún producto del medio de pago fue usado previamente y el tiempo entre este uso y la próxima aceptación del medio de pago es mayor a la ventana de transbordos autorizada. Se debe hacer la prueba con todos los perfiles disponibles.
Condiciones previas	Los medios de pago a probar deben haber sido emitidos y deben tener productos distribuidos
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	Dependiendo la configuración de cada producto, se debe efectuar el cobro de tarifa de forma habitual. Es decir, se debe comenzar un nuevo viaje con la tarifa completa para ese medio de pago. Se debe verificar que se haya efectuado un uso de producto acorde al perfil y a la configuración de productos.
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

SITUACIÓN 2 – ACEPTACIÓN DE MEDIOS DE PAGO CON TRANSBORDO: LÍMITE DE TRANSBORDOS

ID_Prueba	1.15.4.2
Propósito	Garantizar que el usuario de medio de pago recargable no esté en la capacidad de usar el descuento por transbordo si el límite de transbordos se ha cumplido
Configuración	Se han usado el máximo de transbordos permitidos en una ventana de tiempo para los medios de pago a probar
Condiciones previas	Los medios de pago a probar deben haber sido emitidos y deben tener productos distribuidos
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	Dependiendo la configuración de cada producto, se debe efectuar el cobro de tarifa de forma habitual. Es decir, se debe comenzar un nuevo viaje con la tarifa completa para ese medio de pago. Se debe verificar que se haya efectuado un uso de producto acorde al perfil y a la configuración de productos.
Observaciones	

SITUACIÓN 3 – ACEPTACIÓN DE MEDIOS DE PAGO CON TRANSBORDO: TRANSBORDO CON PRODUCTO GENERAL

ID_Prueba	1.15.4.3
Propósito	Garantizar que el usuario de medio de pago recargable haga uso del descuento de transbordo con un medio de pago cuya anterior transacción de aceptación fue hecha con el producto General, y este producto cuenta con saldo disponible.
Configuración	El medio de pago tiene una ventana de transbordo disponible, la última transacción de aceptación fue hecha con el producto General y este producto cuenta con saldo disponible para un transbordo.
Condiciones previas	Los medios de pago a probar deben haber sido emitidos y deben tener productos distribuidos

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	Se cobra la tarifa en el producto General y se cumplen los resultados de la situación 1.10.1.5. Debe aumentar el contador ***NúmeroTransbordos*** del nuevo registro del evento.
Observaciones	

SITUACIÓN 4– ACEPTACIÓN DE MEDIOS DE PAGO CON TRANSBORDO: TRANSBORDO CON CRÉDITO

ID_Prueba	1.15.4.4
Propósito	Garantizar que el usuario de medio de pago recargable pueda usar el descuento de transbordo si tiene la facilidad de viaje a crédito
Configuración	El medio de pago tiene una ventana de transbordo disponible, la última transacción de aceptación fue hecha con el producto General y este producto cuenta con saldo insuficiente para un transbordo, sin embargo cuenta con crédito disponible.
Condiciones previas	Los medios de pago a probar deben haber sido emitidos y deben tener productos distribuidos
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	Se cobra la tarifa en el producto General y se cumplen los resultados de la situación 1.10.1.3. Debe aumentar el contador ***NúmeroTransbordos*** del nuevo registro del evento.
Observaciones	

SITUACIÓN 5 – ACEPTACIÓN DE MEDIOS DE PAGO CON TRANSBORDO: TRANSBORDO CON PRODUCTO ESPECIAL

ID_Prueba	1.15.4.5
Propósito	Garantizar que el usuario de medio de pago recargable pueda usar el descuento de transbordo si la última aceptación del medio de pago fue hecha usando el producto especial

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Configuración	El medio de pago tiene una ventana de transbordo disponible, y la última transacción de aceptación fue hecha con el producto especial
Condiciones previas	Los medios de pago a probar deben haber sido emitidos y deben tener productos distribuidos
Acciones del test	Acercar el medio de pago al dispositivo de aceptación de medios de pago
Resultados	Se debe permitir el acceso al servicio de transporte. Se genera un evento de uso en **EVENTOS.** Debe aumentar el contador ***NúmeroTransbordos*** del nuevo registro del evento. Solo se actualiza **SERVICIOS(ProductoEspecial)** en el campo **NúmeroActualAceptaciones.** Esto quiere decir que no se reduce el saldo del producto, ni se cuenta el transbordo como un viaje en el campo **NúmeroViajesDíaSemana.**
Observaciones	

10.3.1.2 Devolución de la tarifa de la última transacción de aceptación

SITUACIÓN 1 – DEVOLUCIÓN DE LA TARIFA DE LA ÚLTIMA TRANSACCIÓN: DEVOLUCIÓN INVÁLIDA

ID_Prueba	1.16.1
Propósito	Garantizar la devolución de la tarifa a un medio de pago que lo requiera.
Configuración	Medio de pago cuya última transacción registrada en EVENTOS sea diferente a un uso de producto
Condiciones previas	Los medios de pago tuvieron que haber sido previamente inicializados y emitidos
Acciones del test	Acercar el medio de pago a un dispositivo capaz de efectuar la devolución de la tarifa de la última transacción de aceptación.
Resultados	No se otorga la devolución de la tarifa.
Observaciones	

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

SITUACIÓN 2 – DEVOLUCIÓN DE LA TARIFA DE LA ÚLTIMA TRANSACCIÓN: DEVOLUCIÓN VÁLIDA

ID_Prueba	1.16.2
Propósito	Garantizar la devolución de la tarifa a un medio de pago que lo requiera.
Configuración	Medio de pago cuya última transacción registrada en EVENTOS sea un uso de producto.
Condiciones previas	Los medios de pago tuvieron que haber sido previamente inicializados y emitidos
Acciones del test	Acercar el medio de pago a un dispositivo capaz de efectuar la devolución de la tarifa de la última transacción de aceptación.
Resultados	Se genera un nuevo evento en EVENTOS con EVENTOS.PunteroProducto = 0x11 y EVENTOS.TipoEvento = 9. La demás información del evento debe ser igual que la del evento anterior
Observaciones	
Condiciones previas	Los medios de pago tuvieron que haber sido previamente inicializados y emitidos
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	- El primer medio de pago no accede al servicio con una devolución - El segundo medio no accede al servicio con una devolución - El tercer medio de pago accede al servicio de transporte. Se genera un nuevo evento de uso de devolución (8). El registro de esa devolución se reinicia. - El cuarto medio de pago accede al servicio de transporte. Se genera un nuevo evento de uso de devolución (8). El registro de esa devolución se reinicia. - El quinto medio de pago puede acceder si cuenta con saldo disponible para pagar lo que no cubre la devolución, si esto pasa: se genera un nuevo evento de uso de devolución (8) y un nuevo evento de uso de producto(s) (4). El registro de esa devolución se reinicia. Si el medio de pago no tiene saldo suficiente no puede acceder al servicio
Observaciones	

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

10.3.1.3 Ejecución de suspensión de productos

ID_Prueba	1.17
Propósito	Garantizar que la acción de suspender productos efectivamente evita el acceso de los mismos
Configuración	▪ Lista LAP_A actualizada con una operación de suspensión de un producto almacenado en un medio de pago.
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializado y emitido. NúmeroSuspensiónProducto es mayor a CONTRATOS(Producto).NúmeroReactivaciónProducto.
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema de acuerdo a las pruebas con ID 1.10.2.1 a 1.10.2.11 ▪ Se modifica el estado del producto a suspendido (SERVICIOS(Producto).EstadoProducto = 2)
Observaciones	

10.3.1.4 Ejecución de bloqueo de medio de pago

ID_Prueba	1.18
Propósito	Garantizar que un medio de pago bloqueado no puede ser usado para acceder al sistema
Configuración	Lista LAM actualizada con la información del medio de pago NúmeroAcciónMedioPago debe ser mayor que ESTADO_APLICACIÓN.NúmeroAcciónAplicada
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializado y emitido
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ Se escriben datos en ESTADO_APLICACIÓN indicando que el medio de pago está bloqueado (ESTADO_APLICACIÓN.EstadoAplicación = 3 y ESTADO_APLICACIÓN.NúmeroAcciónAplicada aumentan en 1)

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Observaciones

10.3.1.5 Ejecución de desbloqueo de medio de pago

ID_Prueba	1.19
Propósito	Garantizar que un medio de pago bloqueado pueda ser desbloqueado y posteriormente usado por el usuario
Configuración	Lista LAM debe estar actualizada, NúmeroAcciónMedioPago debe ser mayor que ESTADO_APLICACIÓN.NúmeroAcciónAplicada
Condiciones previas	El medio de pago tuvo que haber sido previamente inicializada y emitida
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	▪ permite el acceso al sistema de acuerdo a las pruebas con ID 1.10.1.1 a 1.10.3.3 ▪ Se escriben datos en ESTADO_APLICACIÓN indicando que el medio de pago se encuentra activado (ESTADO_APLICACIÓN.EstadoAplicación = 1 y ESTADO_APLICACIÓN.NúmeroAcciónAplicada aumentan en 1)
Observaciones	

10.3.1.6 Ejecución de desactivación de medio de pago

ID_Prueba	1.20
Propósito	Garantizar que en caso de que la aplicación interoperable se encuentre desactivada no se puedan realizar acciones sobre esta
Configuración	Lista LAM debe estar actualizada, NúmeroAcciónMedioPago debe ser mayor que: ESTADO_APLICACIÓN.NúmeroAcciónAplicada
Condiciones previas	Se debe contar con un medio de pago previamente inicializado y emitido, para cada perfil de usuario definido para el SITM-Q. Se debe ejecutar la prueba para todos los medios de pago.
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

Resultados	▪ Se debe negar el acceso a la aplicación y por ende a los productos del medio de pago. ▪ Se escriben datos en ESTADO_APLICACIÓN indicando que el medio de pago se encuentra desactivado ESTADO_APLICACIÓN.EstadoAplicación = 2 y ESTADO_APLICACIÓN.NúmeroAcciónAplicada aumenta en 1
Observaciones	

10.3.1.7 Ejecución de Renovación remota de producto

ID_Prueba	1.21
Propósito	Garantizar que la acción de renovar productos remotamente se ejecute satisfactoriamente
Configuración	Lista LAP_RP debe estar actualizada, FechaFinValidez de la lista LAP_RP debe ser posterior a CONTRATOS(Producto).FechaFinValidez
Condiciones previas	El medio de pago tuvo que ser inicializado, Emitido y tener un producto vencido
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	▪ Se sobrescriben los archivos CONTRATOS(Producto) y SERVICIOS (Producto) como corresponda. ▪ Se genera un evento de distribución (renovación).
Observaciones	

10.3.1.8 Aceptación del medio de pago precargado

ACEPTACIÓN DEL MEDIO DE PAGO PRECARGADO CON SALDO

ID_Prueba	1.22.1
Propósito	Garantizar que el usuario del medio de pago precargado esté en la capacidad de acceder al sistema
Configuración	
Condiciones previas	El medio de pago fue previamente emitido
Acciones del test	Acercar el medio de pago a un equipo de aceptación de medios

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

	de pago
Resultados	▪ Se permite el acceso al sistema ▪ Se escriben todos los datos de último evento en las páginas 0x07 a 0x0D ▪ Se incrementa el saldo del ***Contador #1*** según el cobro de tarifa ▪ Se recalcula y escribe el nuevo ***MACEstado*** a partir de los datos de las páginas 0x00 a 0x0D junto con el nuevo valor del ***Contador #1***
Observaciones	

ACEPTACIÓN DEL MEDIO DE PAGO PRECARGADO SIN SALDO SUFICIENTE

ID_Prueba	1.22.2
Propósito	Garantizar que el usuario con medio de pago precargado no esté en la capacidad de usarlo si este se encuentra agotado
Configuración	El saldo del medio de pago debe ser insuficiente para pagar la tarifa del servicio de transporte
Condiciones previas	El medio de pago fue previamente emitido
Acciones del test	Acercar el medio de pago a un dispositivo de aceptación de medios de pago
Resultados	▪ Se niega el acceso al sistema ▪ El dispositivo informa al usuario
Observaciones	

10.3.1.9 Aceptación para salida del medio de pago recargable

ACEPTACIÓN PARA SALIDA MEDIO DE PAGO RECARGABLE: SALIDA VALIDA

ID_Prueba	1.23.1
Propósito	Garantizar que el usuario del medio de pago recargable pueda salir del sistema de transporte
Configuración	
Condiciones previas	El medio de pago fue previamente aceptado para entrada al sistema
Acciones del test	Acercar el medio de pago a un equipo de aceptación de medios

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

	de pago
Resultados	▪ Se permite al usuario salir del sistema ▪ Se genera un nuevo evento en EVENTOS con EVENTOS.TipoEvento = 7.
Observaciones	

ACEPTACIÓN PARA SALIDA MEDIO DE PAGO RECARGABLE: SALIDA INVALIDA

ID_Prueba	1.23.2
Propósito	Garantizar que el usuario del medio de pago recargable no pueda salir del sistema de transporte si no hay registro de pago previo.
Configuración	
Condiciones previas	El medio de pago fue previamente aceptado para entrada al sistema
Acciones del test	Acercar el medio de pago a un equipo de aceptación de medios de pago
Resultados	▪ Se niega al usuario la salida del sistema
Observaciones	

10.3.1.10 Aceptación para salida del medio de pago no recargable

ACEPTACIÓN PARA SALIDA MEDIO DE PAGO PRECARGADO: SALIDA VALIDA

ID_Prueba	1.24.1
Propósito	Garantizar que el usuario del medio de pago precargado pueda salir del sistema de transporte
Configuración	
Condiciones previas	El medio de pago fue previamente aceptado para entrada al sistema
Acciones del test	Acercar el medio de pago a un equipo de aceptación de medios de pago

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

Resultados	▪ Se permite al usuario salir del sistema ▪ Se escriben los datos en el medio de pago con TipoEvento = 7.
Observaciones	

ACEPTACIÓN PARA SALIDA MEDIO DE PAGO PRECARGADO: SALIDA INVALIDA

ID_Prueba	1.24.2
Propósito	Garantizar que el usuario del medio de pago precargado no pueda salir del sistema de transporte si no hay registro de pago previo.
Configuración	
Condiciones previas	El medio de pago fue previamente aceptado para entrada al sistema
Acciones del test	Acercar el medio de pago a un equipo de aceptación de medios de pago
Resultados	▪ Se niega al usuario la salida del sistema
Observaciones	

10.3.2 Escenarios de pruebas del subproceso 2

10.3.2.1 Intercambio de archivos entre niveles 3 y 4

ID_Prueba	2.3.1
Propósito	Garantizar que la Cámara de Compensación y los demás Operadores de Recaudo reciban la información asociada a todos los eventos ejecutados por un Operador de Recaudo referentes a la aceptación de medios de pago
Configuración	Se requiere información de los mismos medios de pago usados en las pruebas del subproceso 1
Condiciones previas	Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago
Acciones del test	1. La empresa operadora de recaudo debe recrear la información que debería enviar dados los tipos de casos de uso a probar (Ver hoja ***Aceptación de medios de pago*** del anexo [30]). 2. Posteriormente, debe generar el archivo XML y enviarlo a la Cámara de Compensación

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

3. Para los casos con acciones de lista, la Cámara de Compensación deberá enviar los eventos de difusión o de confirmación a los demás operadores.
4. Verificar la validez de las firmas generadas

Resultados

Todos los destinatarios reciben el archivo de la siguiente forma:

- Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento.
- El número de eventos corresponde con la cantidad enviada y con lo indicado en la hoja ***Aceptación de medios de pago***
- El encabezado de los eventos debe corresponder con lo siguiente:
  - Fecha exacta de supuesta ocurrencia del evento
  - IdSAM otorgado por el Registrador
  - Número secuencial dependiendo del orden de ocurrencia del evento.
- Firma válida generada por la empresa operadora de recaudo

Observaciones

10.3.3 Escenarios de pruebas del subproceso 3

10.3.3.1 Integración de pruebas de subprocesos 1 y 2

ID_Prueba 3.3.1

Propósito Garantizar que todos los procesos relacionados con la aceptación de medios de pago sean ejecutados correctamente desde la interacción con el medio de pago hasta el envío de eventos a la Cámara de Compensación y a los otros Operadores de Recaudo

Configuración

Condiciones previas Se debe tener en cuenta la información entregada por el Registrador sobre los campos del medio de pago

Acciones del test

1 Se ejecutan todas las pruebas del subproceso 1 en concordancia con la hoja ***Aceptación de medios de pago*** del anexo 8 [29]
2 Verificar la validez de las firmas de los archivos recibidos

Resultados

1 La Cámara de Compensación recibe un archivo por la entidad emisora, el cual llega de la siguiente forma:

- Encabezado del archivo en concordancia con lo establecido en la sección 5.3 de este documento.
- El número de eventos corresponde con la cantidad enviada y con lo establecido en la hoja ***Aceptación de medios de pago***
- El encabezado de los eventos debe corresponder con lo siguiente:
  - Fecha exacta de ocurrencia del evento
  - IdSAM otorgado por el Registrador
  - Número secuencial dependiendo del orden de ocurrencia del evento
- Firma válida generada por los actores de la red

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

2. El medio de pago cambia de acuerdo con Los resultados esperados de las pruebas del subproceso 1que se presentan en la hoja ***Aceptación de medios de pago***

Observaciones

11 Anexos

11.1 Definiciones Mapping

Este documento contiene la estructura específica de cada aplicación y de los archivos contenidos por éstas. Adicionalmente incluye definiciones para cada dato presente en los distintos archivos de cada aplicación.

11.2 Mapping

Este documento incluye la información general de la estructura de archivos por aplicación de manera resumida. Contiene información cómo: tipo de archivo, tamaño de archivo en bytes, permisos de acceso e identificadores únicos para cada archivo.

11.3 Eventos

Documento que incluye las directrices para la construcción de esquemas de información en formato XML para la creación de los archivos de eventos. Este archivo de formato XSD puede ser usado para la validación de los archivos XML.

11.4 Eventos con firma

Incluye la misma información que el anexo de Eventos pero ejemplifica cómo se incluye una forma digital en un documento de formato XML.

11.5 CRL

Documento XSD que indica las directrices para la construcción de archivos de revocación de certificados. Puede ser usado para la verificación de los archivos XML que se construyan a partir de estas directrices.

11.6 Formatos generales para el protocolo de pruebas

Este anexo incluye los formatos que se usarán para registrar los protocolos de pruebas.

11.7 Ejemplos de los cambios en el medio de pago

Este anexo documenta los cambios de cada uno de los archivos de la aplicación interoperable para cada transacción definida en el manual de normatividad técnica.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

11.8 Escenarios de prueba para los subprocesos 2 y 3

Este anexo documenta que eventos deben incluirse en el archivo de eventos que se genera al ejecutar cada transacción y caso de uso definido en el manual de normatividad técnica.

11.9 Parámetros días

Este anexo contiene dos archivos. En primer lugar se tiene el archivo XSD, éste determina las directrices para la creación del archivo de tipos de día, el cual es usado para obtener el tipo de día de acuerdo al número del día del año, de esta forma se pueden establecer tarifas diferenciadas por tipo de día, sea día normal, feriado o especial (i.e. cívico). El archivo XML que se incluye es un ejemplo de cómo se puede generar este archivo para un año determinado.

11.10 Parámetros tarifas

Este anexo también incluye dos archivos. El archivo XSD determina las directrices para crear el archivo de configuración de tarifas y puede ser usado para la validación del mismo. El archivo XML que se incluye es un ejemplo en el que se muestra cómo se implementan diferentes esquemas tarifarios y cómo se puede controlar el uso de productos mediante las reglas de validez de un producto.

11.11 Parámetros terminal

Al igual que los dos anexos anteriores se incluyendo archivos, el archivo XSD marca las directrices para la creación del archivo de información de terminal y el archivo XML ejemplifica el uso de este archivo para el control de identificadores dentro del sistema.

11.12 SAMs

Este anexo incluye cada una de las SAMs, asignando las llaves del sistema y llaves de trabajo correspondientes. Este anexo también posee dos formatos dónde se definen los parámetros de cada llave de trabajo y de sistema, la especificación de estos parámetros puede encontrarse en el capítulo 7 de [11]. Finalmente, este anexo define un formato que asigna los contadores de cada módulo SAM a los eventos que debe registrar.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

12 Referencias

[1] ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013.

[2] CNA, Calypso Specification Rev. 3.1 Ref: 060708-CalypsoAppli, Editado por Spirtech, 2013.

[3] NXP, Data sheet - MF0ULx1 MIFARE Ultralight EV1 - Contactless ticket IC Rev 3.1, 2014.

[4] Concejo del Municipio del DMQ, Ordenanza Metropolitana 0201 del 8 de febrero de 2018, Quito, 2018.

[5] Anexo 1. Definiciones de datos para aplicación interoperable en medios de pago Calypso Rev. 3.1, 2018.

[6] ISO/IEC, ISO/IEC 7816-5- dentification cards -- Integrated circuit cards -- Part 5: Registration of application providers, 2004.

[7] BSI, BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements, 2005.

[8] BSI, BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists, 2005.

[9] ISO, ISO/DIS 8601-1: Data elements and interchange formats— Information interchange— Representation of dates and times—, 2016.

[10] Anexo 2. Resumen de la estructura de datos para la aplicación interoperable del SITMQ., 2018.

[11] Calypso, Secure Application Module SAM-C1: 101010-SamCalypso-16, Spirtech, 2018.

[12] Anexo 9. Archivo de parámetros DIAS.xml., 2018.

[13] Anexo 10. Archivo de parámetros TARIFAS.xml, 2018.

[14] Anexo 11. Archivo de parámetros TERMINAL.xml., 2018.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com

[15] BSI, BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements, 2005.

[16] Anexo 4. Esquema de envío de eventos con firma digital., 2018.

[17] Anexo 3. Esquema para envío de eventos., 2018.

[18] BSI, BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists, 2005.

[19] ITU-T, Recomendación X.509.

[20] «W3C Recommendation: XML Signature Syntax and Processing (Second Edition),» 10 junio 2008. [En línea]. Available: http://www.w3.org/TR/xmldsig-core/.

[21] Anexo 5. Esquema para la lista de revocación de certificados (CRL), 2018.

[22] Calypso, Security Architecture and Key Ceremony - 170202-KeyArchitecture-10, SNCF, 2018.

[23] E. Barker y N. Mouha, SP 800-67 Rev. 2: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017.

[24] Anexo 12. Parámetros de módulos SAM., 2018.

[25] Spirtech, «Secure Application Module SAM-C1,» 2018. [En línea]. Available: http://spirtech.com/docs/Products/SAM-C1/en/SamC1-v1.pdf.

[26] Anexo 3. Esquema de envío de eventos con firma digital, 2015.

[27] Anexo 6. Documentación para ejecución de pruebas., 2018.

[28] Anexo 7. Ejemplos de los cambios en el medio de pago para subproceso 1, 2018.

[29] Anexo 8. Escenarios de prueba para subprocesos 2 y 3, 2018.

[30] Anexo 8. Documentación para protocolos de pruebas de subproceso S2 y S3., 2018.

[31] Common Criteria, Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 4, 2012.

www.gsdplus.com
Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

[32] ISO/IEC, ISO/IEC 14443-1 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics, 2016.

[33] ISO/IEC, ISO/IEC 14443-2: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface, 2016.

[34] ISO/IEC, ISO/IEC 14443-3: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision, 2011.

[35] ISO/IEC, ISO/IEC 14443-4: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol, 2016.

[36] ABIresearch, «ABI Research Forecasts Global Contactless Ticketing Shipments to Top 460 Million in 2017,» Feb 2017. [En línea]. Available: https://goo.gl/igfGrx.

[37] CNA, Calypso Handbook - Ref: 100324-CalypsoHandbook-11, 2010.

[38] ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013.

[39] Global Platform, Card Specification v.2.3, 2015.

[40] Arjo Systems (HID Global), SOMA ATLAS - User Manual Calypso Specification Rev. 3.1 v. 1.2, 2016.

[41] ISO/IEC, ISO/IEC 9798-2 Information technology — Security — Part 2: Mechanisms using symmetric encipherment algorithms, 1999.

[42] Gemalto, «Gemalto Calypso G1,» 2018. [En línea]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/transport-celego-calypso.pdf.

[43] HID Global, «MIFARE DESFire EV1 Credentials,» 2010. [En línea]. Available: https://www.hidglobal.com/sites/default/files/resource_files/mifare-desfire-ev1-card-ds-en.pdf.

[44] Spirtech, Stored Value Guidelines, 2016.

[45] Calypso, Calypso Security White Paper, Ref: 080131-CalypsoSecurity, Spitech, 2012.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792

[46] NXP, Data sheet - MF3ICD81 MIFARE DESFire EV1 Rev. 3.6 document number 134036, 2011.

[47] NXP, «Registered Partners,» 2018. [En línea]. Available: https://www.mifare.net/en/.

[48] Gemalto, «Contactless EMV cards,» Octubre 2017. [En línea]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/fs-contactless-EMV-cards.pdf.

[49] Calypso, Calypso vs. EMVCo CL L1 Specifications v1.00, Galitt, 2007.

[50] Calypso, Application Downloading, Trusted Labs, Spirtech, 2011.

[51] NXP, NXP J3D081_M59_DF, and J3D081_M61_DF Secure Smart Card Controller Rev. 2, 2013.

[52] NXP, P5DF081 MIFARE SAM AV2 functional specification, document number 191732.

[53] CNA, «Calypso Networks Association - Membership,» 2018. [En línea]. Available: https://www.calypsonet-asso.org/content/membership.

[54] Calypso, Calypso Host Card Emulation Application Version 1.2, Ref: 141113-CalypsoHCEApplication, Spirtech, 2016.

[55] Concejo del Municipio del DMQ, Ordenanza Metropolitana No. 54 del 2 de abril de 2015, Quito, 2015.

[56] Anexo 7. Documentación para protocolo de pruebas del subproceso S1., 2018.

[57] Anexo 5. Documentos para ejecución de pruebas, 2015.

Carrera 11 N° 79-52 Of. 601
Bogotá D.C. – Colombia
Tel: +57 (1) 9277792
www.gsdplus.com