# MANUAL DE ESPECIFICACIONES TECNICAS PARA EL SISTEMA INTEROPERABLE DE PAGO ELECTRONICO DEL ESTADO DE JALISCO

RELEASE 2

# CONTENIDO

# Tabla de figuras

# 1 Introducción

El presente documento contiene la **definición técnica** que reglamenta la tecnología que se debe usar en el Estado de Jalisco para la implementación de un modelo de interoperabilidad en sistemas de recaudo. En este documento se define la tecnología de los medios de pago, la estructura de la información que se debe almacenar en los mismos, las reglas de uso de los medios de pago y un protocolo de comunicación entre los actores que participan en la red interoperable de Jalisco.

## 1.1 Glosario

**AES:** Advanced Encryption Standard (Estándar avanzado de cifrado)

**AID:** Identificador de aplicación en el medio de pago.

**Aplicación:** estructura de datos dentro de un medio de pago que define archivos, codificaciones y reglas de uso.

**Cámara de compensación:** sistema de control y compensación, para la liquidación y distribución de las operaciones derivadas de las transacciones diarias efectuadas por el pago de la tarifa en la red interoperable.

**DF:** Dedicated File, es un archivo contenedor de otros DF o EF

**EF:** Elementary File, archivo que almacena datos. NO posee sucesor y sus atributos de seguridad pueden ser asignados de manera individual.

Evento: operación básica efectuada sobre la aplicación interoperable.

**LAM:** Lista de Acción para Medios de pago interoperables

**LAP_R:** Lista de Acción para productos en dispositivos de Recarga

**LAP_V:** Lista de Acción para Productos en dispositivos de Validación

**Llave:** secreto que comparten varios elementos de un sistema que es utilizado para efectuar operaciones de seguridad.

**Medio de pago:** instrumento electrónico con el cual el usuario puede obtener el servicio de transporte público mediante el pago de la tarifa en la red interoperable

**Operación:** acción llevada a cabo por un usuario o una entidad que conlleva a la ocurrencia de un conjunto de eventos.

**Producto:** conjunto de reglas comerciales que se almacenan en un medio de pago y cuya ejecución y uso permite prestar un servicio

**SAM:** módulo de acceso seguro. Usado para almacenar llaves y efectuar operaciones criptográficas con los medios de pago, permite a su vez, la comunicación segura entre terminal y backend.

**Tarifa:** unidades de valor que se descuentan de un producto en transacciones de validación. Dichas unidades son determinadas para cada usuario según las condiciones que se definan

Usuario: persona que utiliza el sistema integrado de recaudo

**Validación:** uso de un producto para acceder a un servicio

**Viaje:** conjunto de validaciones que transportan al usuario desde el principio de su recorrido hasta el final del mismo.

**Ventana de Transbordo:** La ventana de transbordo se define como el cumplimiento de todas las condiciones necesarias, temporales y de sentido de viaje, para recibir el beneficio de una tarifa de transbordo durante un viaje

## 1.2 Representación de los datos

La información numérica consignada en este documento está expresada en formato hexadecimal si el dato incluye el prefijo "0x". En caso en que el dato expresado conste de más de dos (2) bytes, la representación es realizada en el sistema Big-Endian. Por el contrario, si el dato está expresado en formato decimal, este no incluye ningún prefijo. El siguiente ejemplo presenta las dos posibles representaciones del mismo número en este documento.

| Decimal | Hexadecimal |
|---|---|
| **651316845** | 0x26D24E6D |

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 (hex) |
|---|---|---|---|
| **6333** | 13 | 2 | 0x18BD |

## 1.3 Especificaciones de la tarjeta MIFARE DESFire EV1 y EV2

El modelo de datos descrito en este documento se basa en el medio de pago MIFARE DESFire EV1 (NXP, Data sheet - MF3ICD81 MIFARE DESFire EV1 Rev. 3.6 document number 134036, 2011) y MIFARE DESFire EV2 (NXP, Data sheet - MF3D(H)x2 MIFARE DESFire EV2 Rev. 3.2 document number 364232, 2019). Esta tecnología es totalmente compatible con las 4 partes del estándar ISO/IEC 14443A (ISO/IEC, ISO/IEC 14443-4 Identification cards - Contactless integrated circuit cards - Proximity cards - Part4: Transmission protocol, 2008).

MIFARE DESFire EV2 cuenta con un modo de compatibilidad con versiones anteriores para MIFARE DESFire EV1 y D40 (MF3ICD40) siendo este el modo en el que operara la tarjeta EV2

Adicionalmente MIFARE DESFire EV1 define mecanismos para las siguientes acciones:

Flujo de comunicación segura entre los medios de pago y los lectores de medios de pago.

Manejo de la colisión de medios de pago para permitir el manejo de más de una tarjeta MIFARE DESFire EV1 y EV2 en un campo al mismo tiempo.
Manejo de la integridad de los datos en los casos en que se remueve la tarjeta de un campo antes de terminar una escritura de datos.
Transmisión de datos orientada a archivos.
Manejo de la seguridad de archivos basada en un esquema de llaves de aplicación.

Por otra parte la tarjeta consta de las siguientes especificaciones basadas en estándares abiertos:

Nombres de archivos basados en ISO 7816
Esquema de seguridad basado en AES (FIPS PUB 197 Advanced Encryption Standard (AES), 2001) o 3DES
Comandos de manejo de archivos basados en ISO 7816-4 (ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013)

Un medio de pago MIFARE DESFire EV1 puede almacenar hasta 28 directorios, llamados aplicaciones. Estos se distinguen en este documento por el sufijo "DF" del inglés *Dedicated File*. Cada aplicación consta de un Identificador de Aplicación (AID) de 3 bytes y un identificador de archivo de 2 bytes según ISO 7816-4 (ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013).

Cada aplicación puede almacenar hasta 32 archivos elementales. Estos se distinguen en este documento por el sufijo "EF" del inglés *Elementary File*. Por último cada aplicación puede almacenar de forma segura hasta 14 llaves numeradas desde 0 hasta 13 y dos opciones adicionales – "free" y "never". La llave 0 se denomina *llave maestra de aplicación* la cual permite realizar operaciones especiales según la configuración de la aplicación.

Los archivos EF dentro de una aplicación en el medio de pago pueden ser de los siguientes tipos:

Archivos estándar: almacenan una secuencia plana de datos.
Archivos de datos con backup: almacenan una secuencia plana de datos. Cuentan con el mecanismo de manejo de la integridad de archivos en transacciones.
Archivos de valor: están destinados a almacenar una cantidad o un monto. Disponen de comandos específicos para su manipulación (aumentar o disminuir su valor.
Archivos de registro lineales: constan de una secuencia fija de registros con un tamaño definido.
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.

Por último un medio de pago MIFARE DESFire EV1 siempre incluye un directorio maestro que almacena una única llave maestra denominada *PICC key*. La autenticación con dicha llave permite crear y borrar aplicaciones, así como borrar por completo la información del medio de pago.

# 2 Interoperabilidad

El modelo de interoperabilidad presentado en este documento está basado en el **estándar ISO 24014 parte 1 (ISO, 2007)**. Una red interoperable se define como un sistema en el que existe un conjunto mínimo de medios de pago que son aceptados por múltiples prestadores de servicios independientemente del emisor de dichos medios de pago.

## 2.1 Actores de la red interoperable

Siguiendo el modelo pueden existir los siguientes actores:

**Comité rector**: es la entidad encargada de emitir y actualizar las reglas técnicas y comerciales de la red interoperable, supervisar el cumplimiento de las reglas que emite, adherir y retirar entidades de la red, y supervisar la operación de la Cámara de compensación. Cumple el rol de propietario de aplicación.

**Comité Técnico:** es la entidad encargada de supervisar la calidad de servicio que deberán cumplir los actores del entorno interoperable, definir las políticas y condiciones de servicio, determinar las politicas de sanciones, instruir al fiduciario para que destine los recursos ingresados al FIDEICOMISO MAESTRO, instruir al fiduciario para que haga la dispersión de los recursos recaudados y vigilar el debido cumplimiento de los fines del FIDEICOMISO MAESTRO.

**Cámara de compensación**: es la entidad encargada de interconectar a todas las entidades de la red interoperable, realiza la recolección de la información transaccional de toda la red y genera las órdenes de pago para el cruce de cuentas entre entidades.

**Emisores de medios de pago**: son las entidades autorizadas por el Comité rector para fabricar, programar y emitir medios de pago con la aplicación interoperable descrita en este documento.

**Distribuidores de productos**: son las entidades autorizadas por el Comité rector para almacenar un conjunto de productos en los medios de pago con la aplicación interoperable. Además están autorizados para hacer recargas de valor a los productos que distribuyen.

**Prestadores de servicio**: son las entidades autorizadas por el Comité rector para hacer uso de productos en transacciones de validación para prestar un servicio dentro de la red interoperable.

## 2.2 Especificaciones de la red interoperable

Dada una definición y unas entidades participantes de la red interoperable, esta debe cumplir con las siguientes características:

Pueden existir múltiples emisores de medios de pago.

Los medios de pago pueden almacenar múltiples productos para acceder a servicios de los prestadores de servicio.

Pueden existir múltiples distribuidores de productos para los medios de pago.

Existe independencia entre la emisión de un medio de pago y la distribución de los productos que puede almacenar un medio de pago.

Existe una definición común de la estructura de datos de los medios de pago denominada aplicación interoperable.

Existe una definición común de los productos que se pueden ofrecer en los medios de pago. Estos se almacenan dentro de la aplicación interoperable.

Los usuarios pueden hacer validaciones en toda la red interoperable para acceder a los servicios prestados según las reglas definidas por el Comité rector.

Los usuarios pueden hacer recargas de valor a sus productos a través de distribuidores de productos autorizados para cada produto

## 2.3 Certificaciones de operadores tecnológicos para incorporación al SIR

Para integrarse en la red interoperable es necesario cumplir con los requisitos establecidos en el manual de procesos y aprobar las pruebas que se apliquen para la certificación de los niveles 0-1 y 3-4

## 2.4 Especificación de alcances mínimos de equipos y servicios prestados por el operador tecnológico a cada EUR

Las especificaciones técnicas de los alcances mínimos tanto de hardware como de software que deberán suministrar los operadores tecnológicos para cada uno de los EUR (EUR TREN, EUR MASIVO y EUR COLECTIVO), están detalladas en el CATALOGO DE ESPECIFICACIONES TECNICAS POR EUR. Dicho catálogo se actualizará periódicamente donde el último publicado será el vigente.

# 3 Tipos de productos

Los medios de pago deberán tener la capacidad de almacenar como mínimo cuatro productos: un monedero, un producto de viaje a crédito,un producto de BPD y un producto BPD2. Cada uno de estos productos debe ser único en un medio de pago, por lo que solo se debe cargar una instancia de cada uno en el mismo.

## 3.1 Producto Monedero.

Permite hacer la validación para el pago de un pasaje. Este producto almacena un valor positivo equivalente a la cantidad de dinero que un pasajero recaga en algún dispositivo del sistema interoperable y luego se actualiza debitando del mismo los valores de las transacciones de pago que se realicen. La cantidad que puede contener este producto es limitada por el parámetro máximo que se permita almacenar, dictado por la gerencia del sistema interoperable, este producto puede trabajar combinado con el producto de crédito para completar el pago de un pasaje si la gerencia dictamina que esta regla pueda aplicarse y el producto de crédito existe. Su valor minimo es 0

## 3.2 Validación a crédito

Permite hacer una validación aun cuando el valor del pago es inferior al valor de la tarifa aplicada. Este almacena un valor que se hace negativo una vez se usa el producto en una transacción de validación, y vuelve a cero cuando se paga el valor negativo acumulado en una transacción de recarga. La activación de la validación con crédito solo se maneja con el monedero y la funcionalidad de que las reglas de operación lo contemplen activo para aplicarlo

En un evento de recarga del monedero tendrá prioridad el pago del crédito, el restante se agregara al producto Monedero

### 3.3 BPD (Boletos para Descuento)

Este almacena un número de viajes disponibles en su archivo de valor. El producto puede restringir la forma de usar los viajes según los días de la semana, la hora y el número de viajes al día. La prioridad de este producto es superior a la prioridad del monedero y el viaje a crédito. Por lo tanto si existen viajes disponibles de BPD y se cumplen las condiciones de uso, siempre se debe usar este producto en una validación.

# 4 Modelo de seguridad en nivel 0-1

El modelo de seguridad definido para la comunicación entre los medios de pago (nivel 0) y los lectores de medios de pago (nivel 1) está basado en criptografía simétrica. En este modelo los dos dispositivos deben compartir un secreto denominado llave. La tecnología MIFARE DESFire EV1 y DESFIRE EV2 emulando EV1 (NXP, Data sheet - MF3ICD81 MIFARE DESFire EV1 Rev. 3.6 document number 134036, 2011) define cómo se debe hacer uso de las llaves para garantizar confidencialidad e integridad de la información. Además se define un protocolo de autenticación mutua entre medios de pago y lectores para verificar la veracidad de cada uno de ellos.

Por otra parte, el almacenamiento y uso de las llaves por parte de los lectores de medios de pago debe ser realizado a través de módulos de acceso seguro (SAM) (NXP, P5DF081 MIFARE SAM AV2 functional specification, document number 191732). Los SAM se comunican con los lectores de medios de pago y ejecutan procesos tales como autenticación mutua con el medio de pago, generación y verificación de códigos de autenticación de mensajes (MAC) (ISO/IEC, ISO/IEC 9797-1 Information technology -- Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011), y finalmente cifrado y descifrado de datos.

Esta norma exige el uso del esquema de cifrado por bloques AES definido en el estándar FIPS PUB 197 (FIPS PUB 197 Advanced Encryption Standard (AES), 2001). Por lo tanto, la comunicación llevada a cabo entre un SAM y un medio de pago debe hacer uso de AES utilizando un bloque de cifrado de 128 bits. Las operaciones de seguridad que se derivan del uso de AES-128 deben seguir la especificación de MIFARE DESFire EV1. Adicionalmente las llaves que se almacenan en los medios de pago deben ser diversificadas de tal forma que estas son únicas dentro de toda la red interoperable.

# 5 Diversificación de llaves

Todas las llaves a almacenar en los medios de pago deben ser diversificadas. Esto significa que cada llave que se almacena en un medio de pago debe ser inferida en un SAM emitido por la Direccion del Sistema Integrado de Recaudo mediante una función de

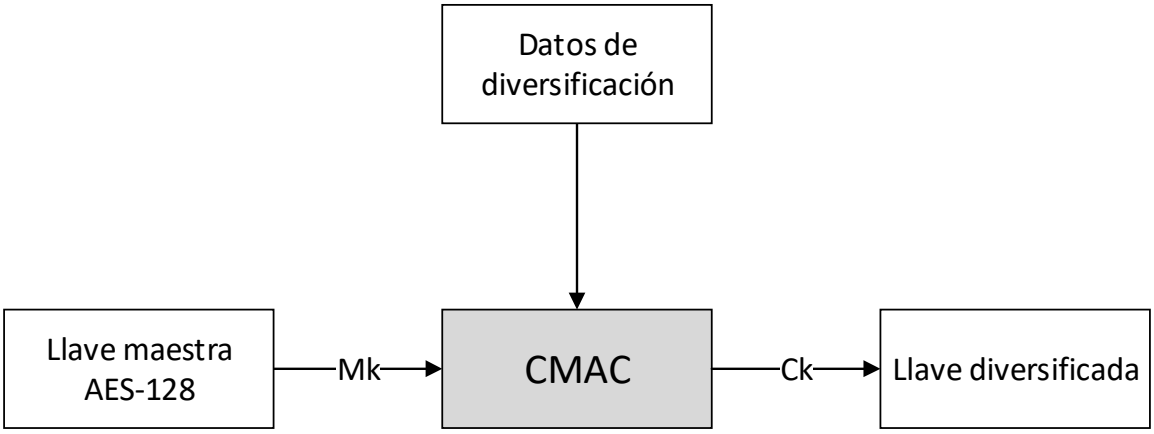
diversificación. La función de diversificación a usar debe ser la función CMAC según la NIST Special Publication 800-38B (NIST, 2005) y siguiendo las recomendaciones definidas en el documento Symmetric key diversifications de NXP (NXP, Symmetric key diversifications AN10922 Rev 1.3, 2010) para llaves AES-128.

Los datos de diversificación se componen por los siguientes elementos:

$$Datos\ de\ diversificación = 0x01||UID||ID\_App||ID\_Sistema$$

La generación de una llave diversificada se realiza como se muestra en la siguiente figura:

**Figura 1 – Función de diversificación de llaves**




La llave diversificada Ck debe ser única para cada medio de pago. Esta debe derivarse mediante el cálculo de un CMAC, el cual utiliza los siguientes parámetros:

Llave maestra Mk almacenada en el SAM.
Datos de diversificación = 0x01 || UID ||ID_App||ID_Sistema

Donde:

UID = Identificador único del medio de pago
ID_App = Identificador de la aplicación en la cual se encuentra la llave. El valor de ID_App para el directorio raíz es 0x000000
ID_Sistema = valor asignado para el estado de Jalisco

# 6 Aplicación interoperable en medios de pago MIFARE DESFire EV1

## 6.1 Introducción

El presente capítulo está compuesto por una definición general y una definición detallada de la información que se debe almacenar en los medios de pago MIFARE DESFire EV1 de la red interoperable de Jalisco. La definición general presenta los archivos que debe contener el medio de pago. La definición detallada presenta la información que debe contener cada uno de los archivos presentados en la definición general. Esta definición incluye una asignación de cada tipo de dato y una representación del mismo con base en los estándares BS EN 1545-1:2005 (BSI, BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements, 2005) y BS EN 1545-2:2005 (BSI, BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists, 2005).

## 6.2 Especificaciones generales de la estructura de archivos

La estructura de archivos interoperable de Jalisco está compuesta por dos aplicaciones: la aplicación/directorio raíz y la aplicación interoperable. La aplicación interoperable corresponde a un directorio DF que contiene un conjunto de archivos EF. La siguiente tabla presenta la estructura general de los archivos que pueden ser almacenados en el medio de pago. Los elementos resaltados en gris representan directorios/aplicaciones según la definición de ISO 7816-4 (ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013) y MIFARE DESFire EV1

| # aplicación | Nombre de archivo/directorio | Tipo |
|---|---|---|
| **0x000000** | Directorio raíz | DF |
| | Llave maestra | Llave |
| **0x484000** | Jalisco_DF | DF |
| | Llaves (13) | Llave |
| | Emisión_EF | Estándar |
| | Entorno_EF | Estándar |
| | Usuario_EF | Estándar |

| | | |
|---|---|---|
| | Funcionario_EF | Backup |
| | EstadoAplicación_EF | Backup |
| | ListaProductos_EF | Backup |
| | Eventos_EF | Cíclico |
| | ContratoMonedero_EF | Estándar |
| | ServicioMonedero_EF | Backup |
| | ValorMonedero_EF | Valor |
| | ContratoCrédito_EF | Estándar |
| | ServicioCrédito_EF | Backup |
| | ValorCrédito_EF | Valor |
| | ContratoBPD_EF | Estándar |
| | ServicioBPD_EF | Backup |
| | ValorBPD_EF | Valor |
| | ContratoBPD2_EF | Estandar |
| | ServicioBPD2_EF | Valor |
| | ValorBPD2_EF | Backup |

Las siguientes secciones presentan las especificaciones y la funcionalidad de cada uno de los archivos presentados en esta definición general.

## 6.3 Directorio raíz del medio de pago

Este directorio siempre está presente en los medios de pago MIFARE DESFire EV1. Cuando un medio de pago es energizado, este directorio es seleccionado por defecto.

El directorio raíz debe ser modificado de tal forma que cuente con las siguientes especificaciones:

AID: 0x000000
Configuración modificable.
No se permite la creación/eliminación de aplicaciones sin previa autenticación con la llave maestra.
Libre acceso a la lista de aplicaciones.
Número de llaves: 1 (llave maestra).

La llave maestra del directorio raíz es igual a la llave 0 del directorio Jalisco_DF. Esta llave es propiedad del Sistema Integrado de Recaudo y se hace disponible a las entidades encargadas de emitir medios de pago. La llave maestra debe ser cargada al momento de inicialización del medio de pago, y sus parámetros deben ser modificados para operar usando AES-128.

## 6.4 Directorio Jalisco_DF

Este directorio corresponde a la aplicación interoperable. Este almacena toda la información que permite la prestación del servicio de transporte en la red interoperable. El directorio Jalisco_DF consta de las siguientes especificaciones:

AID: 0x484000
Identificador de archivo ISO: 0x4840
Se requiere autenticación con la llave a ser cambiada para modificar dicha llave
Configuración de la aplicación modificable
No se permite la creación/eliminación de archivos sin previa autenticación con la llave maestra
Libre acceso a la lista de archivos
Se permite modificar la llave maestra
Herramienta criptográfica: AES-128
Soporte para nombres de archivo ISO
Número de llaves: 14

Este directorio debe contener obligatoriamente los siguientes archivos:

Emisión_EF
Entorno_EF
Usuario_EF
EstadoAplicación_EF
ListaProductos_EF
Eventos_EF

Adicionalmente según la funcionalidad requerida, este directorio puede contener alguno de los siguientes archivos:

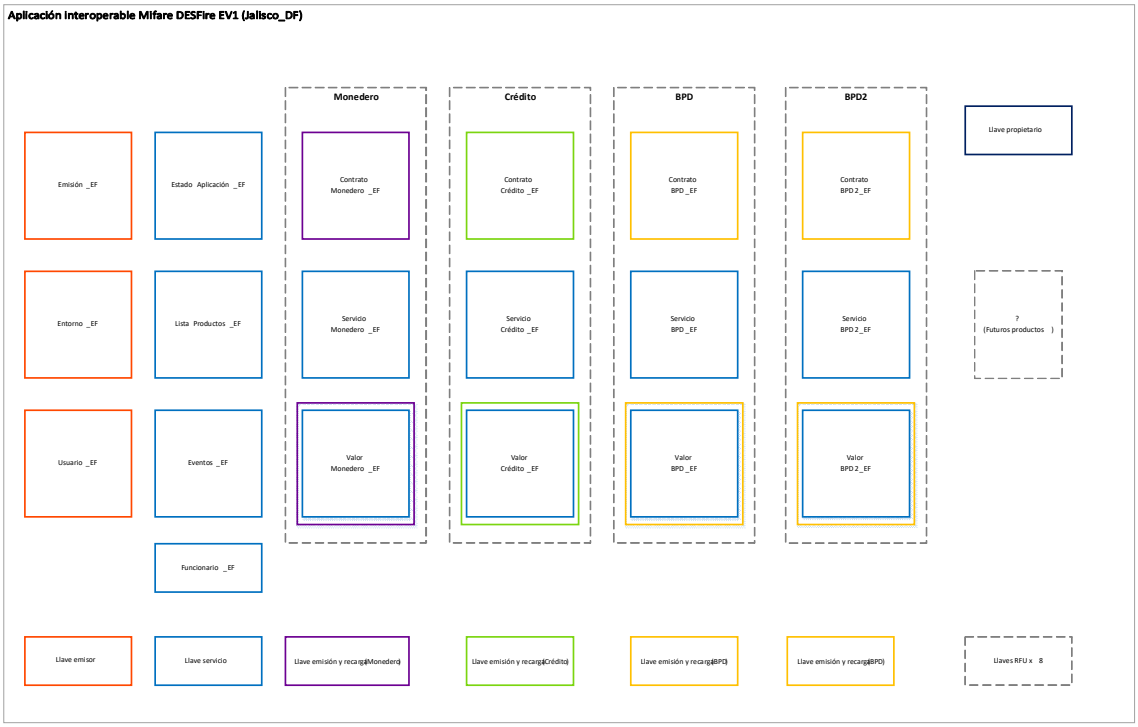
ContratoMonedero_EF

ServicioMonedero_EF
ValorMonedero_EF
ContratoCrédito_EF
ServicioCrédito_EF
ValorCrédito_EF
ContratoBPD_EF
ServicioBPD_EF
ValorBPD_EF
Funcionario_EF

ContratoBPD2_EF
ServicioBPD2_EF
ValorBPD2_EF

Con base en lo anterior, la estructura de archivos de una aplicación que almacena los tres productos disponibles en la red interoperable se representa a continuación.

**Figura 2 – Estructura de archivos de la aplicación interoperable**




### 6.4.1 Archivo Emisión_EF

Este archivo se encarga de almacenar toda la información invariable relacionada con el emisor del medio de pago. Este archivo se crea durante el proceso de inicialización o emisión y nunca debe ser modificado una vez el medio de pago entra en circulación.

La configuración del archivo Emisión_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x01
Identificador de archivo ISO: 0x0001
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave E (posición # 1)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 48 bytes

## Descripción de la estructura del Archivo de Emisión

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **País** | CountryNumeric | 10 | 2 | Según ISO 3166-1 |
| **SerialMedioPago** | SerialNumber | 32 | 4 | Número serial identificador del medio de pago en la red interoperable |
| **FechaFinValidezMedioPago** | EndDate | 16 | 2 | El día en que el medio de pago ya no es válido |
| **PropietarioAplicación** | ApplicationOwner, SEQUENCE | | | Entidad que emite y controla la especificación de la aplicación. Equivale al Comité rector |
| **IdRed** | NetworkId | 24 | 3 | Identificador de la red a la cual pertenece el propietario de la aplicación. Asignado por el Registrar |
| **IdPropietario** | CompanyId | 16 | 2 | Identificador de la entidad propietaria de la aplicación |

| | | | | |
|---|---|---|---|---|
| **EmisorAplicación** | ApplicationOwner, SEQUENCE | | | Entidad autorizada para emitir la aplicación interoperable |
| **IdRed** | NetworkId | 24 | 3 | Identificador de la red a la cual pertenece el emisor de la aplicación. Asignado por el Registrar |
| **IdDistribuidor** | CompanyId | 16 | 2 | Identificador de la entidad que emite la aplicación |
| **VersiónSeguridad** | SecurityVersion, SEQUENCE | | | |
| **IdSAM** | ReferenceIdentifier | 56 | 7 | Identificador del SAM usado en la emisión del medio de pago. Este campo corresponde al UID del SAM según la especificación de NXP SAM AV2 (NXP, P5DF081 MIFARE SAM AV2 functional specification, document number 191732) |
| **IdAlgSeguridad** | AlgorithmId | 12 | 2 | Permite identificar el algoritmo de seguridad usado en el medio de pago. Asignado por el Registrar |
| **IdVersiónLlaves** | KeyVersionNumber | 8 | 1 | Indica la versión de las llaves asignadas en el medio de pago. Asignado por el Registrar |
| **RFU** | | | 20 | Reservado para uso futuro |

| | | | | |
|---|---|---|---|---|
| | | | **48** | **Tamaño total** |

### 6.4.2 Archivo Entorno_EF

El archivo Entorno_EF almacena las variables que indican cuál es la red interoperable donde es aceptada la aplicación interoperable.

La configuración del archivo Entorno_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x02
Identificador de archivo ISO: 0x0002
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave E (posición # 1)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 24 bytes

**Descripción de la estructura del archivo Entorno_EF**

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **VersiónAplicación** | VersionNumber | 8 | 1 | Se refiere a la versión de la aplicación interoperable. 4 primeros bits vara versión mayor y siguientes 4 bits para versión menor. La versión inicial debe ser 1.0. (0x10) |
| **IdRed** | NetworkId | 24 | 3 | Red interoperable de origen del medio de pago. Permite determinar si el medio de pago es aceptado en una red interoperable diferente. |
| **FechaFinValidezAplicación** | EndDate | 16 | 2 | El día en que la aplicación ya no es válida. Representa el número de |

| | | | | |
|---|---|---|---|---|
| | | | | días transcurridos desde el 1 de enero de 1997 |
| **RFU** | | | 18 | Reservado para uso futuro |
| | | | **24** | **Tamaño total** |

### 6.4.3 Archivo Usuario_EF

Este archivo contiene información del propietario del medio de pago en caso en que se desee definir un perfil especial para el mismo. Los perfiles de usuario especial permiten calcular tarifas diferenciadas según el tipo de usuario.

La configuración del archivo Usuario_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x03
Identificador de archivo ISO: 0x0003
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave E (posición # 1)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 96 bytes

**Descripción de la estructura del archivo Usuario_EF**

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **FechaNacimientoUsuario** | BirthDate | 32 | 4 | Valor en BCD (0xYYYYMMDD) |
| **Perfil** | SEQUENCE | | | |
| **CódigoPerfil** | ProfileCodeIOP | 6 | 1 | Código que clasifica el segmento especial al cual pertenece perfil asignado al usuario según los valores definidos para este campo |

| | | | | |
|---|---|---|---|---|
| | | | | en los catalogos del sistema interoperable, que se detallan en el Manual de Procesos. |
| **FechaFinPerfil** | EndDate | 16 | 2 | Fecha de vencimiento de la validez del perfil |
| **NombreUsuario** | Name | 312 | 39 | Nombre del propietario del medio de pago personalizado en codificación UTF8 |
| **CredencialUsuario** | HolderId | 192 | 24 | Indica el código de identificación del usuario en codificación UTF8. Este campo puede corresponder al CURP del usuario o a algún otro documento de identificación. |
| **RFU** | | | 23 | Reservado para uso futuro |
| | | | **96** | **Tamaño total** |

Un medio de pago pertenece a un usuario de segmentos especiales cuando cuando CódigoPerfil es diferente de 0; de lo contrario el medio de pago debe pertenecer a un usuario general. Perfiles adicionales como el perfil de menor de edad verificara además la FechaNacimientoUsuario para determinar si el usuario aun debe recibir el beneficio.

### 6.4.4 Archivo Funcionario_EF

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 emisor de medios de pago puede establecer sus propias reglas de acceso para sus funcionarios, se deja a discreción de cada emisor la estructura de este archivo.

La configuración del archivo Funcionario_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x10
Identificador de archivo ISO: 0x0010
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: nunca

- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

**Descripción de la estructura del archivo Funcionario_EF**

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **DatosPerfilFuncionario** | OCTET STRING | 144 | 23 | Campo destinado a ser usado con funcionarios de la red interoperable. Este campo se deja a discreción de cada emisor de medios de pago en caso en que se desee distinguir entre perfiles de funcionarios o se desee agregar información adicional.<br>Este campo no está destinado a ser interoperable entre emisores de medios de pago o prestadores de servicio. |
| | | | **23** | **Tamaño total** |

### 6.4.5 Archivo EstadoAplicación_EF

Indica el estado de la aplicación interoperable con base en la definición de su ciclo de vida.

La configuración del archivo EstadoAplicación_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x04
Identificador de archivo ISO: 0x0004
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave E (posición # 1)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

## Descripción de la estructura del archivo EstadoAplicación_EF

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **EstadoAplicación** | Integer (0 .. 3) | 2 | 1 | Indica el estado actual de la aplicación interoperable. Los posibles estados están definidos en los catalogos del sistema interoperable, que se detallan en el Manual de Procesos. |
| **ConsecutivoAplicación** | Integer (0 .. 16777215) | 24 | 3 | Corresponde al número de eventos que se han efectuado en el medio de pago. Debido a que una operación efectuada por un usuario puede constar de varios eventos, este número puede aumentar en más de 1 por cada operación. Por ejemplo, una operación de emisión del medio de pago requiere de mínimo 2 eventos: emisión del medio de pago y distribución de un producto. Por lo tanto ConsecutivoAplicación >= 2 una vez el medio de pago entra en circulación. |
| **NúmeroAcciónAplicada** | Integer<br>(0 .. 255) | 8 | 1 | Indica el número acciones que se han aplicado en el medio de pago a través de la lista LAM |
| **RFU** | | | 18 | Reservado para uso futuro |
| | | | **23** | **Tamaño total** |

### 6.4.6 Archivo ListaProductos_EF

Almacena una secuencia de datos que indica los productos almacenados en el medio de pago. Su propósito es determinar cuál es la disponibilidad y prioridad de uso de cada producto.

La configuración del archivo ListaProductos_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x05
Identificador de archivo ISO: 0x0005
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 57 bytes

**Descripción de la estructura del archivo ListaProductos_EF**

**El archivo ListaProductos_EF consta de 8 secciones que forman una secuencia de datos. Cada sector representa la información asociada a un producto. La distribución de las secciones ocurre de la siguiente forma:**

| Sector 1 | Sector 2 | Sector 3 | Sector 4 | Sector 5 | Sector 6 | Sector 7 | Sector 8 |
|---|---|---|---|---|---|---|---|

Todos los sectores que contengan información de la existencia de un producto deberán estar listados de manera consecutiva evitando la existencia de sectores sin información en posiciones intermedias.

La posición de los productos no es definitiva ni exclusiva y esta puede cambiar, por lo que para realizar una transacción es necesario leer por completo el **archivo ListaProductos_EF**

La estructura de datos de cada sector es la siguiente:

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **IdProducto** | ProductId | 16 | 2 | Código que identifica el producto en la red interoperable.<br>Asignado por el Registrar |
| **PunteroContrato** | InstancePointer | 8 | 1 | Indica el identificador de archivo |

| | | | | |
|---|---|---|---|---|
| | | | | del archivo de contrato correspondiente al producto apuntado |
| **PunteroServicio** | InstancePointer | 8 | 1 | Indica el identificador de archivo del archivo de servicio correspondiente al producto apuntado |
| **PunteroValor** | InstancePointer | 8 | 1 | Indica el identificador de archivo de valor correspondiente al producto apuntado |
| **PrioridadProducto** | Priority | 8 | 1 | Indica la prioridad del producto. Un número mayor indica una prioridad superior. Si existen varios productos en la aplicación interoperable, su prioridad siempre debe ser distinta entre sí. La prioridad es asignada por el Registrar así:<br>--Monedero(16)<br>--Crédito (8)<br>--BPD(24)<br>--BPD2(23)<br>Para el caso de recarga de MONEDERO, es condición que se verifique antes el producto CREDITO el cual devera estar en 0 para que pueda ser recargado el MONEDERO |
| **RFU** | | | 9 | Reservado para uso futuro |
| | | | **57** | **Tamaño total** |

### 6.4.7 Archivo Eventos_EF

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

Emisión del medio de pago

Distribución de producto
Recarga de producto
Uso de producto
Devolución de la tarifa en la última validación

La configuración del archivo Eventos_EF es la siguiente:

Tipo de archivo: Cíclico
Número de registros: 10
Número de archivo: 0x06
Identificador de archivo ISO: 0x0006
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de cada registro: 64 bytes

### Descripción de la estructura de los registros del archivo Eventos_EF

### Cada registro dentro del archivo Eventos_EF consta de los siguientes datos:

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (byte) | Valor inicial, comentarios |
|---|---|---|---|---|
| **IdProducto** | ProductId | 16 | 2 | Identificador del producto usado en el evento. En el caso en que TipoEvento corresponda a *Emisión del medio de pago*, este campo tomará el valor de 0 (0x0000) |
| **PunteroProducto** | InstancePointer | 4 | 1 | Indica el identificador de archivo del contrato correspondiente al producto referido en el evento. En el caso en que TipoEvento sea *Emisión del medio de pago*, se debe apuntar al identificador del archivo Emisión_EF (0x01). De lo contrario debe tomar alguno de los siguientes valores:<br><br>--ContratoMonedero_EF |

| | | | | |
|---|---|---|---|---|
| | | | | (0x07)<br>--ContratoCrédito_EF (0x0A)<br>--ContratoBPD(0x0D)<br>--ContratoBPD2_EF (0x0012)-- |
| **InformaciónGeneral** | SEQUENCE | | | |
| **IdEntidad** | CompanyId | 16 | 2 | Código de identificación de la entidad que ha generado el evento en el medio de pago |
| **FechaHoraEvento** | DateTimeCompact | 32 | 4 | Fecha y hora de ocurrencia del evento |
| **TipoEvento** | Integer (0 .. 255) | 8 | 1 | Indica el tipo de evento registrado en la aplicación.<br>--no especificado (0)<br>--Distribución de producto (1)<br>--Uso de producto(4)<br>--Recarga de producto (6)<br>--Devolución de la tarifa (14)<br>--Emisión del medio de pago (20) |
| **MontoEvento** | Amount | 16 | 2 | Indica el monto intercambiado entre el dispositivo y el medio de pago. En el caso de un evento de *Distribución de producto* o *Emisión del medio de pago*, la unidad del monto corresponde a Centavos de Peso Mexicano. De lo contrario la unidad de valor del monto es definida por IdProducto |
| **ConsecutivoEvento** | Integer (0.. 16777215) | 24 | 3 | Corresponde al valor de |

| | | | | |
|---|---|---|---|---|
| | | | | ConsecutivoAplicación del archivo EstadoAplicación_EF en el momento en que se efectuó el evento. |
| **IdSAM** | ReferenceIdentifier | 56 | 7 | Identificador UID del módulo SAM usado en el evento. |
| **ConsecutivoSAM** | SerialNumber | 64 | 8 | Indica el número único de transacción del evento ejecutado en el SAM. Consecutivo SAM se define el el capítulo **¡Error! No se encuentra el origen de la referencia.** |
| **IdDispositivo** | DeviceId | 16 | 2 | Identificador del dispositivo usado en el evento. Asignado por el Registrar |
| **InformaciónVentaRecarga** | SEQUENCE | | | |
| **IdUbicación** | LocationId | 16 | 2 | Número que identifica el punto donde ocurrió el evento. Usado en transacciones diferentes a validación. |
| **InformaciónValidación** | SEQUENCE | | | |
| **TipoTransporte** | TransportTypeCode | 5 | 1 | Indica el tipo de modo de transporte usado en la validación.<br>--sin especificar (0)<br>--Camión urbano (1)<br>--Tren eléctrico (3)<br>--SiTren (29)<br>--Alimentador Macrobús (31)<br>--Macrobús (33) |
| **IdRuta_Estación** | ReferenceIdentifier | 16 | 2 | Número identificador de la ruta o de la estación donde |

| | | | | |
|---|---|---|---|---|
| | | | | se generó la transacción. |
| **NúmeroTransbordos** | CountOfJourneyLegs | 4 | 1 | Número actual de transbordos efectuados con el producto dentro de TiempoTransbordo. Este número nunca debe superar el valor de TransbordosPermitidos |
| **LímiteTransbordo** | DateTimeCompact | 32 | 4 | Indica la fecha y hora límite en la que una validación se considera un transbordo dentro de un viaje. Sí la siguiente validación supera este límite se considera una validación dentro de un nuevo viaje. |
| **NúmeroPassbacks** | NumberOfPassbacks | 4 | 1 | Número de passbacks acumulados dentro de la definición del contrato. |
| **InformaciónDevolución** | SEQUENCE | | | |
| **MotivoDevolución** | Integer (0..255) | 8 | 1 | Motivo por el cual fue necesario efectuar la devolución de la última tarifa aplicada.<br>--(1) Falla técnica: daño del vehículo<br>--(2) Falla logística: retraso del arribo del vehículo en una estación de la red interoperable<br>--(3) Agente externo: bloqueo de la vía, protestas o manifestaciones |
| IdTipoDispositivo | integer | 16 | 2 | Identificador tipo del dispositivo usado en el evento. Asignado por el Registrar<br>1=Validador<br>2=Maquina Recargadora |

| | | | | |
|---|---|---|---|---|
| | | | | 3=Modulo atención<br>4=Dispositivo Portátil<br>5= Punto de Venta |
| **RFU** | | | 18 | Reservado para uso futuro |
| | | | **64** | **Tamaño total** |

### 6.4.8 Archivo Contrato(Producto)_EF

La estructura del archivo Contrato(Producto)_EF es una generalización para los siguientes archivos en los que se comparte la misma estructura:

ContratoMonedero_EF
ContratoCrédito_EF
ContratoBPD_EF
ContratoBPD2_EF

Cada uno de estos archivos almacena la información estática del producto, incluyendo una definición de sus reglas de uso y sus restricciones. En cada caso, la configuración de cada archivo Contrato(Producto)_EF es específica del producto.

La configuración del archivo ContratoMonedero_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x07
Identificador de archivo ISO: 0x0007
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave M o llave RFU según el estado del producto (posición # 3)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 72 bytes

La configuración del archivo ContratoCrédito_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x0A
Identificador de archivo ISO: 0x000A
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca

- Lectura/Escritura: llave C o llave RFU según el estado del producto (posición # 4)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 72 bytes

La configuración del archivo ContratoBPD_EF es la siguiente:

Tipo de archivo: Estándar
Número de archivo: 0x0D
Identificador de archivo ISO: 0x000D
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave B o llave RFU según el estado del producto (posición # 5)
- Cambio de configuración: llave P (posición 0)

Tamaño de archivo: 72 bytes

La configuración del archivo ContratoBPD2_EF es la siguiente:

- Tipo de archivo: Estándar
- Número de archivo: 0x12
- Identificador de archivo ISO: 0x0012
- Configuración de comunicación: Plano + MAC
- Condiciones de acceso:
  - Lectura: libre
  - Escritura: nunca
  - Lectura/Escritura: llave B o llave RFU según el estado del producto (posición # 5)
  - Cambio de configuración: llave P (posición 0)

Tamaño de archivo: 72 bytes

### Descripción de la estructura de un archivo Contrato(Producto)_EF

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **DistribuidorProducto** | ProductRetailer, SEQUENCE | | | |
| **IdRedProducto** | NetworkId | 24 | 3 | Identificador de la red interoperable a la cual pertenece el distribuidor del producto |
| **IdDistribuidorProducto** | CompanyId | 16 | 2 | Identificador de la entidad que distribuye |

| | | | | |
|---|---|---|---|---|
| | | | | el producto |
| **IdProducto** | ProductId | 16 | 2 | Identificador del producto en la red interoperable. Asignado por el Registrar |
| **SerialProducto** | SerialNumber | 32 | 4 | Valor de ConsecutivoEvento correspondiente a la distribución del producto |
| **PrecioProducto** | Amount | 16 | 2 | Monto pagado al momento de la distribución del producto. Expresado en centésimas (centavos) de Peso Mexicano (MXN). Por ejemplo, para un valor de 1.53 MXN el valor correspondiente será de 153. |
| **UnidadValorProducto** | PayUnitMap | 4 | 1 | Indica la equivalencia que tiene una unidad de valor del producto correspondiente. Sus valores pueden ser:<br>--Centavo de Peso Mexicano (0)<br>--Viaje (1)<br>--RFU (2)<br>--RFU (3) |
| **MínimoValor** | MinAmountLimit | 32 | 4 | Valor mínimo que puede tomar el producto en su archivo Valor(Producto)_EF. Valor representado en |

| | | | | |
|---|---|---|---|---|
| | | | | Complemento a 2 en formato Big-Endian |
| **MáximoValor** | MaxAmountLimit | 32 | 4 | Valor máximo que puede tomar el producto en su archivo Valor(Producto)_EF. Valor representado en Complemento a 2 en formato Big-Endian |
| **NúmeroReactivaciónProducto** | INTEGER (0 .. 65535) | 16 | 2 | Identifica la última reactivación de un producto que ha sido previamente suspendido a través de listas LAP_V |
| **NúmeroAcciónAplicadaProducto** | INTEGER (0 .. 65535) | 16 | 2 | Identifica la última acción sobre el producto llevada a cabo con listas LAP_R. Usado junto con NúmeroAcciónProducto en las listas LAP_R para aplicar acciones sobre el producto |
| **InformaciónDistribución** | SEQUENCE | | | |
| **FechaDistribución** | DateTimeCompact | 32 | 4 | Fecha y hora de distribución del producto |
| **IdSAMDistribución** | ReferenceIdentifier | 32 | 4 | Identificador del módulo SAM usado en el evento de distribución del producto |
| **IdDispositivoDistribución** | DeviceId | 16 | 2 | Identificador del dispositivo utilizado para efectuar y registrar la |

| | | | | |
|---|---|---|---|---|
| | | | | distribución del producto. Asignado por el Registrar. |
| **ValidezProducto** | SEQUENCE | | | |
| **InicioValidezProducto** | DateTimeCompact | 32 | 4 | Fecha y hora de inicio de la validez del producto |
| **FinValidezProducto** | DateTimeCompact | 32 | 4 | Fecha y hora de vencimiento del producto. Si la fecha actual es posterior a esta fecha, el producto no es aceptado |
| **InicioValidezDía** | StartTimeStamp | 11 | 2 | Hora en la que se empieza a aceptar el producto en la red interoperable durante el día. Expresado en minutos transcurridos después de media noche. |
| **FinValidezDía** | EndTimeStamp | 11 | 2 | Hora en la que se deja de aceptar el producto durante el día. |
| **RestriccionesProducto** | SEQUENCE | | | |
| **DíasRestringidos** | RestrictedDayOfWeek | 8 | 1 | Días de la semana en que el producto no es válido. |
| **MaxViajesDíaSemana** | MaxTripsPerDayOfWeek | 32 | 4 | Número máximo de viajes que puede realizar el usuario para cada día de la semana con el producto. Un valor de 0 asignado a un día de la semana significa que no existe |

| | | | | |
|---|---|---|---|---|
| | | | | un máximo de viajes para ese día. |
| **TiempoPassback** | PassbackTime | 16 | 2 | Número de minutos en los que aplica la restricción de acceso anti-passback |
| **PassbacksPermitidos** | NumberOfPassbacks | 4 | 1 | Número de accesos permitidos dentro de un rango del tiempo TiempoPassback hasta que aplica el sistema anti-passback |
| **TiempoTransbordo** | TransferTimeLimitSS | 16 | 2 | Tiempo máximo expresado en minutos en el cual se pueden efectuar transbordos dentro de un viaje |
| **TransbordosPermitidos** | InterchangesAllowed | 4 | 1 | Número de transbordos permitidos dentro de TiempoTransbordo |
| **RFU** | | | 13 | Reservado para uso futuro |
| | | | **72** | **Tamaño total** |

### 6.4.9 Archivo Servicio(Producto)_EF

La estructura del archivo Servicio(Producto)_EF es una generalización para los siguientes archivos en los que se comparte la misma estructura:

ServicioMonedero_EF
ServicioCrédito_EF
ServicioBPD_EF
ServicioBPD2_EF

Cada uno de estos archivos es usado por parte de los prestadores de servicio. Estos están destinados a ser manipulados en transacciones de uso de productos. Incluyen información

del producto que puede ser modificada cada vez que se hace uso de un producto. En este caso, la configuración de cada archivo Servicio(Producto)_EF es específica del producto.

La configuración del archivo ServicioMonedero_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x08
Identificador de archivo ISO: 0x0008
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

La configuración del archivo ServicioCrédito_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x0B
Identificador de archivo ISO: 0x000B
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

La configuración del archivo ServicioBPD_EF es la siguiente:

Tipo de archivo: Backup
Número de archivo: 0x0E
Identificador de archivo ISO: 0x000E
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: libre
- Escritura: nunca
- Lectura/Escritura: llave S (posición # 2)
- Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

La configuración del archivo ServicioBPD2_EF es la siguiente:

- Tipo de archivo: Backup
- Número de archivo: 0x13
- Identificador de archivo ISO: 0x0013

- Configuración de comunicación: Plano + MAC
- Condiciones de acceso:
  - Lectura: libre
  - Escritura: nunca
  - Lectura/Escritura: llave S (posición # 2)
  - Cambio de configuración: llave P (posición # 0)

Tamaño de archivo: 23 bytes

## Descripción de la estructura de un archivo Servicio(Producto)_EF

| Nombre del dato | Tipo de dato | Tamaño (bits) | Tamaño (bytes) | Valor inicial, comentarios |
|---|---|---|---|---|
| **EstadoProducto** | Integer (0 .. 3) | 2 | 1 | Indica el estado actual del producto.<br>--Inicializado (0)<br>--Activado (1)<br>--Suspendido (2) |
| **NúmeroSemanaAño** | INTM | 6 | 1 | Indica el número de la semana del año según ISO 8601 en la cual se realizó la última validación con el producto. |
| **NúmeroViajesDíaSemana** | TripsPerDayOfWeek | 16 | 2 | Contador de los viajes que ha realizado el usuario cada día de la semana. Este contador nunca debe superar los valores definidos en MaxViajesDíaSemana. En el caso del producto de BPD, no se debe sumar un viaje si el uso del producto es considerado un transbordo. |
| **NúmeroActualUsos** | Quantity | 12 | 2 | Número total de usos realizados con el producto. Un viaje puede incluir varios usos según el producto. El producto de BPD contabiliza los transbordos como usos |

| | | | | |
|---|---|---|---|---|
| | | | | del producto, sin embargo no se debitan viajes en un transbordo. |
| FechaUltimoDebito | DateTimeCompact | 32 | 4 | Fecha y hora del instante en que se realizó la última validación del producto, utilizado para control del transbordo solo para validaciones |
| IdEntidadUltimoDebito | CompanyId | 16 | 2 | Código de identificación de la entidad en que se realizó la última validación del producto, utilizado para control del transbordo solo para validaciones |
| IdRutaEstaciónUltimoDebito | ReferenceIdentifier | 16 | 2 | Ruta o Estación en que se realizó la última validación del producto, utilizado para control del transbordo solo para validaciones |
| IdDispositivoUltimDebito | DeviceId | 16 | 2 | Identificador del dispositivo usado en el evento |
| **RFU** | | | 7 | Reservado para uso futuro |
| | | | **23** | **Tamaño total** |

### 6.4.10 Archivo Valor(Producto)_EF

La estructura del archivo Valor(Producto)_EF es una generalización para los siguientes archivos en los que se comparte la misma estructura:

ValorMonedero_EF
ValorCrédito_EF
ValorBPD_EF
ValorBPD2_EF

Cada uno de estos archivos almacena unidades de valor que corresponden al valor actual del producto. El significado del contenido de este archivo puede variar según el producto y su definición depende de la información almacenada en Contrato(Producto)_EF del

producto correspondiente. La configuración de cada archivo Valor(Producto)_EF es específica del producto.

La configuración del archivo ValorMonedero_EF es la siguiente:

Tipo de archivo: Valor
Número de archivo: 0x09
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: nunca
- Escritura: llave S (posición # 2)
- Lectura/Escritura: llave M (posición # 3)
- Cambio de configuración: llave P (posición # 0)

Límite inferior: 0x00000000
Límite superior: 0x7FFFFFFF
Valor inicial: 0x00000000
Leer valor sin llaves (Free GetValue) = sí
Crédito limitado: deshabilitado

La configuración del archivo ValorCrédito_EF es la siguiente:

Tipo de archivo: Valor
Número de archivo: 0x0C
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: nunca
- Escritura: llave S (posición # 2)
- Lectura/Escritura: llave C o llave RFU según el estado del producto (posición # 4)
- Cambio de configuración: llave P (posición # 0)

Límite inferior: 0x80000000
Límite superior: 0x00000000
Valor inicial: 0x00000000
Leer valor sin llaves (Free GetValue) = sí
Crédito limitado: deshabilitado

La configuración del archivo ValorBPD_EF es la siguiente:

Tipo de archivo: Valor
Número de archivo: 0x0F
Configuración de comunicación: Plano + MAC
Condiciones de acceso:

- Lectura: nunca
- Escritura: llave S (posición # 2)
- Lectura/Escritura: llave B o llave RFU según el estado del producto (posición # 5)
- Cambio de configuración: llave P (posición # 0)

Límite inferior: 0x000000

Límite superior: 0x7FFFFF
Valor inicial: 0x000000
Leer valor sin llaves (Free GetValue) = sí
Crédito limitado: deshabilitado

La configuración del archivo ValorBPD2_EF es la siguiente:

- Tipo de archivo: Valor
- Número de archivo: 0x14
- Configuración de comunicación: Plano + MAC
- Condiciones de acceso:
  - Lectura: nunca
  - Escritura: llave S (posición # 2)
  - Lectura/Escritura: llave B o llave RFU según el estado del producto (posición # 5)
  - Cambio de configuración: llave P (posición # 0)
- Límite inferior: 0x000000
- Límite superior: 0x7FFFFF
- Valor inicial: 0x000000
- Leer valor sin llaves (Free GetValue) = sí

Crédito limitado: deshabilitado

**Descripción de la estructura de un archivo Valor(Producto)_EF**

| Nombre del dato | Tipo de dato | Tamaño (bits) | Valor inicial, comentarios |
|---|---|---|---|
| **ValorProducto** | MIFARE DESFire EV1 Value File | 32 | Indica el valor actual del producto. Su significado depende de la información almacenada en Contrato(Producto)_EF |

# 7 Ciclos de vida

La vida de la aplicación interoperable o de un producto se puede caracterizar mediante un conjunto de estados que determinan funcionalidades en un momento determinado. Este conjunto de estados se denomina ciclo de vida y según el caso define diferentes estados. 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 este es desechado. Adicionalmente cada producto consta de 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 es restringida su funcionalidad.

## 7.1 Ciclo de vida de la aplicación interoperable

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 el campo *EstadoAplicación_EF.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. 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.

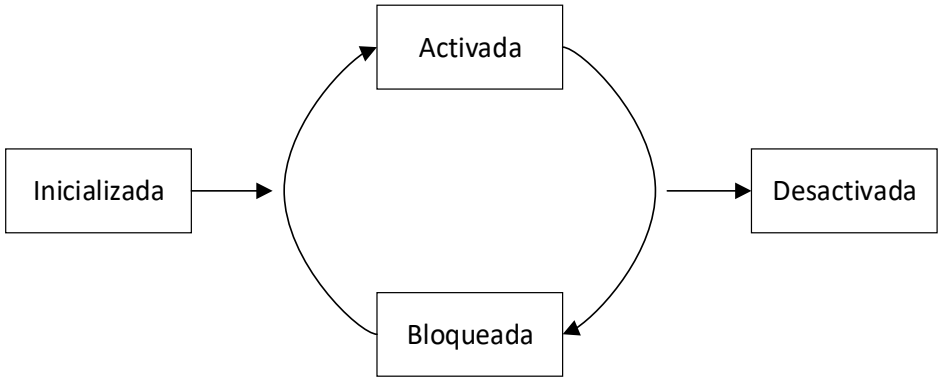
**Activada:** este estado permite usar el medio de pago en la red interoperable. Una aplicación pasa a Activada cuando esta pasa por el proceso de emisión del medio de pago. Una vez activada, la aplicación debe tener activado como mínimo un producto. Sin embargo son una excepción los medios de pago para funcionarios, los cuales no tienen que almacenar ningún producto debido a que estos almacenan un perfil de funcionario en Usuario_EF y un archivo Funcionario_EF con información propietaria de validación.

**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 siguiente figura describe cómo pueden ocurrir las transiciones entre los estados de la aplicación interoperable.

**Figura 3 – Ciclo de vida 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 en el cual no puede salir.

## 7.2 Ciclo de vida de los productos

Cada producto a distribuir 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 el campo *Servicio(Producto)_EF.EstadoProducto.* El ciclo de vida de un producto consta de los siguientes estados:

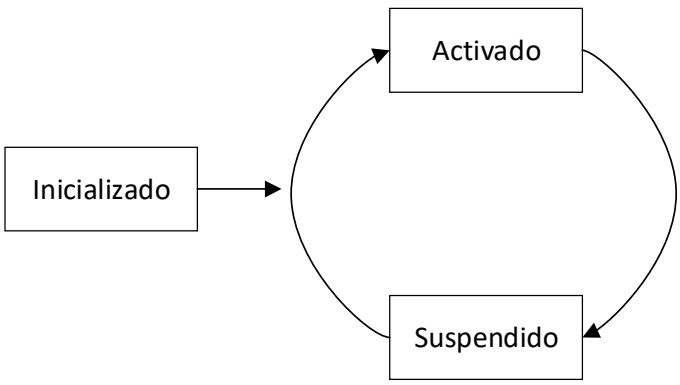
**Inicializado:** este estado se alcanza cuando la aplicación interoperable ha sido igualmente inicializada. En este punto solamente se han creado los archivos correspondientes al producto y no contienen información. Igualmente las llaves que protegen la modificación del producto no han sido cargadas,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

**Activado:** en este estado el producto podrá ser usado en la red interoperable. Los archivos Contrato(Producto)_EF, Servicio(Producto)_EF y Valor(Producto)_EF deben haber sido inicializados. Adicionalmente debe haber sido cargada la llave correspondiente al producto 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 siguiente figura describe cómo pueden ocurrir las transiciones entre los estados de un producto almacenado en la aplicación interoperable.

**Figura 4– Ciclo de vida de un producto**




# 8 Instrucciones de uso de la aplicación interoperable en medios de pago

A continuación se presentan los requerimientos, reglas y restricciones necesarias para efectuar posibles acciones en un medio de pago con la aplicación interoperable.

## 8.1 Inicialización de la aplicación en el medio de pago

Cada vez que se desea emitir un medio de pago para ser usado en la red interoperable este debe ser en primer lugar inicializado con la aplicación interoperable. La inicialización de los medios de pago debe ocurrir en un entorno controlado y seguro con el fin de evitar la emisión fraudulenta de estos en la red interoperable. A continuación se describen las acciones que se deben llevar a cabo en el medio de pago para lograr la inicialización del mismo:

Cargar la llave maestra (propiedad del Sistema Integrado de Recaudo ) del directorio raiz y modificar sus parámetros para operar bajo AES-128.
Modificar los parámetros del directorio raiz conforme a las especificaciones de este documento.
Crear el directorio Jalisco_DF conforme a las especificaciones de este documento.
Cargar en el directorio Jalisco_DF la llave de propietario (P) en la posición 0, llave de emisor de medios de pago (E) en la posición 1, llave de prestador de servicios (S) en la posición 2 y llave de uso futuro (RFU) en la posición 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, y 14.
Crear todos los archivos dentro de la aplicación interoperable:
- Emisión_EF,
- Entorno_EF
- Usuario_EF
- EstadoAplicación_EF
- ListaProductos_EF
- Eventos_EF
- ContratoMonedero_EF
- ContratoCrédito_EF
- ContratoBPD_EF
- ContratoBPD2_EF
- ServicioMondero_EF
- ServicioCrédito_EF
- ServicioBPD_EF
- ServicioBPD2_EF
- ValorMonedero_EF
- ValorCrédito_EF
- ValorBPD_EF
- ValorBPD2_EF

En caso en que el medio de pago esté destinado a un funcionario, crear el archivo Funcionario_EF
Escribir como mínimo los datos SerialMedioPago y PropietarioAplicación en el archivo Emisión_EF

## 8.2 Emisión del medio de pago

Una vez un medio de pago ha sido inicializado, este debe ser emitido según los requerimientos del usuario (personalización, productos). 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:

Completar los datos de emisión en Emisión_EF
Escribir toda la información de Entorno_EF

Modificar los datos de Usuario_EF en caso en que se esté emitiendo un medio de pago personalizado para un usuario.

En caso en que se emita un medio de pago para un funcionario, crear el archivo Funcionario_EF con la información determinada por la entidad a la cual pertenece el funcionario.

Modificar el estado de la aplicación al estado Activada. Esto significa que el valor de EstadoAplicación_EF.EstadoAplicación = 1 (Activada).

Crear una nueva entrada en Eventos_EF con la información de emisión del medio de pago.

Distribuir como mínimo un (1) producto en el medio de pago si se ha asignado un perfil diferente al perfil de Funcionario.

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

Escribir FechaNacimientoUsuario en caso de ser necesario

Escribir Perfil con los datos del usuario

Si el usuario es un funcionario (CódigoPerfil = 9), configurar el archivo Funcionario_EF según los criterios definidos por el emisor de medios de pago.

Aumentar EstadoAplicación_EF.ConsecutivoAplicación en 1.

## 8.4 Identificación de productos

Un producto almacenado en un medio de pago puede ser identificado con el campo IdProducto, almacenado en ListaProductos_EF y en Contrato(Producto)_EF. Adicionalmente los punteros del producto PunteroContrato, PunteroServicio y PunteroValor almacenados en ListaProductos_EF permiten asociar un producto identificado con IdProducto a sus correspondientes archivos dentro de la aplicación.

## 8.5 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, sin embargo esta solo debe almacenar un producto de cada tipo (Monedero, BPD, BPD2, Crédito). Por lo tanto, cuando un dispositivo desea distribuir un producto en un medio de pago, se debe verificar que no existe un producto activado del mismo tipo en el mismo. En caso en que exista el producto, es posible realizar una renovación del producto según los permisos que asigne el *Registrar* 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.

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

Verificar que no existe el producto que se desea distribuir en el archivo ListaProductos_EF
Cconfigurar el correspondiente archivo Contrato(Producto)_EF conforme a las especificaciones de este documento
Configurar el correspondiente archivo Servicio(Producto)_EF conforme a las especificaciones de este documento.
Configurar el correspondiente archivo Valor(Producto)_EF conforme a las especificaciones de este documento.
Escribir la información de contrato en el archivo Contrato(Producto)_EF.
Modificar el estado del producto a Activado. Esto significa que el valor de Servicio(Producto)_EF.EstadoProducto = 1 (Activado).
Escribir la información necesaria del producto en un sector sin usar en el archivo ListaProductos_EF
Crear una nueva entrada en el archivo Eventos_EF con la información de distribución del producto.
Aumentar EstadoAplicación_EF.ConsecutivoAplicación en 1.
Cambiar la llave RFU ubicada en la posición del producto por la llave del producto. (posición # para Monedero, posición # 4 para Crédito y posición # 5 para BPD)

## 8.6 Recarga de productos

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:

Siempre se debe verificar la presencia de una acción disponible en listas LAP_V para productos antes de intentar recargar un producto.
No está permitida la recarga de un producto almacenado en un medio de pago que esté en estado inicializado. Sin embargo es posible realizar la recarga de un producto activado o suspendido.
No está permitida la recarga de un producto almacenado en un medio de pago que no pertenece a la misma red interoperable que el dispositivo usado para la recarga de productos.
No está permitida la recarga de un producto cuya fecha de vencimiento de validez indicada en Contrato(Producto)_EF.FinValidezProducto sea inferior a la fecha actual.
La recarga de un producto implica las siguientes acciones en el medio de pago:
Incrementar Valor(Producto)_EF por el monto de la recarga.
Aumentar EstadoAplicación_EF.ConsecutivoAplicación en 1.
Crear nueva entrada en Eventos_EF con la información de recarga del producto.
La recarga del producto Crédito implica pagar la deuda adquirida al usar el producto, por lo que el archivo ValorCrédito_EF pasa de un valor negativo a cero.
Si se recarga el producto Crédito por un monto mayor a la deuda adquirida con este producto, el excedente se recarga en el producto Monedero.
No es posible recargar el producto Crédito por un valor inferior a la deuda total del producto.

No es posible recargar el producto Monedero sin antes haber saldado la deuda adquirida con el producto Crédito. Es decir, ValorCrédito_EF debe ser 0 antes de poder recargar el producto Mondedero.

Se sugiere el siguiente proceso para la recarga de productos con el fin de satisfacer las reglas mencionadas:

Esperar por medio de pago.

Al detectar medio de pago:

Leer Emisión_EF

Verificar FechaFinValidezTarjeta

Determinar DistribuidorAplicación

Determinar VersiónSeguridad

Leer Entorno_EF

Determinar VersiónAplicación

Verificar la aceptación del medio de pago según IdRed

Verificar FechaFinValidezAplicación

Leer EstadoAplicación_EF

Verificar EstadoAplicación

Buscar acciones disponibles en lista LAM para el medio de pago

(Terminar si el medio de pago no está Activado)

Leer ListaProductos_EF

SEGÚN producto a recargar HACER

CASO Monedero, Crédito

Verificar ValidezProducto Monedero

SI ValorCrédito_EF < 0 ENTONCES

Verificar ValidezProducto Crédito

Recargar producto Crédito por el valor de la deuda

Recargar producto Monedero por la diferencia entre la recarga total y el valor de la deuda del producto Crédito

SI NO

Recargar producto Monedero por el monto total de la recarga

FIN SI

CASO BPD

Verificar ValidezProducto BPD

Recargar producto BPD por el monto total de la recarga

FIN SEGÚN

TERMINAR

## 8.7 Uso de productos en transacciones de validación

Cuando un usuario acerca su medio de pago a un dispositivo de validación, 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:

No está permitido el uso de un producto suspendido.

No está permitido el uso de un producto almacenado en un medio de pago que no esté activado.

Solo está permitido el uso de un producto almacenado en un medio de pago que no pertenece a la misma red interoperable que el dispositivo de validación si existen los acuerdos comerciales necesarios para poder efectuar dicha acción.

Siempre se debe verificar la presencia de una acción disponible en listas LAM para el medio de pago o en listas LAP_V para productos antes de intentar usar un producto.

Si Usuario_EF.Perfil = 9 (funcionario) se deben aplicar las reglas de validación definidas por la entidad a la que pertenece el funcionario y que se encuentran almacenadas en el archivo Funcionario_EF. Estas reglas solo se pueden aplicar de forma local en los dispositivos de validación de la entidad a la que pertenece el funcionario.

La validez y las restricciones de un producto deben verificarse con la información almacenada en Contrato(Producto)_EF y Servicio(Producto)_EF

El cálculo de la tarifa a aplicar con un producto debe basarse en la información almacenada en Contrato(Producto)_EF, Servicio(Producto)_EF y Usuario_EF.

La selección de un producto para su uso depende de las siguientes condiciones:

Si existe una ventana de transbordo se debe intentar usar el producto usado en la validación anterior. Si el producto usado previamente no es válido se debe buscar un producto válido con una prioridad menor al producto usado en la anterior validación.

Si no existe una ventana de transbordo vigente se debe buscar un producto válido según la prioridad de los productos.

La priorización descendente de los productos se logra usando el archivo ListaProductos_EF y las reglas de aceptación del dispositivo de validación. Se debe intentar usar el producto válido con mayor prioridad. Si el intento de uso falla, se debe proceder a intentar usar el producto con la siguiente prioridad. Este proceso se debe llevar a cabo hasta lograr usar un producto o hasta agotar los intentos de uso con todos los productos.

Cuando un producto es válido para su uso, se deben llevar a cabo las siguientes acciones para hacer uso del producto:

Debitar Valor(Producto)_EF por la tarifa aplicada.

Aumentar EstadoAplicación_EF.ConsecutivoAplicación en 1.

Actualizar Servicio(Producto)_EF con la información de validación.

Crear nueva entrada en Eventos_EF con el evento de uso del producto en la transacción de validación.

El producto BPD no puede ser usado simultáneamente con ningún otro producto.

El producto Crédito solo puede ser usado si ValorCrédito_EF = 0

El producto de Monedero y el producto de Crédito pueden ser usados simultáneamente en una transacción de validación. Este caso puede darse si se cumplen todas las siguientes condiciones:

El producto BPD no existe en el medio de pago o no es válido en la transacción de validación.

El valor almacenado en ValorMonedero_EF es superior a cero (0).

El valor almacenado en ValorMonedero_EF no es suficiente para pagar la tarifa.

El valor almacenado en ValorCrédito_EF es igual a cero (0). Es decir, no existe una deuda vigente con este producto.

Tanto el producto Monedero como el producto Crédito son válidos para la transacción de validación.

El uso simultáneo del producto Monedero y el producto Crédito puede darse así exista una ventana de transbordo originada por el uso previo del producto Monedero.

El uso simultáneo del producto Monedero y el producto Crédito consiste en el uso de dos productos en una sola transacción de validación. Se debe descontar el valor total de ValorMonedero_EF. Se debe descontar el monto de ValorCrédito_EF equivalente a la diferencia entre la tarifa aplicada y el valor descontado en ValorMonedero_EF. Por último, se deben registrar dos usos de producto en el medio de pago siguiendo las reglas de uso de un producto.

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.

Se sugiere el siguiente proceso para el uso de productos con el fin de satisfacer las reglas mencionadas:

Esperar por medio de pago.

Al detectar medio de pago:

Leer Emisión_EF

Verificar FechaFinValidezTarjeta

Determinar DistribuidorAplicación

Determinar VersiónSeguridad

Leer Entorno_EF

Determinar VersiónAplicación

Verificar la aceptación del medio de pago según IdRed

Verificar FechaFinValidezAplicación

Leer EstadoAplicación_EF

Verificar EstadoAplicación

Buscar acciones disponibles en lista LAM para el medio de pago

(Terminar si el medio de pago no está Activado)

Leer Usuario_EF

Calcular perfil según FechaNacimientoUsuario y Perfil

SI Perfil = 9 (funcionario) y DistribuidorAplicación es válido ENTONCES

Leer Funcionario_EF

Aplicar reglas propietarias de validación de funcionario

TERMINAR

FIN SI

Leer ListaProductos_EF

Leer primer registro de Eventos_EF (información de última validación)

Determinar la existencia de una ventana de transbordo

SI existe ventana de transbordo ENTONCES

(el viaje actual es un transbordo)

Seleccionar producto usado en la última validación

Verificar ValidezProducto y RestriccionesProducto

(Si el producto es inválido, IR al Ciclo de priorización de productos)

Calcular tarifa según el producto seleccionado

Leer Valor(Producto)_EF

SI Valor(Producto) >= tarifa ENTONCES

Usar producto según las reglas de uso de productos

Otorgar acceso

TERMINAR

SI NO

SI el producto seleccionado es Monedero y es posible usar simultáneamente Monedero y Crédito ENTONCES

Usar producto Monedero

Usar producto Crédito

Otorgar acceso

TERMINAR

FIN SI

FIN SI

FIN SI

(Este punto se alcanza si no existe ventana de validación o si no fue posible utilizar el producto usado según la ventana de validación)

Priorización descendente de los productos almacenados según cada PrioridadProducto en ListaProductos_EF

CICLO selección de productos por prioridad

(Seleccionar producto)

Verificar ValidezProducto y RestriccionesProducto

Calcular tarifa

Leer Valor(Producto)_EF

SI ValorProducto >= tarifa ENTONCES

Usar producto

Otorgar acceso

TERMINAR

SI NO

SI el producto seleccionado es Monedero y es posible usar simultáneamente Monedero y Crédito ENTONCES

Usar producto Monedero

Usar producto Crédito

Otorgar acceso

FIN SI

FIN SI

TERMINAR CICLO

Si se termina el ciclo y no fue posible usar algún producto no se otorga el acceso

TERMINAR

## 8.8 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 que se haya averiado o perdido. Este proceso consiste en la reconstrucción de la aplicación en un nuevo medio de pago y la reconstrucción de los productos que esta tenía almacenados. La reconstrucción de un medio de pago solo puede ser llevada a cabo por el emisor del mismo.

Debido a que los lectores de medios de pago pueden estar fuera de línea con 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 la reconstrucción del mismo.

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

Inicialización de un medio de pago nuevo. El identificador SerialMedioPago debe ser nuevo y único.

Emisión de la aplicación interoperable en un medio de pago nuevo con la información del medio de pago antiguo.

Distribución de todos los productos almacenados en el medio de pago antiguo en el medio de pago nuevo. Esto incluye la escritura de la última información registrada de los archivos Contrato(Producto)_EF, Servicio(Producto)_EF y Valor(Producto)_EF en el medio de pago antiguo.

## 8.9 Acciones sobre medios de pago a través de la 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 validación 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 UID del MedioPago, 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 UID del MedioPago.

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

El campo CódigoAcción puede tomar los siguientes valores:
1 (acción de reactivación)
2 (acción de desactivación)
3 (acción de bloqueo)
A continuación se describe el proceso que debe seguir un dispositivo para ejecutar una acción sobre un medio de pago:

Esperar por medio de pago

Al detectar medio de pago:

```
Leer Emisión_EF
    Buscar Emisión_EF.SerialMedioPago en la lista LAM
SI Emisión_EF.SerialMedioPago EXISTE en la lista LAM ENTONCES
    Leer EstadoAplicación_EF
    SI NúmeroAcciónMedioPago > NúmeroAcciónAplicada ENTONCES
       SEGÚN CódigoAcción HACER
              CASO 1 (acción de reactivación)
                     (Desbloquear aplicación)
                     NúmeroAcciónAplicada = NúmeroAcciónMedioPago
                     EstadoAplicación_EF.EstadoAplicación = 1 (activada)
              CASO 2 (acción de desactivación)
                     (Desactivar aplicación)
                     EstadoAplicación_EF.EstadoAplicación = 2 (desactivada)
                     NúmeroAcciónAplicada = NúmeroAcciónMedioPago
              CASO 3 (acción de bloqueo)
                     (Bloquear medio de pago)
                     EstadoAplicación_EF.EstadoAplicación = 3 (bloqueada)
                     NúmeroAcciónAplicada = NúmeroAcciónMedioPago
       FIN SEGÚN
    SI NO
       Efectuar la acción solicitada con base en EstadoAplicación_EF
    FIN
SI NO
    Efectuar la acción solicitada con base en EstadoAplicación_EF
FIN
```

## 8.10 Suspensión de productos a través de la lista LAP_V

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 validación (LAP_V). Los dispositivos de validación deben almacenar la lista LAP_V 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 Contrato(Producto)_EF.NúmeroReactivaciónProducto.

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

Esperar por medio de pago

Al detectar medio de pago:

Leer Emisión_EF

Buscar Emisión_EF.SerialMedioPago en la lista LAP_V

SI Emisión_EF.SerialMedioPago EXISTE en la lista LAP_V ENTONCES

Leer ListaProductos_EF

Determinar los punteros del producto indicado en CódigoProducto

Leer Contrato(Producto)_EF

SI NúmeroSuspensiónProducto > NúmeroReactivaciónProducto ENTONCES

(Suspender producto)

Servicio(Producto)_EF.EstadoProducto = 2 (suspendido)

FIN

FIN

## 8.11 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_V.

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 Emisión_EF

Leer ListaProductos_EF

SI el producto con IdProducto en el medio de pago con SerialMedioPago puede ser reactivado ENTONCES

AUMENTAR Contrato(Producto)_EF.NúmeroReactivaciónProducto en 1

Servicio(Producto)_EF.EstadoProducto = 1 (activado)

FIN SI

## 8.12 Recarga remota de productos a través de la 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 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 Contrato(Producto)_EF.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.

La lista LAP_R no puede incluir acciones de recarga remota sobre el producto Crédito. Sin embargo la recarga del producto Crédito se puede llevar a cabo mediante una acción de recarga sobre el producto Monedero. En este caso deben aplicarse las reglas de recarga de los dos productos según el estado de los mismos.
A continuación se describe el proceso que debe seguir un dispositivo para ejecutar una acción de recarga remota de un producto:

Esperar por medio de pago

Al detectar medio de pago:

Leer Emisión_EF

Buscar Emisión_EF.SerialMedioPago en la lista LAP_R

SI Emisión_EF.SerialMedioPago EXISTE en la lista LAP_R ENTONCES

```
    Leer ListaProductos_EF
        Determinar los punteros del producto indicado en CódigoProducto
    Leer Contrato(Producto)_EF
    SI NúmeroAcciónProducto > NúmeroAcciónAplicadaProducto ENTONCES
        (Recarga remota de producto)
        Recargar Valor(Producto)_EF por el monto MontoAcción
        NúmeroAcciónAplicadaProducto = NúmeroAcciónProducto
    SI NO
        TERMINAR
    FIN SI
SI NO
    TERMINAR
FIN  SI
```

## 8.13 Renovación de productos

Los productos incluyen reglas de validez y de vencimiento del mismo en su contrato. Es posible renovar un producto con el fin de modificar estas reglas de aceptación en la red interoperable.

Por ejemplo, el producto de BPD está sujeto a renovación periódica debido a que está diseñado para ser aceptado por un tiempo limitado. En este caso, los distribuidores autorizados para distribuir el producto de BPD podrán efectuar una operación de renovación de este producto. En esta operación se sobrescribe el archivo ContratoBPD_EF para extender la validez para un nuevo periodo, se sobrescribe el archivo ServicioBPD_EF para reiniciar los parámetros de uso del producto, adicionalmente se recarga el archivo de valor ValorBPD_EF con el nuevo valor del producto para el nuevo periodo. Estas acciones aplican para cualquier producto que sea renovado. Por lo tanto un evento de renovación de producto incluye la sobrescritura de los archivos Contrato(Producto)_EF y Servicio(Producto)_EF, así como la recarga opcional del producto según las reglas de recarga definidas en este documento.

# 9 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(TISC)

**Nivel 1**: todos aquellos dispositivos lectores de medios de pago. Pueden ser dispositivos de validación, dispositivos de emisión de medios de pago y dispositivos de recarga de productos.

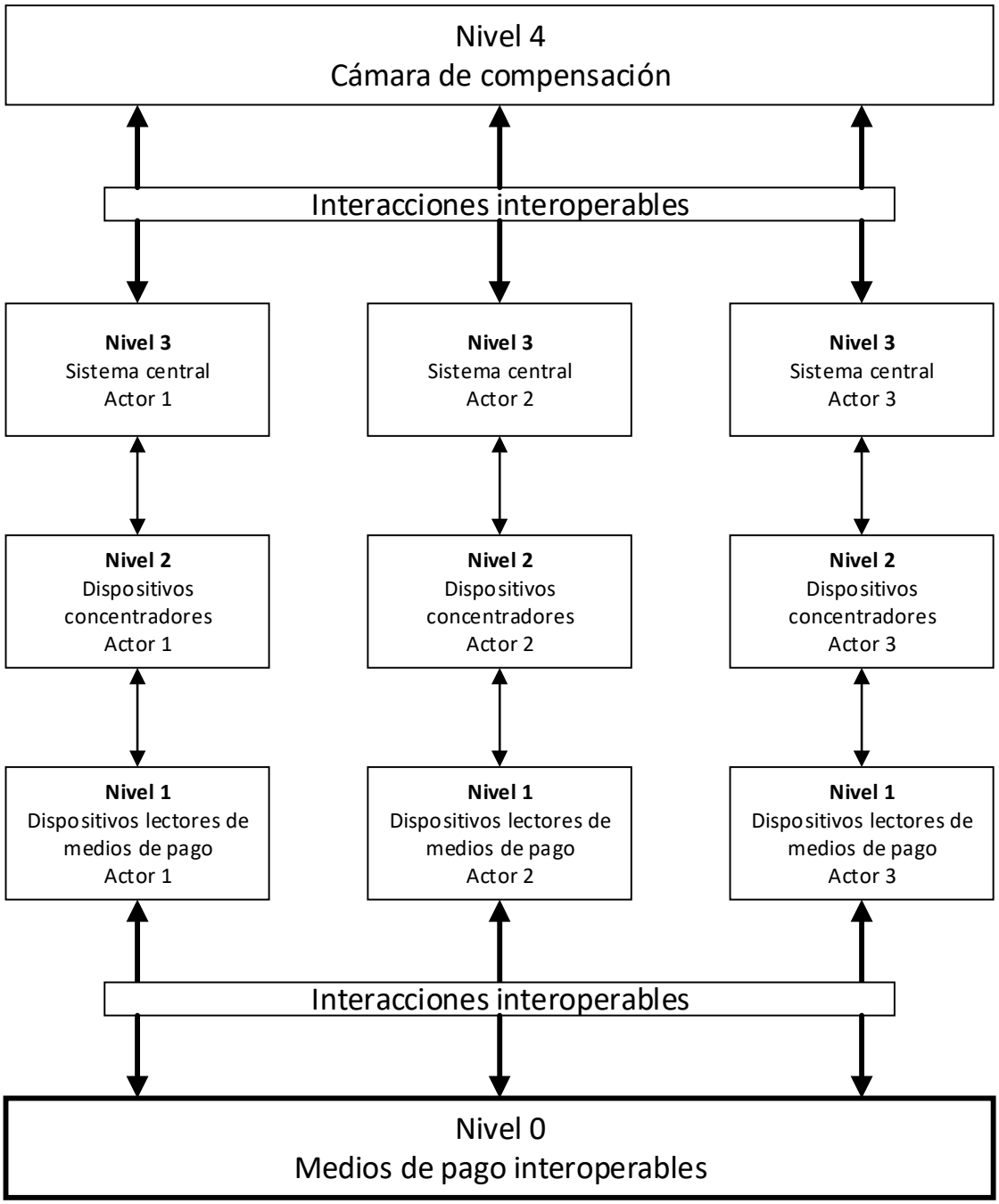
**Nivel 2**: dispositivos concentradores de transacciones que interconectan los dispositivos de nivel 1 con un sistema central de nivel 3

**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.

**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. Igualmente ocurre el intercambio de información entre cada una de los entidades que participan en la red interoperable. Este nivel es supervisado por el comitê de supervición para regular la red interoperable.

Con el fin de garantizar interoperabilidad, las interacciones llevadas a cabo entre cada uno de los niveles debe ser estandardizada, conforme a esta norma. Sin embargo debido a la naturaleza jerárquica de la red interoperable, solo se debe garantizar que el flujo de información al inicio y al final de la jerarquía sea estandarizada. Es decir solo la información almacenada en el nivel 0 e intercambiada con el nivel 1, así como la información intercambiada entre el nivel 3 y el nivel 4 deben ser interoperables.

Figura 8– Estructura multinivel de la red interoperable



# 10 Flujo de datos de eventos

Con base en el modelo de flujo de datos, los eventos generados en los medios de pago de la red interoperable son transmitidos en forma de interacciones interoperables entre el nivel 3 y el nivel 4. Estas sirven para cumplir con dos propósitos principales:

Cruce de cuentas entre los actores cuando se deben dinero por concepto de uso de productos en servicios prestados por diferentes Sistemas interoperables de recaudo.

Recolección de la actividad de los medios de pago para seguimiento y reconstrucción del estado de los mismos.

Todos los eventos deben pasar por la Cámara de compensación para ejecutar el proceso de cruce de cuentas.

La Cámara de compensación a es la entidad que actúa como punto de interconexión entre todos los actores. Por lo tanto, es esta la encargada de retransmitir los eventos generados con los medios de pago a sus respectivos emisores. Dichos emisores estarán en el deber de proporcionar a la câmara de compensacion toda la informacion necesária para reconstruir la actividad de los medios de pago o productos emitidos y en caso de ser necesario, solicitar a la Cámara de compensación la ejecución de acciones sobre los medios de pago a través de listas de acción.

La estructura de los archivos que se utilizan para la trasmision de los eventos, acciones, listas negras, catálogos operativos y toda aquella información que se comparte entre los operadores tecnológicos y la câmara de compensación, asi como los métodos de encriptacion y los canales de segurida que se utilizan para trasmitir, son proporcionados por la empresa que sea encargada de administrar y supervisar la câmara de compensación.. ESTOS DEBEN CUMPLIR COMO MINIMO CON EL DETALLE DEFINIDO EN EL ITEM 10.1 SIGUIENTE.

Del mismo modo la empresa responsable de la cámara de compensación proporciona la metodología para informar del exito o los problemas que se presenten al procesar los archivos enviados por los operadores tecnológicos

Los catálogos operativos que sean requeridos y enviados a la cámara de compensacion son utilizados para realizar los procesos de validacion de la información por lo que sera responsabilidade de los Operadores Tecnológicos el envío y mantenimiento de la información que radique en ellos

La empresa encargada de los servicios de la câmara de compensacion proporcionara las reglas de operacion de los procesos y la estructura de los archivos a los operadores tecnológicos

## 10.1 Datos requeridos por evento

Es importante destacar que los UID del MEDIO DE PAGO y del modulo SAM sirven como base para la identificación y validez de todos los eventos que se generan en la red interoperable. Los siguientes son los datos minimos que se espera se almacenen en sus bases de datos y se generen directamente en sus equipos al momento de un evento, estos datos servirán para estructurar la información que la cámara de compensación requiere.

### 10.1.1 Eventos de validación

| DATO | Mapping | Observaciones |
|---|---|---|
| Folio consecutivo de transacción en la tarjeta | ConsecutivoAplicación | |
| Fecha y hora de la transacción | FechaHoraEvento | La fecha incluye segundos |
| Identificador del medio de pago | UID | |
| Perfil del medio de pago | CódigoPerfil | |
| Producto operado | IdProducto | |
| Monto de la Transacción | MontoEvento | |
| Saldo Inicial | ValorMonedero_EF (Antes Transacción) | |
| Saldo Final | ValorMonedero_EF (Desp. Transaccion | |
| ID SAM | IdSAM | |
| Folio de Transaccion en SAM | ConsecutivoSAM | |
| Latitud | | Para el Cobro abordo |
| Longitud | | Para el Cobro abordo |
| Tipo de transaccion | TipoEvento | |
| Identificador dispositivo | IdDispositivo | |
| Identificador Unidad/Estacion | IdUbicación | |
| Identificador empresa | Identidad | |
| Identificador Ruta | IdRuta_Estación | |

### 10.1.2 Eventos de recarga

| DATO | Mapping | Observaciones |
|---|---|---|
| Folio consecutivo de transacción en la tarjeta | ConsecutivoAplicación | |
| Fecha y hora de la transacción | FechaHoraEvento | La fecha incluye segundos |
| Identificador del medio de pago | UID | |
| Perfil del medio de pago | CódigoPerfil | |
| Producto operado | IdProducto | |
| Inicio de vigencia producto | | |
| Fin Vigencia Producto | | |
| Hora de inicio de activación al dia | InicioValidezDía | |
| Hora de fin de activación del dia | FinValidezDía | |
| Monto de la Transacción | MontoEvento | |
| Saldo Inicial | ValorMonedero_EF (Antes Transacción) | |
| Saldo Final | ValorMonedero_EF (Desp. Transaccion | |
| ID SAM | IdSAM | |
| Folio de Transaccion en SAM | ConsecutivoSAM | |
| Latitud | | |
| Longitud | | |
| Tipo de transaccion | TipoEvento | |
| Identificador dispositivo | IdDispositivo | |
| Identificador Unidad/Estacion | IdUbicación | |
| Identificador empresa | Identidad | |
| Identificador Ruta | IdRuta_Estación | |

### 10.1.3 Eventos venta de medios de pago

En este evento existe la posibilidad de que se entreguen mas de un producto, para cada uno de ellos se registra el evento de venta mas los eventos de recarga

| DATO | Mapping | Observaciones |
|---|---|---|
| Folio consecutivo de transacción en la tarjeta | ConsecutivoAplicación | |
| Fecha y hora de la transacción | FechaHoraEvento | La fecha incluye segundos |
| Identificador del medio de pago | UID | |
| Perfil del medio de pago | CódigoPerfil | |
| Producto operado | IdProducto | |
| Inicio de vigencia producto | | |
| Fin Vigencia Producto | | |
| Hora de inicio de activación al dia | InicioValidezDía | |
| Hora de fin de activación del dia | FinValidezDía | |
| Costo del plastico | MontoEvento | |
| ID SAM | IdSAM | |
| Folio de Transaccion en SAM | ConsecutivoSAM | |
| Latitud | | |
| Longitud | | |
| Tipo de transaccion | TipoEvento | |
| Identificador dispositivo | IdDispositivo | |
| Identificador Unidad/Estacion | IdUbicación | |
| Identificador empresa | Identidad | |
| Identificador Ruta | IdRuta_Estación | |

### 10.1.4 Eventos de Bloqueo o Cancelacion

| DATO | Mapping | Observaciones |
|---|---|---|
| Fecha y hora de la transacción | FechaHoraEvento | La fecha incluye segundos |
| Identificador del medio de pago | UID | |
| Folio consecutivo de acción aplicado a la tarjeta | NúmeroAcciónAplicada | |
| Tipo de accion | | |

### 10.1.5 Eventos de Transferecia de Saldos

| DATO | Mapping | Observaciones |
|---|---|---|
| Folio Reporte | | Es el reporte que autorizo este evento |
| Folio consecutivo de transacción en la tarjeta | ConsecutivoAplicación | |
| Fecha y hora de la transacción | FechaHoraEvento | La fecha incluye segundos |
| Identificador del medio de pago | UID | |
| Perfil del medio de pago | CódigoPerfil | |
| Producto operado | IdProducto | |
| Inicio de vigencia producto | | |
| Fin Vigencia Producto | | |
| Hora de inicio de activación al dia | InicioValidezDía | |
| Hora de fin de activación del dia | FinValidezDía | |
| Monto de la Transacción | MontoEvento | |
| Saldo Inicial | ValorMonedero_EF (Antes Transacción) | |
| Saldo Final | ValorMonedero_EF (Desp. Transaccion | |
| ID SAM | IdSAM | |
| Folio de Transaccion en SAM | ConsecutivoSAM | |
| Latitud | | |
| Longitud | | |
| Tipo de transaccion | TipoEvento | |
| Identificador dispositivo | IdDispositivo | |
| Identificador Unidad/Estacion | IdUbicación | |
| Identificador empresa | Identidad | |
| Identificador Ruta | IdRuta_Estación | |

Con base en el modelo de flujo de datos, los eventos generados en los medios de pago de la red interoperable son transmitidos en forma de interacciones interoperables entre el nivel 3 y el nivel 4. Estas sirven para cumplir con dos propósitos principales

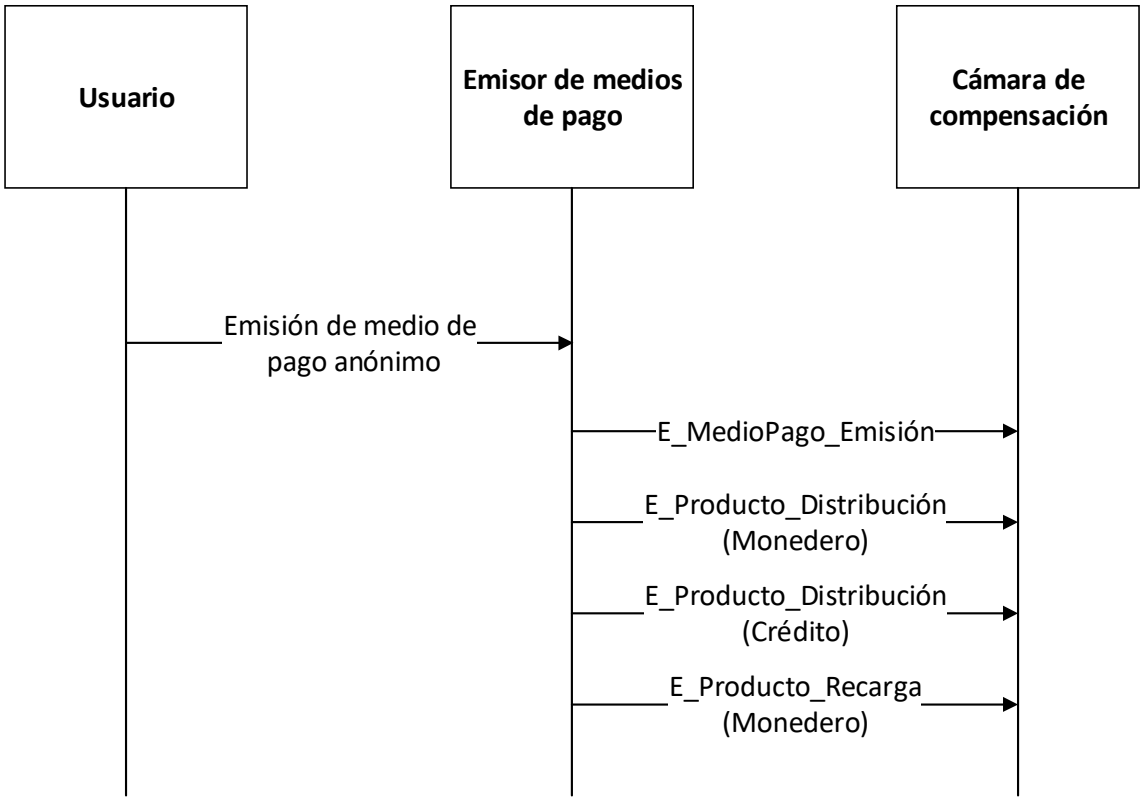
# 11 Casos de uso de medios de pago

Los casos de uso de medios de pago describen las posibles situaciones que se pueden dar en las cuales es necesaria la comunicación entre entidades de la red interoperable 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.

## 11.1 Emisión de medio de pago tarifa general

| **Nombre del caso de uso** | **Emisión de medio de pago anónimo** |
|---|---|
| **Resumen** | Un usuario adquiere un medio de pago con un saldo inicial de monedero en un dispositivo de emisión de medios de pago. |
| **Prerrequisitos** | Ninguno |
| **Accionado por** | Usuario |
| **Actores** | Emisor del medio de pago<br>Usuario<br>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.<br>El dispositivo de emisión de medios de pago efectúa:<br>Emisión del medio de pago a través de la escritura de la aplicación interoperable<br>Distribución y recarga inicial del producto Monedero.<br>Distribución del producto Crédito.<br>Almacenamiento de la información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |

**Figura 9 – Eventos enviados en la emisión de un medio de pago tarifa general**



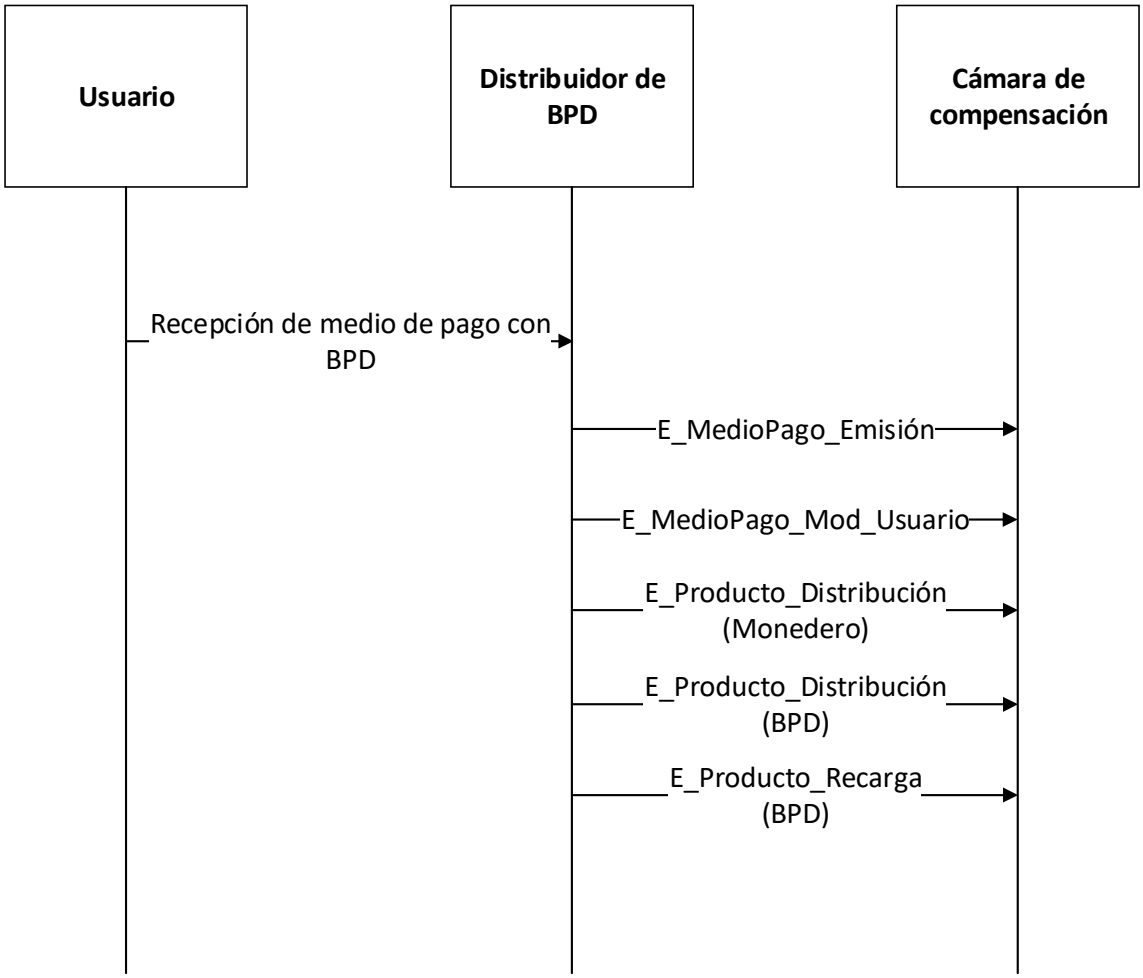

## 11.2 Emisión de medio de Pago Tarifa Preferencial

### Tarifa preferencial

| **Nombre del caso de uso** | **Entrega de medio de pago personalizado con BPD** |
|---|---|
| **Resumen** | Se realiza la entrega de un medio de pago a un beneficiario que es beneficiario de tarifa preferencial y que podría ser acreedor del programa BPD. Este medio de pago incluye los productos BPD y el producto Monedero. Se realiza una recarga de valor al producto de BPD, solo si el usuario es beneficiario y el emisor esta autorizado. |
| **Prerrequisitos** | Personalizacion |
| **Accionado por** | Usuario<br>Distribuidor de medios de pago preferenciales |

| | |
|---|---|
| | Distribuidor de producto (BPD) opcional |
| **Actores** | Emisor del medio de pago o distribuidor de productos<br>Usuario<br>Cámara de compensación |
| **Descripción del caso de uso** | Un medio de pago con la aplicación interoperable es entregado a un usuario. Esta entrega es efectuada por una entidad autorizada para distribuir el producto de BPD a través de un dispositivo lector de medios de pago.<br>El dispositivo lector de medios de pago efectúa:<br>Emisión del medio de pago a través de la escritura de la aplicación interoperable.<br>Modificación del perfil de usuario a través de la escritura del perfil en el medio de pago.<br>Distribución del producto Monedero.<br>Distribución y recarga inicial del producto BPD.<br>Almacenamiento de la nueva información generada en el medio de pago<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Revisar que el usuario no tenga otra tarjeta de perfil preferencial ACTIVA para proceder |

Figura 11 – Eventos enviados en la entrega de medio de pago tarifa preferencial

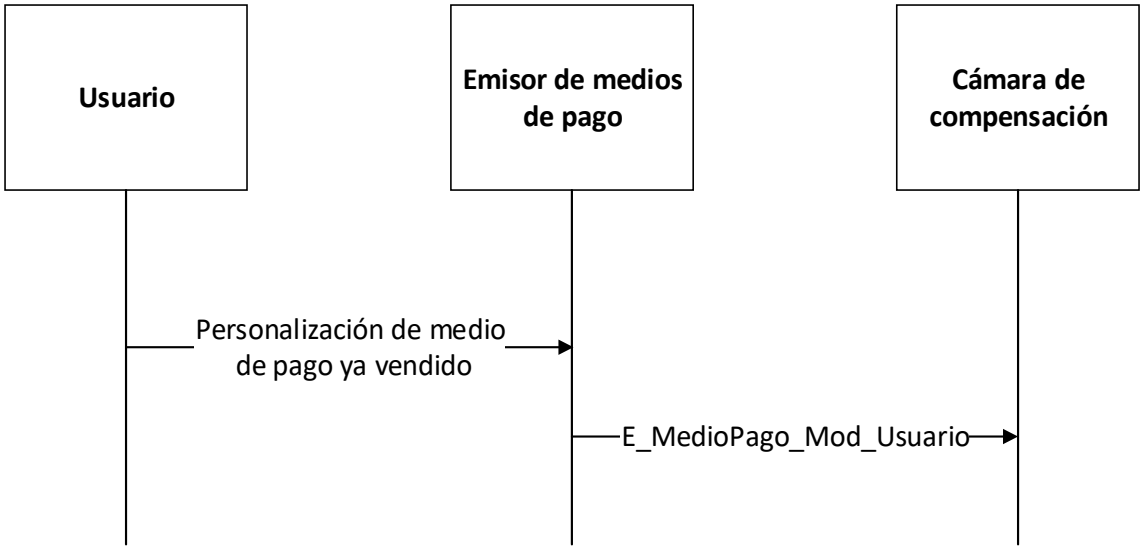



## 11.3 Personalización del medio de pago

| **Nombre del caso de uso** | **Personalización del medio de pago ya vendido** |
|---|---|
| **Resumen** | Un usuario con un medio de pago entregado por un emisor de medios de pago solicita la personalización del mismo. |
| **Prerrequisitos** | Emisión de medio de pago anónimo |
| **Accionado por** | Usuario |
| **Actores** | Emisor del medio de pago o Modulo de atención a pasajeros |

| | |
|---|---|
| | Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Dado un medio de pago emitido (vendido) por una entidad, un pasajero solicita personalizar este medio de pago. A través de un dispositivo de emisión de medios de pago, este emisor realiza:<br>Registro de los datos del usuário y de la relacion entre el usuário y la tarjeta. Personalización del medio de pago almacenando los datos necessários em la BD central .<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Revisar que el usuario no tenga otra tarjeta de perfil preferencial ACTIVA para proceder |

**Figura 12 – Eventos enviados durante la personalización del medio de pago ya vendido**

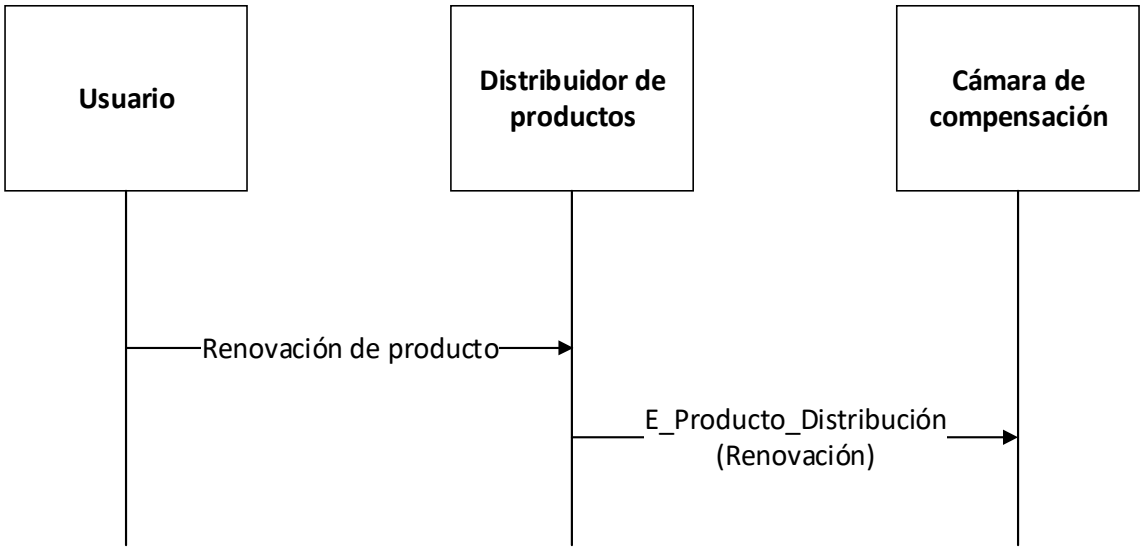



## 11.4 Renovación del perfil de una tarjeta

| **Nombre del caso de uso** | **Renovación** del perfil de una tarjeta |
|---|---|
| **Resumen** | Un usuario solicita a un distribuidor de productos la renovación del contrato de la vigencia de un perfil para extender su validez. |

| | |
|---|---|
| **Prerrequisitos** | Emisión de medio de pago con tarifa preferencial |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario solicita a un distribuidor de productos la renovación de la vigencia del perfil de tarifa preferencial a través de un dispositivo lector de medios de pago, este distribuidor realiza:<br>Autorización y renovación de los parámetros del perfil.<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | En caso de que la vigencia del perfil no pueda ya reactivarse por parte del pasajero, la tarjeta dejara de funcionar y el SALDO en el monedero podrá transferirse a una tarjeta de tarifa general |

Figura 14 – Eventos enviados durante la renovación del perfil de una tarjeta

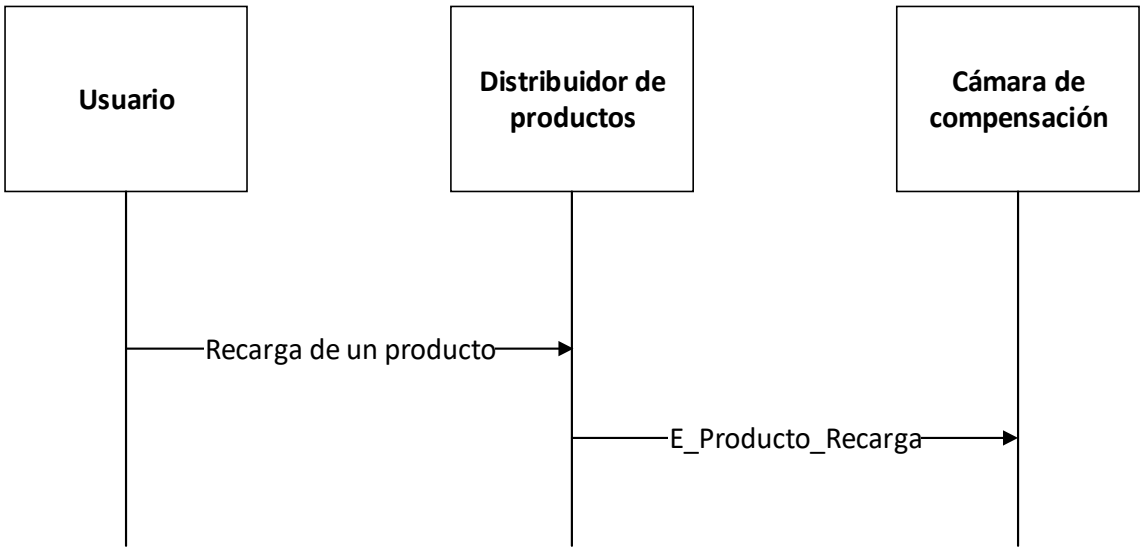



## 11.5 Recarga de un producto

| 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 anónimo o<br>Emisión de medio de pago personalizado o<br>Emisión de medio de pago personalizado con BPD o<br>Adquisición de un producto |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario solicita a un distribuidor de productos autorizado la recarga de un producto almacenado en su medio de pago. A través de un dispositivo de lector de medios de pago, este distribuidor realiza:<br>Recarga de valor del producto solicitado y generación del |

| | |
|---|---|
| | registro del evento en el medio de pago.<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar |

**Figura 15– Eventos enviados durante la recarga de un producto**

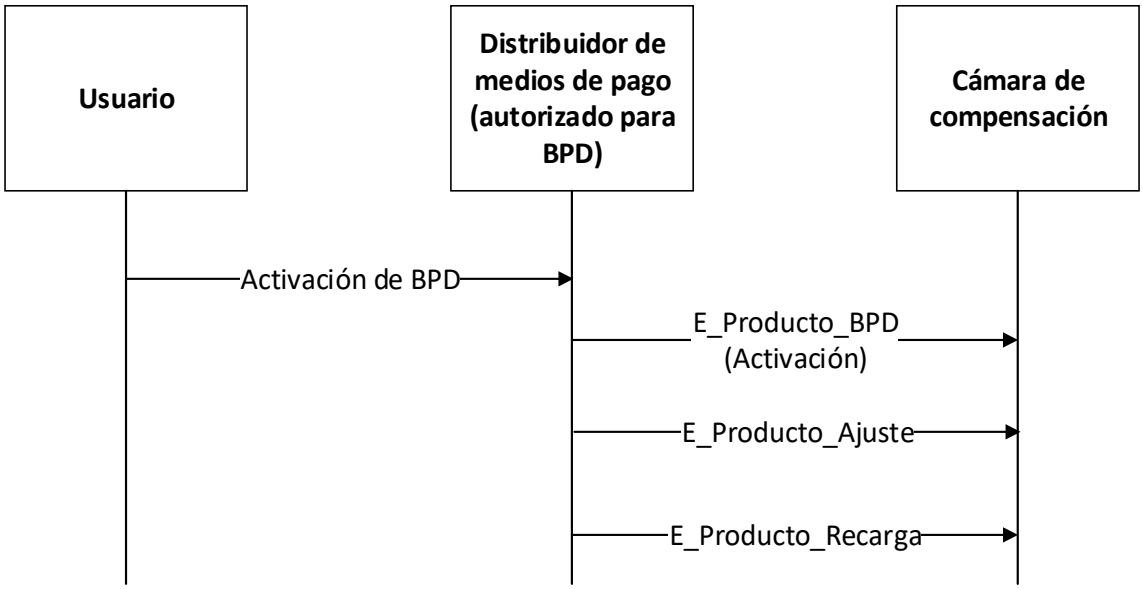



## 11.6 Activación y Recarga del producto de BPD / BPD2

| **Nombre del caso de uso** | **Activación y Recarga del producto de BPD / BPD2** |
|---|---|
| **Resumen** | Un usuario se dirige a un distribuidor de productos autorizado para activar su producto de BPD/BPD2 |
| **Prerrequisitos** | Entrega de medio de pago personalizado con BPD/BPD2<br>o<br>Adquisición de un producto |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos autorizado para distribuir BPD / BPD2<br>Cámara de compensación |

| | |
|---|---|
| | Usuario |
| **Descripción del caso de uso** | Un usuario solicita activar y recarga un producto de BPD al distribuidor de productos autorizado. En este caso, el producto debe ser activado por un periodo. Adicionalmente el producto debe ser recargado para que el valor del producto de BPD corresponda al valor designado para el nuevo periodo, en caso de que el valor del producto antes de la renovación sea mayor a 0 se realizara una transacción de ajuste de saldo, que se registrara también en la cámara de compensación, para liquidar el saldo existente . A través de un dispositivo lector de medios de pago, el distribuidor de productos realiza:<br><br>Activacion del producto de BPD / BPD2<br>Programacion con las fechas de valides de validez.<br>Gravar valor del producto de BPD y generación del registro del evento en el medio de pago, si el produto BPD/BPD2 tenia un saldo, generar el registro de ajuste tanto em el médio de pago como para la câmara de compensación.<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar<br><br>Solo puede estar activo y vigente un producto BPD/BPD2 |

Figura 16 – Eventos enviados durante la renovación del producto BPD




## 11.7 Validación al ingreso

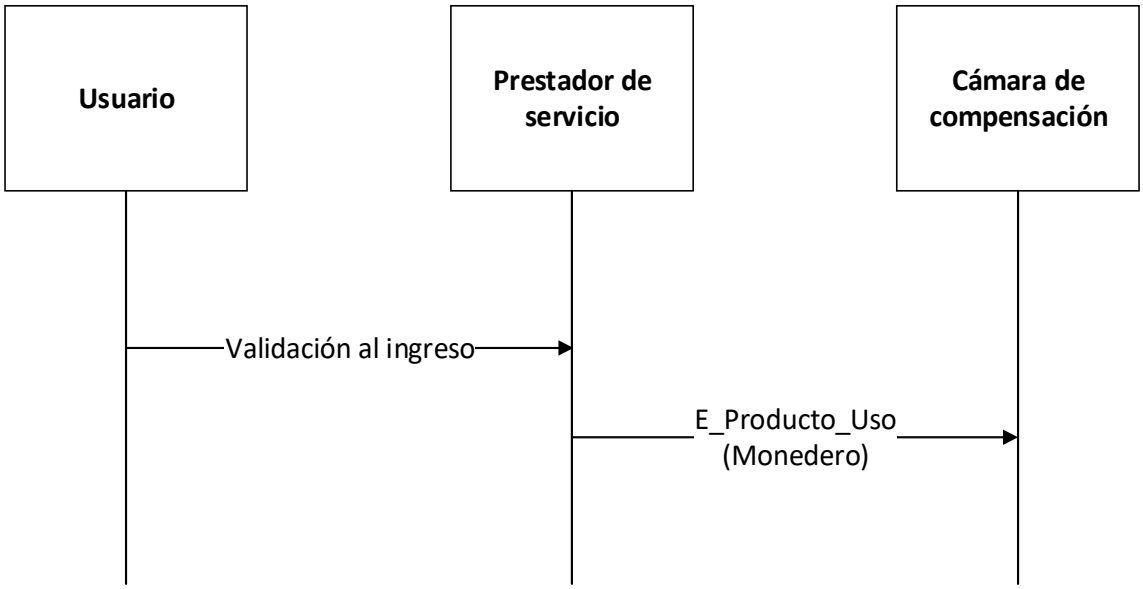
La validación del medio de pago al ingreso depende principalmente de los productos que se han almacenado en el medio de pago y su respectivo estado. Por lo tanto es necesaria la segmentación de estos casos de uso.

### 11.7.1 Validación con Monedero

| **Nombre del caso de uso** | **Validación con Monedero** |
|---|---|
| **Resumen** | Un usuario acerca su medio de pago a un dispositivo de validación para acceder a un servicio de la red interoperable. Su medio de pago tiene activado el producto Monedero y el producto Crédito. Su saldo en el Monedero es suficiente para pagar la tarifa. Su saldo en el producto crédito es igual a cero. Opcionalmente tiene el producto de BPD pero este no es válido para cobrar el pasaje. |
| **Prerrequisitos** | Emisión de medio de pago de tarifa general anónimo o<br>Emisión de medio de pago de tarifa general personalizado o<br>Emisión de medio de pago de tarifa preferencial personalizado o<br>Emisión de medio de pago de tarifa preferencial |

| | |
|---|---|
| | personalizado con BPD inactivos o con saldo 0 |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario presenta su medio de pago con el producto Monedero.<br>El prestador de servicio realiza las siguientes operaciones a través de un dispositivo de aceptación de medios de pago:<br>Aun que tiene los archivos BPD, es el caso que no puede cobrar con ellos<br>Verificación de la validez del medio de pago y del producto Monedero.<br>Verifica que el valor en el producto credito sea 0<br>Verifica que el saldo del Monedero cubra el pago de la tarifa<br>Generación del registro del evento en el medio de pago.<br>Almacenamiento de la nueva información generada en el medio de pago (saldo del monedero, información de históricos, informacion de archivo de servicio.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar<br>Debera revisar los parámetros definidos para los transbordos<br>Revisara que los parámetros fueron almanceados correctamente al terminar la transacción<br>Revisara las tarifas correspondientes para el perfil |

Figura 17 – Eventos enviados durante la validación con Monedero

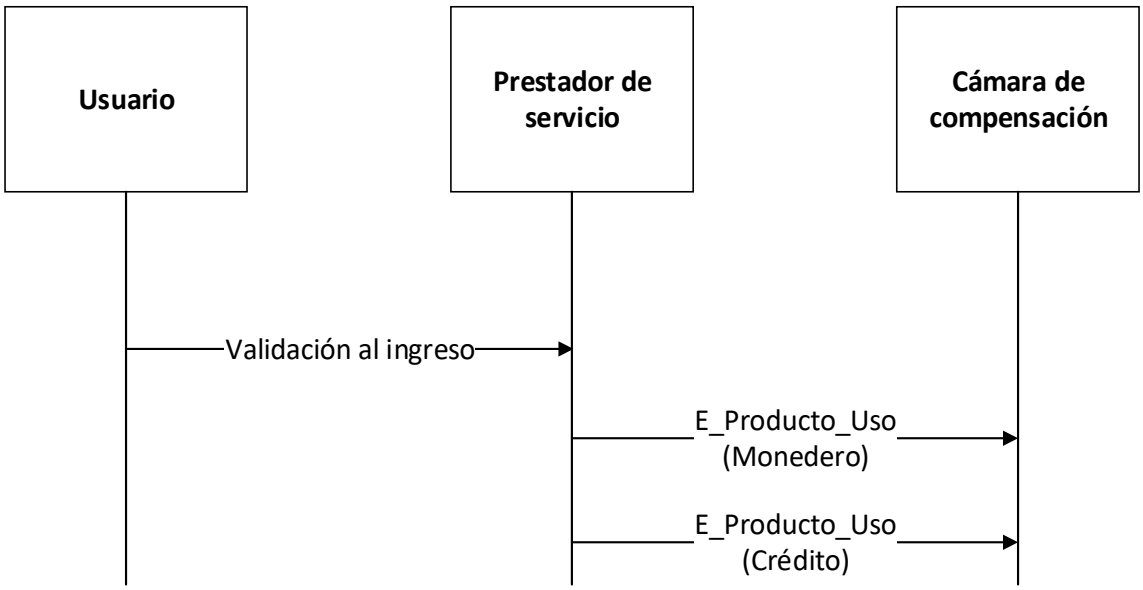



### 11.7.2 Validación con Monedero y Crédito simultáneamente

| **Nombre del caso de uso** | **Validación con Monedero y Crédito simultáneamente** |
|---|---|
| **Resumen** | Un usuario presenta su medio de pago a un dispositivo de validación para acceder a un servicio de la red interoperable. Su medio de pago almacena los productos Monedero y Crédito. El saldo en el Monedero no es insuficiente para pagar la tarifa. Adicionalmente tiene disponible el producto de Crédito con saldo igual a cero y los productos BPD no están. |
| **Prerrequisitos** | Emisión de medio de pago anónimo tarifa general o<br>Emisión de medio de pago personalizado tarifa general<br>La funcionalidad esta activa de acuerdo a los parámetros operativos |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario presenta su medio de pago con el producto |

| | |
|---|---|
| | Monedero y Crédito. El prestador de servicio realiza las siguientes operaciones a través de un dispositivo de aceptación de medios de pago:<br>Verificación de la validez del medio de pago, del producto Monedero y el producto Crédito (que el valor sea mayor o igual a 0 y menor que la tarifa a pagar).<br>Cálculo de la tarifa, uso del producto Monedero y el producto Crédito según la disponibilidad de valor de cada producto con valor máximo a lo necesário para completar el pago de uma tarifa asignada al prestador de servicio.<br>Generación de los registros de eventos en el medio de pago.<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | El CREDITO solo se aplica en conjunto con el MONEDERO<br>El crédito solo se aplica si las reglas de operacion así lo indican |

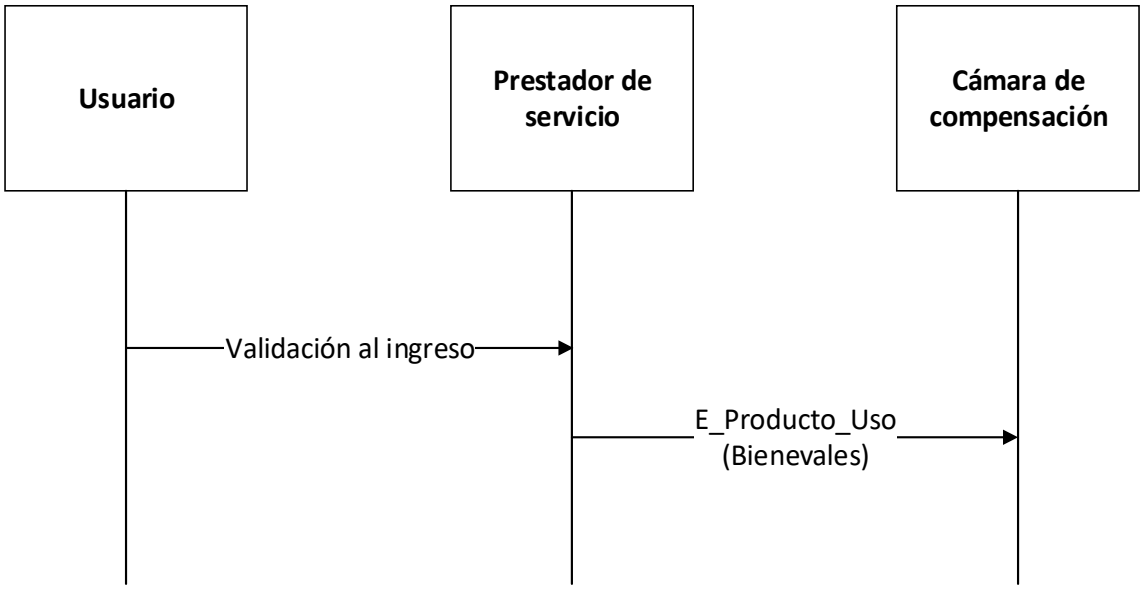
**Figura 18 – Eventos enviados durante la validación con Monedero y Crédito simultáneamente**



### 11.7.3 Validación con BPD

| **Nombre del caso de uso** | **Validación con BPD** |
|---|---|
| **Resumen** | Un usuario acerca su medio de pago a un dispositivo de validación para acceder a un servicio de la red interoperable. Su medio de pago almacena activo y vigente un producto BPD (uno o dos) con saldo mayor a cero. |
| **Prerrequisitos** | Emisión de medio de pago personalizado con BPD |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario presenta su medio de pago con el producto BPD. El prestador de servicio realiza las siguientes operaciones a través de un dispositivo validación de medios de pago:<br>Verificación de la validez y vigencia del medio de pago, el perfil y el producto BPD.<br>Cálculo de la tarifa y uso del producto BPD.<br>Generación del registro de evento en el medio de pago.<br>Almacenamiento de la nueva información generada en el medio de pago.<br>Envío de la información de eventos a la Cámara de compensación. |
| **Nota:** | Solo puede estar activo y vigente un producto BPD |

Figura 20 – Eventos enviados durante validación con BPD




## 11.8 Reemplazo o reconstrucción del medio de pago

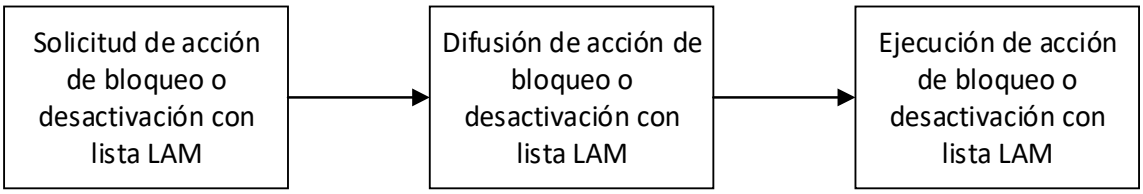
| Nombre del caso de uso | Reemplazo del medio de pago |
|---|---|
| **Resumen** | Un usuario tiene un medio de pago dañado o extraviado y solicita se transfiera su saldo a otro medio de pago. |
| **Prerrequisitos** | Emisión de medio de pago de tarifa general o<br>Emisión de medio de pago de tarifa preferencial con o sin BPD<br>Activación y personalización del medio de pago<br>Para medios de pago de tarifa preferencial, desactivacio lógica o envio a lista negra del medio de pago a reemplazar |
| **Accionado por** | Usuario |
| **Actores** | Emisor de medios de pago<br>Cámara de compensación |

| | |
|---|---|
| | Usuario |
| **Descripción del caso de uso** | Un usuario solicita en un punto de atención a pasajeros correspondiente al tipo de medio de pago, la reconstrucción de su medio de pago dañado o extraviado en un nuevo medio de pago.<br><br>El emisor de medios de pago debe reconstruir los datos del medio de pago usando la información recolectada de los eventos ocurridos en dicho medio de pago. Para reconstruir el nuevo medio de pago se deben efectuar las siguientes acciones:<br><br>Emisión del nuevo medio de pago con los productos que y el perfil que tenía en su medio de pago anterior.<br><br>Activavion y Personalizacion del médio de pago.<br><br>Recarga de valor de los productos que tenía almacenados en su medio de pago anterior.<br>Envío de la información de los eventos efectuados en la reconstrucción a la Cámara de compensación. |

## 11.9 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 24 – Secuencia de casos de uso necesarios para el bloqueo o desactivación del medio de pago**

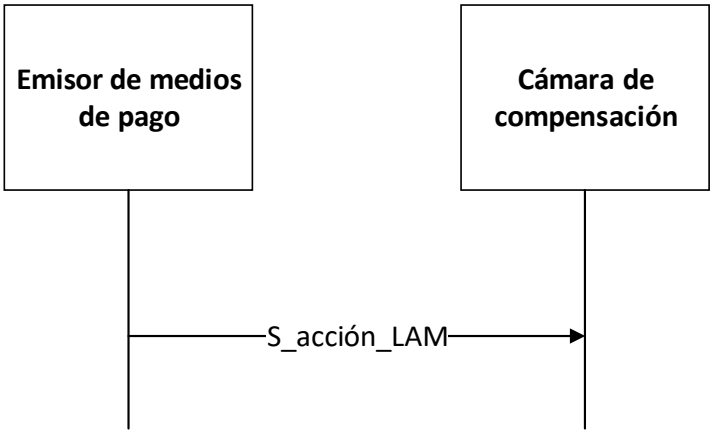



A continuación se describen los tres casos de uso que se deben efectuar para lograr el bloqueo o desactivación de un medio de pago.

| | |
|---|---|
| **Nombre del caso de uso** | **Solicitud de acción de bloqueo o desactivación con lista LAM** |

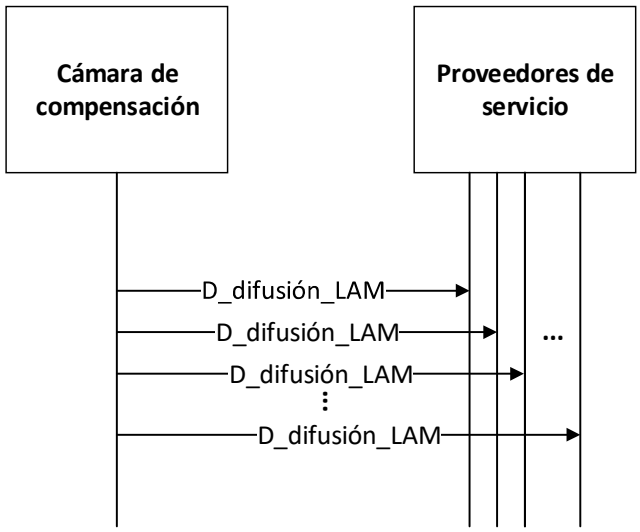
| | |
|---|---|
| **Resumen** | El usuario o alguno de los actores del sistema tienen un motivo valido por el cual es necesario el bloqueo o desactivación de un medio de pago que se ha emitido. |
| **Prerrequisitos** | Emisión de cualquier tipo de medio de pago |
| **Accionado por** | Los usuarios de los medios de pago o cualquier actor del sistema interoperable |
| **Actores** | Punto de atención a pasajeros o<br>Direccion del sistema integrado de recaudo o<br>Cámara de compensación o<br>Usuarios de medios de pago o |
| **Descripción del caso de uso** | Desde el punto de atención a pasajeros o desde la dirección del sistema integrado de recaudo se 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. |

**Figura 25 – Evento enviado durante la solicitud de acción de bloqueo o desactivación con lista LAM**



| Nombre del caso de uso | Difusión de acción de bloqueo o desactivación con lista LAM |
|---|---|
| **Resumen** | La Cámara de compensación difunde un mensaje de acción de bloqueo o desactivación con lista LAM hacia los prestadores de servicio. |
| **Prerrequisitos** | Solicitud de acción de bloqueo o desactivación con lista LAM |
| **Accionado por** | Cámara de compensación |
| **Actores** | Prestadores de servicio<br>Cámara de compensación |
| **Descripción del caso de uso** | La Cámara de compensación analiza y aprueba una solicitud de acción con lista LAM. Una vez aprobada la solicitud, se difunde un mensaje que actualiza la lista LAM en los dispositivos de todos los prestadores de servicio. |

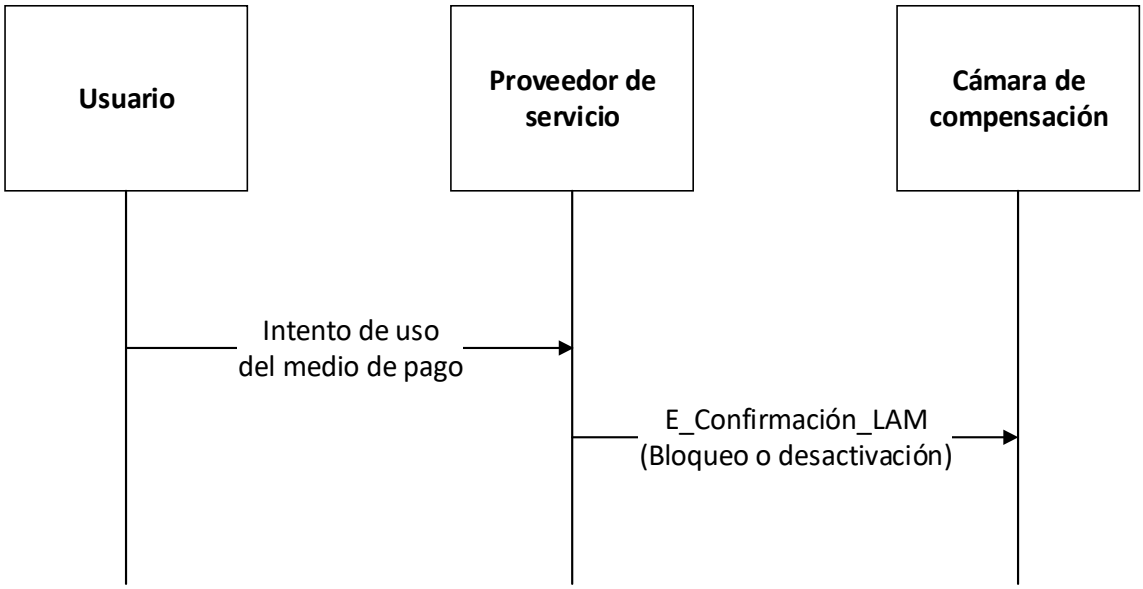
**Figura 26 – Evento enviado durante la difusión de acción de bloqueo o desactivación con lista LAM**




| Nombre del caso de uso | Ejecución de acción de bloqueo o desactivación con |
|---|---|

| | **lista LAM** |
|---|---|
| **Resumen** | Un usuario intenta validar un medio de pago al cual se le debe aplicar una acción de bloqueo o desactivación de lista LAM |
| **Prerrequisitos** | Difusión de acción de bloqueo o desactivación con lista LAM |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario intenta validar su medio de pago para acceder a un servicio de la red interoperable acercándolo a un dispositivo de validación de medios de pago.<br>El prestador de servicio al cual se le solicita el acceso realiza las siguientes acciones con dicho dispositivo:<br>Verificación de la existencia de una acción disponible para el medio de pago presentado en lista LAM.<br>Ejecución de la acción en el medio de pago mediante escritura de datos.<br>Almacenamiento del evento de ejecución de la acción con lista LAM<br>Envío de una confirmación del evento efectuado a la Cámara de compensación |

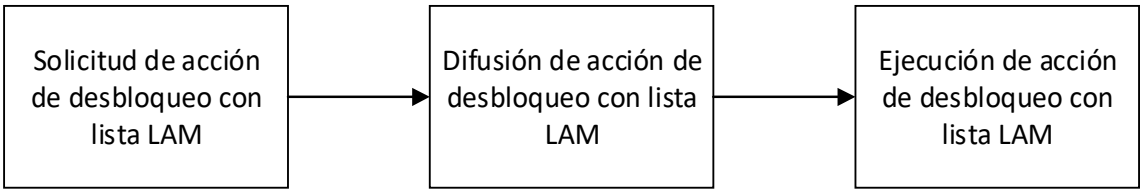
Figura 27 – Eventos enviados durante la ejecución de acción de bloqueo o desactivación con lista LAM




## 11.10 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.

Figura 28 – Secuencia de casos de uso necesarios para el desbloqueo del medio de pago

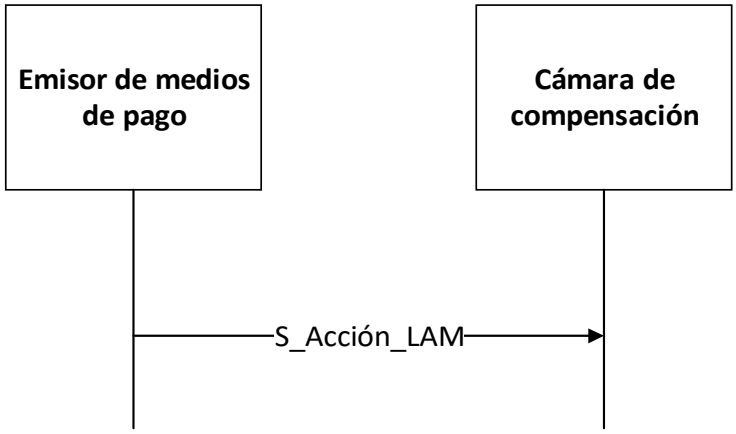



A continuación se describen los tres casos de uso que se deben efectuar para lograr el desbloqueo de un medio de pago.

| **Nombre del caso de uso** | **Solicitud de acción de desbloqueo con lista LAM** |
|---|---|
| **Resumen** | Alguno de los actores del sistema tiene un motivo valido 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** | Punto de atención a pasajeros o |

| | |
|---|---|
| | Direccion del sistema integrado de recaudo |
| **Descripción del caso de uso** | Desde un punto de atención a pasajeros o desde la<br>Direccion del sistema integrado de Recaudo se envía a la Cámara de compensación un mensaje donde solicita la actualización de la lista LAM con una operación de reactivación sobre un medio de pago. |

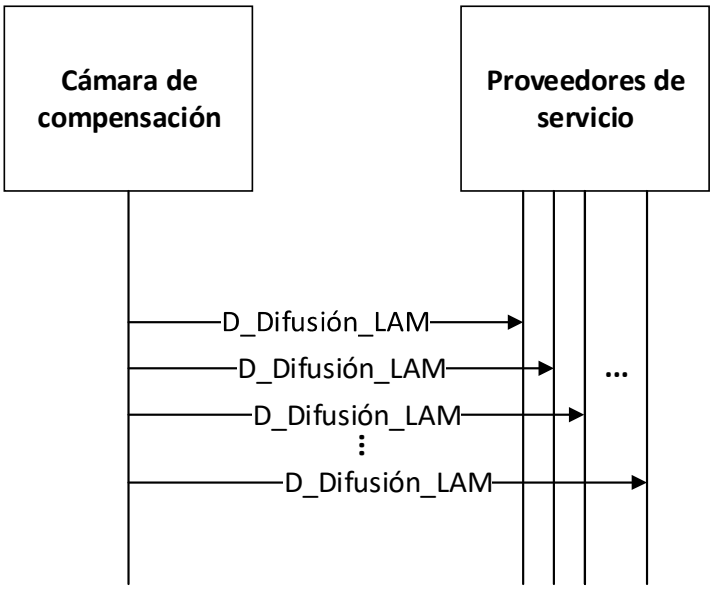
**Figura 29 – Eventos enviados durante la solicitud de acción de desbloqueo con lista LAM**




| **Nombre del caso de uso** | **Difusión de acción de desbloqueo con lista LAM** |
|---|---|
| **Resumen** | La Cámara de compensación difunde un mensaje de acción de desbloqueo con lista LAM hacia los prestadores de servicio. |
| **Prerrequisitos** | Solicitud de acción de desbloqueo con lista LAM |
| **Accionado por** | Cámara de compensación |
| **Actores** | Prestadores de servicio<br>Cámara de compensación |
| **Descripción del caso de uso** | La Cámara de compensación analiza y aprueba una solicitud de acción con lista LAM. Una vez aprobada la solicitud, se difunde un mensaje que actualiza la lista LAM en los dispositivos de todos los prestadores de |

| | |
|---|---|
| | servicio. |

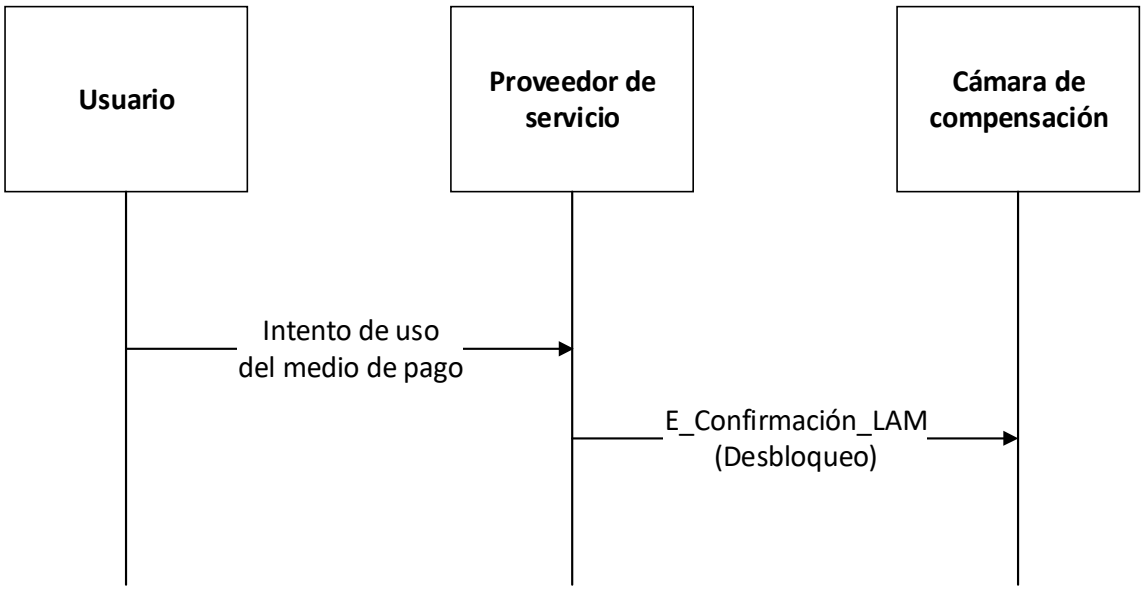
**Figura 30 – Eventos enviados durante la difusión de acción de desbloqueo con lista LAM**




| Nombre del caso de uso | Ejecución de acción de desbloqueo con lista LAM |
|---|---|
| **Resumen** | Un usuario intenta validar un medio de pago al cual se le debe aplicar una acción de desbloqueo con la lista LAM |
| **Prerrequisitos** | Difusión de acción de desbloqueo hacia lista LAM |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario intenta validar su medio de pago para acceder a un servicio de la red interoperable acercándolo a un dispositivo de validación de medios de pago.<br>El prestador de servicio al cual se le solicita el acceso |

| | |
|---|---|
| | realiza las siguientes acciones con dicho dispositivo:<br><br>Verificación de la existencia de una acción disponible para el medio de pago presentado.<br>Ejecución de la acción en el medio de pago mediante escritura de datos.<br>Almacenamiento del evento de ejecución de la acción con lista LAM<br>Envío de una confirmación del evento efectuado a la Cámara de compensación |

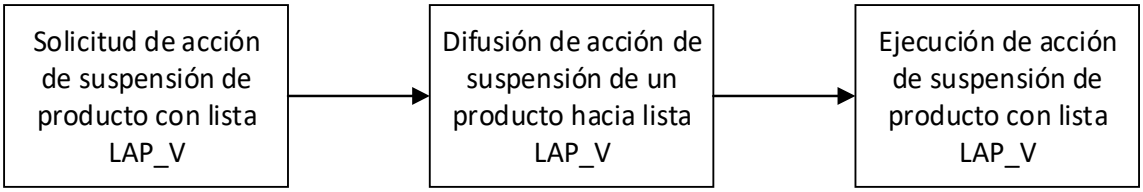
**Figura 31 – Eventos enviados durante la ejecución de acción de desbloqueo con lista LAM**




## 11.11 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 32 – Secuencia de casos de uso necesarios para la suspensión de productos**

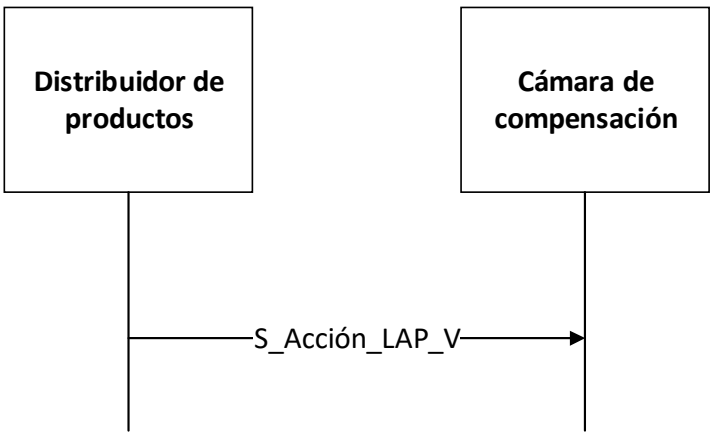



A continuación se describen los tres casos de uso que se deben efectuar para lograr la suspensión de un producto.

| **Nombre del caso de uso** | **Solicitud de acción de suspensión de producto con lista** |
|---|---|

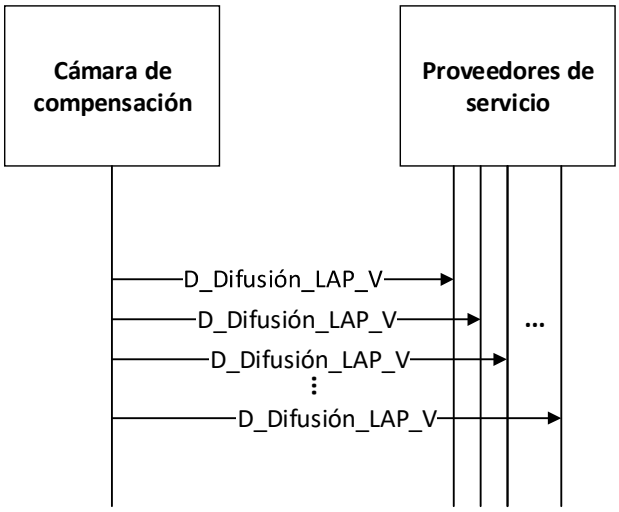
| | LAP_V |
|---|---|
| **Resumen** | Un distribuidor de productos adquiere un motivo por el cual es necesaria la suspensión de un producto almacenado en un medio de pago |
| **Prerrequisitos** | Emisión de medio de pago anónimo o<br>Emisión de medio de pago personalizado o<br>Emisión de medio de pago personalizado con BPD o<br>Adquisición de un producto |
| **Accionado por** | Distribuidor de productos |
| **Actores** | Distribuidor de productos<br>Cámara de compensación |
| **Descripción del caso de uso** | El distribuidor de productos envía a la Cámara de compensación un mensaje donde solicita la actualización de la lista LAP_V con una operación de suspensión de un producto almacenado en un medio de pago. |

**Figura 33 - Eventos enviados durante la solicitud de acción de suspensión de producto con lista LAP_V**



| Nombre del caso de uso | Difusión de acción de suspensión de un producto hacia lista LAP_V |
|---|---|
| Resumen | La Cámara de compensación difunde un mensaje de acción de suspensión de producto hacia los prestadores de servicio. |
| Prerrequisitos | Solicitud de acción de suspensión de producto con lista LAP_V |
| Accionado por | Cámara de compensación |
| Actores | Prestadores de servicio<br>Cámara de compensación |
| Descripción del caso de uso | La Cámara de compensación analiza y aprueba una solicitud de acción con lista LAP_V para suspender un producto. Una vez aprobada la solicitud, se difunde un mensaje que actualiza la lista LAP_V en los dispositivos de todos los prestadores de servicio. |

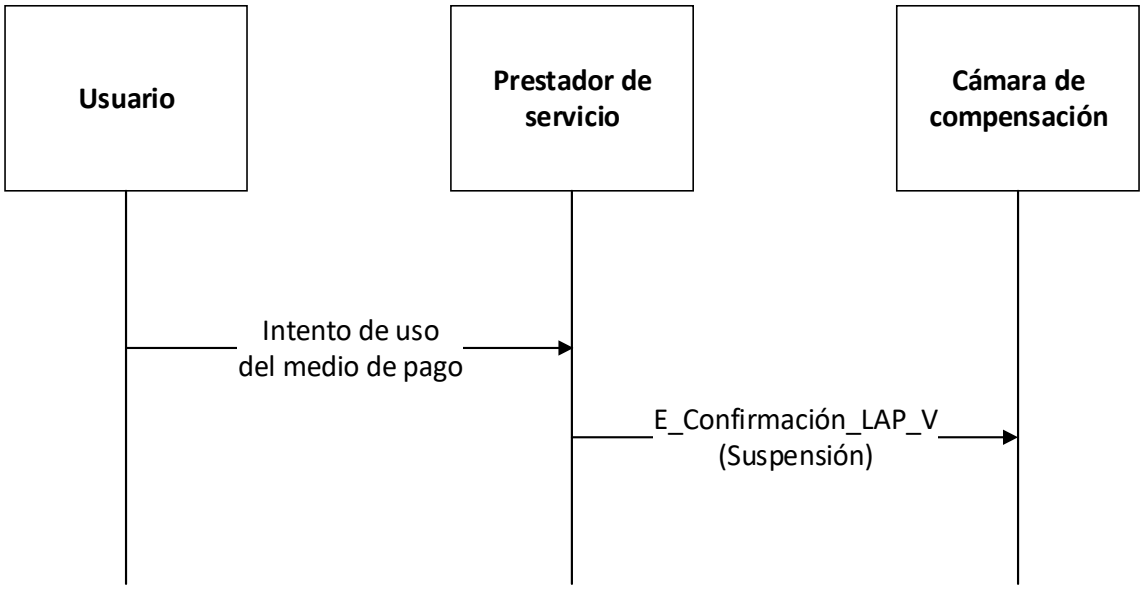
**Figura 34 – Eventos enviados durante la difusión de acción de suspensión de un producto hacia lista LAP_V**




| Nombre del caso de uso | Ejecución de acción de suspensión de producto con lista LAP_V |
|---|---|

| | |
|---|---|
| **Resumen** | Un usuario intenta validar un medio de pago al cual se le debe aplicar una acción de suspensión con la lista LAP_V |
| **Prerrequisitos** | Difusión de acción de suspensión de producto con lista LAP_V |
| **Accionado por** | Usuario |
| **Actores** | Prestador de servicio<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario intenta validar su medio de pago para acceder a la red interoperable acercándolo a un dispositivo de validación de medios de pago.<br>El prestador de servicio al cual se le solicita el acceso realiza las siguientes acciones con dicho dispositivo:<br>Verificación de la existencia de una acción disponible para el medio de pago presentado.<br>Ejecución de la acción en el medio de pago mediante escritura de datos.<br>Almacenamiento del evento de ejecución de la acción con lista LAP_V<br>Envío de una confirmación del evento efectuado a la Cámara de compensación |

Figura 35 – Eventos enviados durante la ejecución de acción de suspensión de producto con lista LAP_V



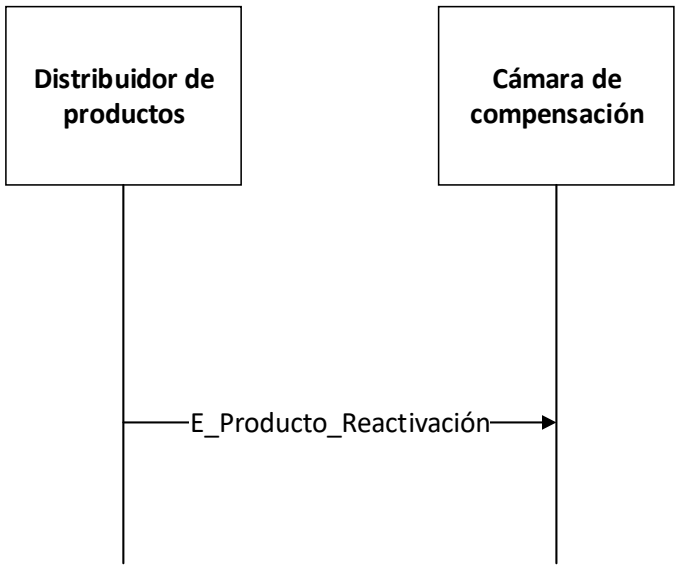

## 11.12 Reactivación de productos

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_V |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos<br>Cámara de compensación<br>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.<br><br>El usuario propietario del medio de pago al cual se desea reactivar el producto se presenta ante el distribuidor de productos.<br><br>El distribuidor de productos realiza las siguientes operaciones a través de un dispositivo de lector de medios de pago:<br><br>Escritura de la información necesaria en el medio de pago para reactivar el producto.<br>Almacenamiento de la información del evento en el dispositivo.<br>Envío de la información del evento a la Cámara de compensación. |

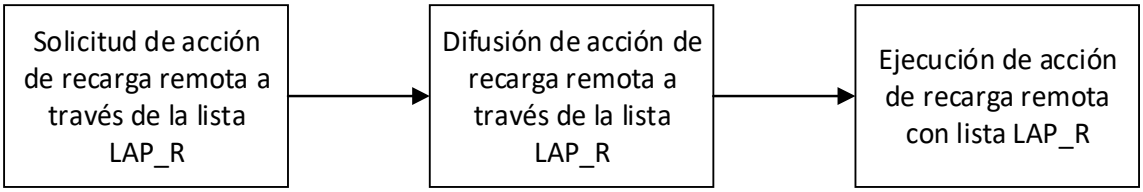
**Figura 36 – Eventos enviados durante la reactivación de un producto**




## 11.13 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.

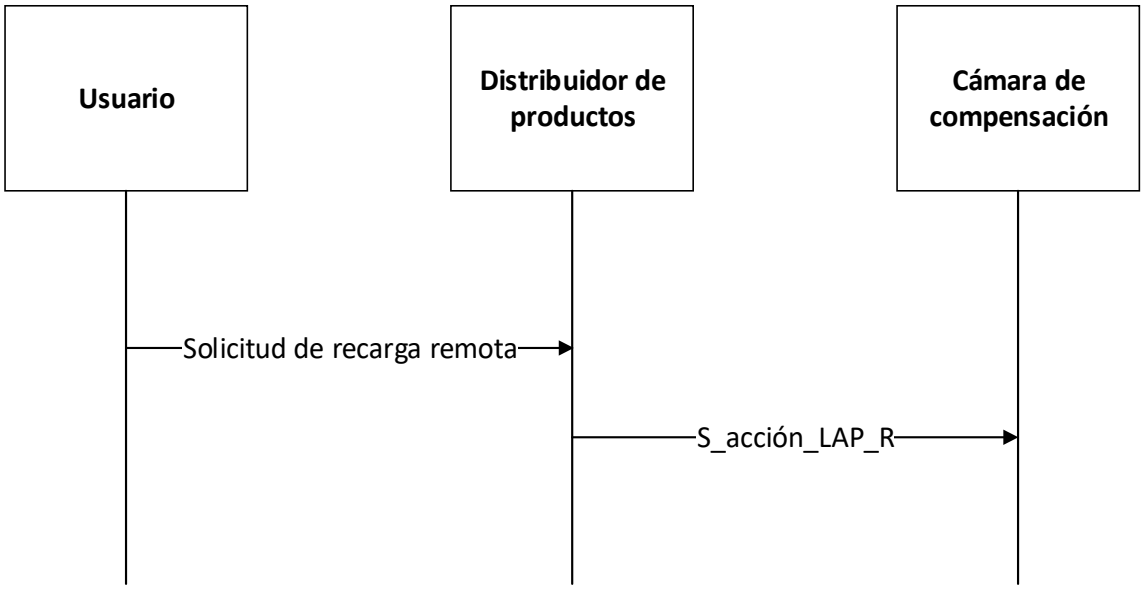
Figura 37 – Secuencia de casos de uso necesarios para la recarga remota de productos




A continuación se describen diferentes casos de uso que pueden llevarse a cabo para recargar productos en diferentes condiciones.

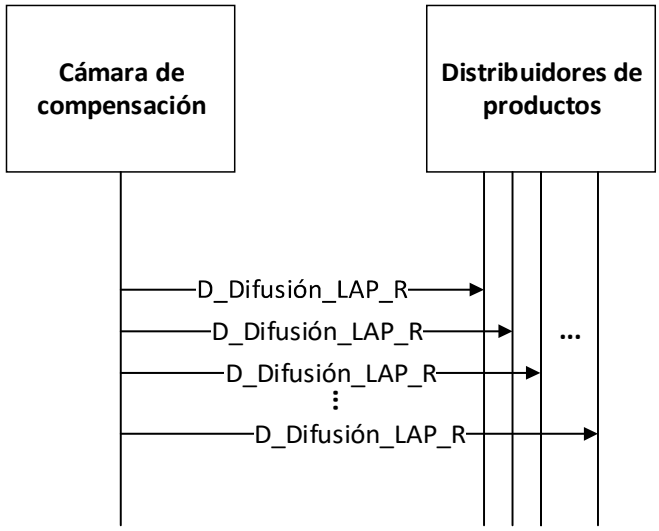
| **Nombre del caso de uso** | **Solicitud de acción de recarga remota a través de la lista LAP_R** |
|---|---|
| **Resumen** | Un usuario solicita, a un distribuidor de recargas, la recarga remota de un producto almacenado en su medio de pago. |
| **Prerrequisitos** | Emisión de medio de pago de tarifa general o preferencial<br>Activación y personalización de medio de pago |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de recargas<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | El usuario solicita y paga a un distribuidor de productos 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.<br>El distribuidor de productos hace la solicitud de la recarga remota a la Cámara de compensación. |
| **Nota:** | Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar en caso de sobrepasarlos dejara pendiente la recarga e informara al pasajero |

Figura 38 – Eventos enviados durante la solicitud de acción de recarga remota a través de la lista LAP_R




| **Nombre del caso de uso** | **Difusión de acción de recarga remota a través de la lista LAP_R** |
|---|---|
| **Resumen** | La Cámara de compensación realiza la difusión de la acción de recarga remota a los dispositivos de recarga del producto a recargar. |
| **Prerrequisitos** | Solicitud de acción de recarga remota a través de la lista LAP_R |
| **Accionado por** | Cámara de compensación |
| **Actores** | Distribuidor de productos<br>Cámara de compensación |
| **Descripción del caso de uso** | La Cámara de compensación analiza y aprueba una solicitud de acción con lista LAP_R para realizar la recarga de valor de un producto. Una vez aprobada la solicitud, se difunde un mensaje que actualiza la lista LAP_R en los dispositivos autorizados para la recarga de dicho producto. |

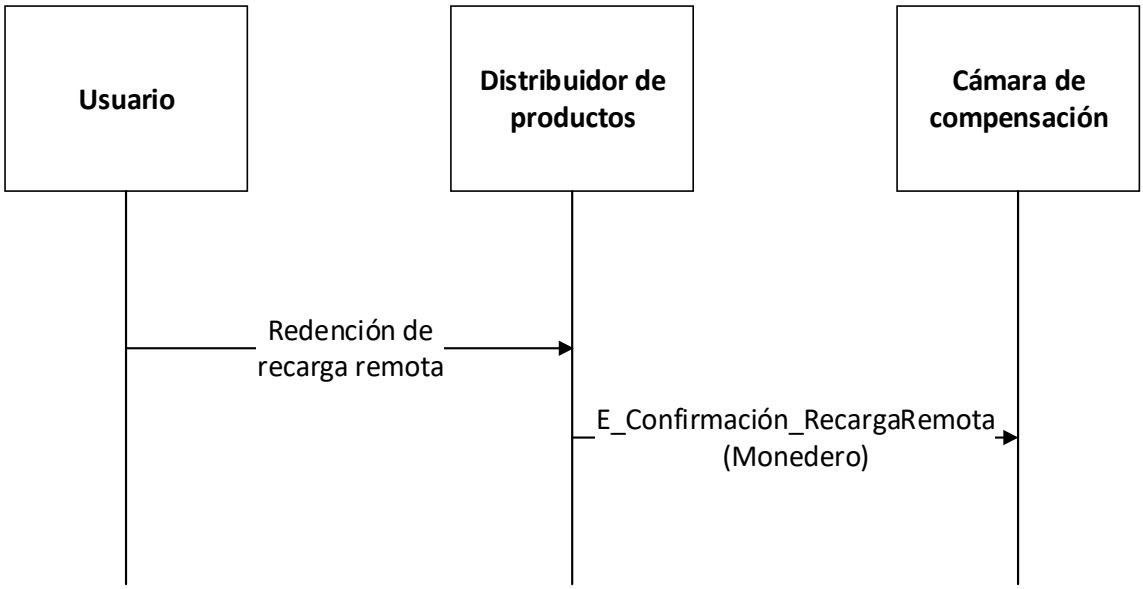
Figura 39 – Eventos enviados durante la difusión de acción de recarga remota a través de la lista LAP_R




| **Nombre del caso de uso** | **Ejecución de acción de recarga remota de Monedero con lista LAP_R y saldo de Crédito igual a cero** |
|---|---|
| **Resumen** | Un usuario lleva su medio de pago para aplicar una recarga remota que ha realizado previamente. |
| **Prerrequisitos** | Difusión de acción de recarga remota a través de lista LAP_R |
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario presenta su medio de pago en un dispositivo de recarga y solicita la aplicacon de su recarga.<br>El distribuidor de productos realiza las siguientes acciones con dicho dispositivo:<br>Verificación de la existencia de una acción de recarga remota disponible para el medio de pago y el producto presentado.<br>Ejecución de la acción de recarga del producto Monedero en el medio de pago mediante escritura de datos. |

| | |
|---|---|
| | Almacenamiento del evento de ejecución de la acción con lista LAP_R<br>Envío de una confirmación del evento efectuado a la Cámara de compensación |
| **Nota:** | Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar en caso de sobrepasarlos dejara pendiente la recarga e informara al pasajero |

**Figura 40 – Eventos enviados durante la ejecución de acción de recarga remota de Monedero con lista LAP_R y saldo de Crédito igual a cero**

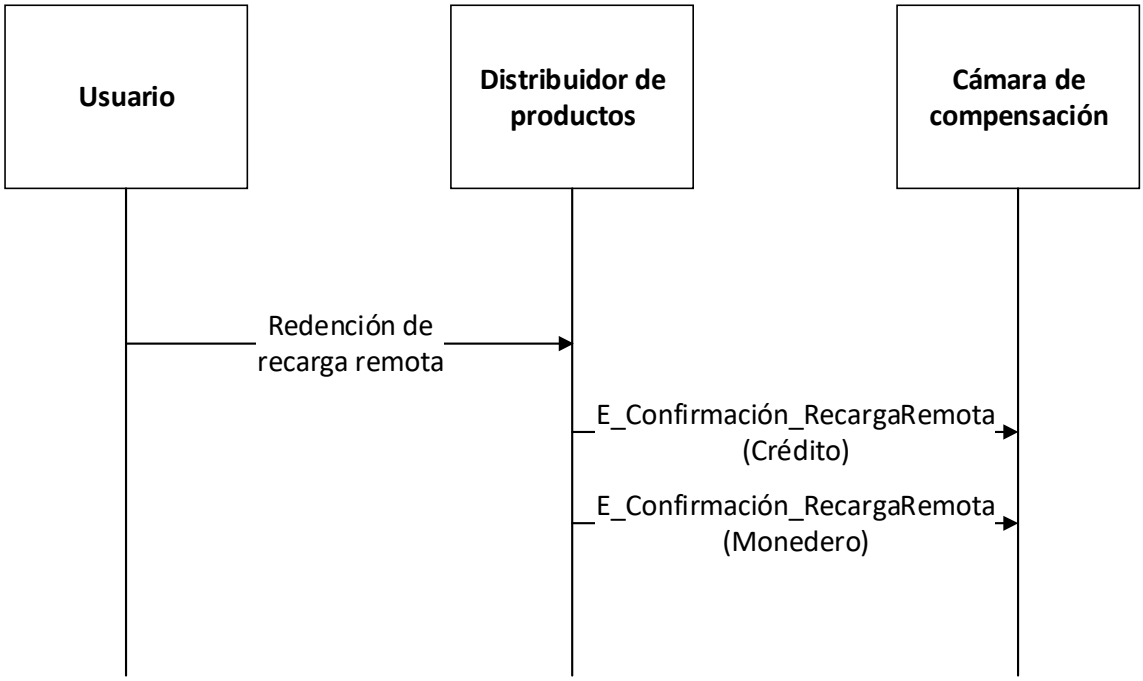



Un usuario ejecuta una acción previa de recarga remota del producto de Monedero en su medio de pago y el valor del producto Crédito es diferente de cero. Posteriormente se acerca a un dispositivo de venta y recarga de medios de pago para aplicar la recarga que ha pagado.

| **Nombre del caso de uso** | **Ejecución de acción de recarga remota de Monedero con lista LAP_R y saldo de Crédito diferente de cero** |
|---|---|
| **Resumen** | Un usuario lleva su medio de pago para aplicar una recarga remota que ha realizado previamente. |
| **Prerrequisitos** | Difusión de acción de recarga remota a través de lista LAP_R |

| | |
|---|---|
| **Accionado por** | Usuario |
| **Actores** | Distribuidor de productos<br>Cámara de compensación<br>Usuario |
| **Descripción del caso de uso** | Un usuario presenta su medio de pago en un dispositivo de recarga y solicita la redención de su recarga.<br>El distribuidor de productos realiza las siguientes acciones con dicho dispositivo:<br>Verificación de la existencia de una acción de recarga remota disponible para el medio de pago y el producto presentado.<br>Ejecución de la acción de recarga del producto Crédito en el medio de pago por el saldo del producto Crédito<br>Ejecución de la acción de recarga del producto Monedero en el medio de pago por el valor excedente después de recargar el producto Crédito<br>Almacenamiento de los eventos de ejecución de la acción con lista LAP_R<br>Envío de una confirmación del evento efectuado a la Cámara de compensación |
| **Nota:** | **Deberán respetarse los parámetros máximos y minimos de monto que el monedero pueda almacenar en caso de sobrepasarlos dejara pendiente la recarga e informara al pasajero** |

**Figura 41 – Eventos enviados durante la ejecución de acción de recarga remota de Monedero con lista LAP_R y saldo de Crédito diferente de cero**



# 12 Seguridad en el envío de eventos

Los procesos de recolección y envío de eventos requieren del uso de firmas digitales basadas en la recomendación ITU-T X.509 (ITU-T) de Infraestructura de Llave Pública (PKI), Emitidas por la Dirección del Sistema Integrado de Recaudo. 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.

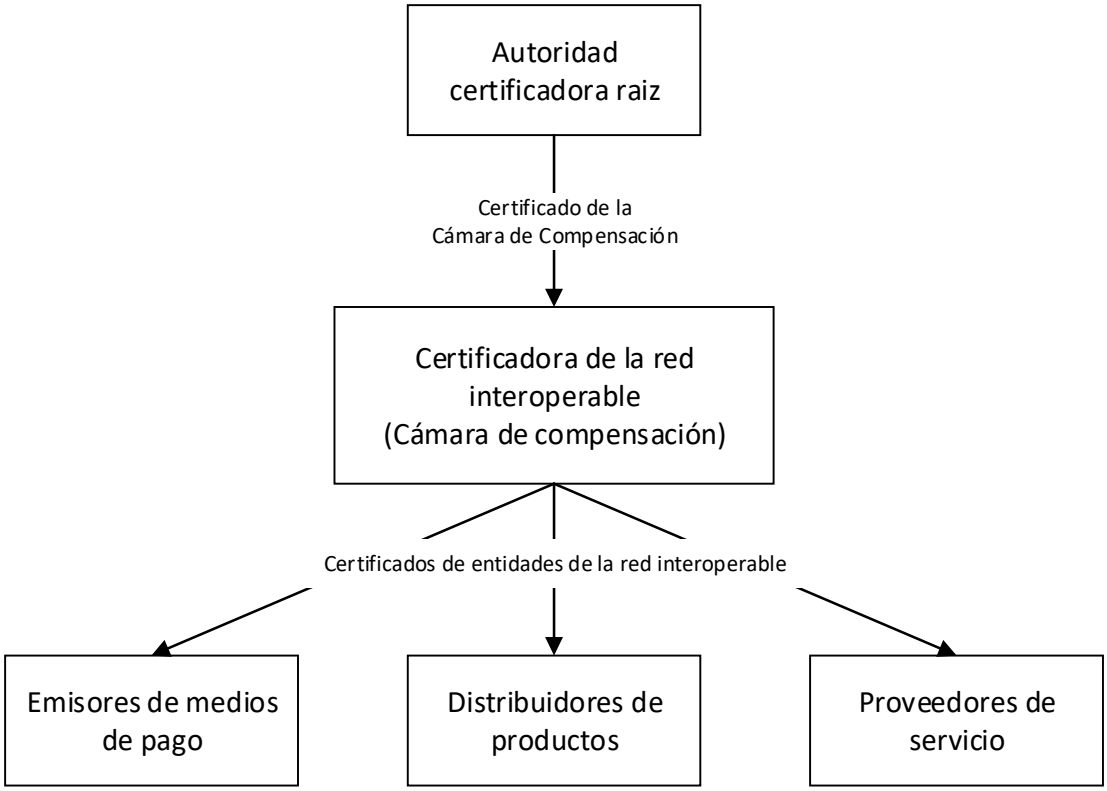
## 12.1 Estructura de seguridad

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 la Direccion del Sistema Integrado de Recaudo 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 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.

El proceso de generación de certificados se basa en la recomendación ITU-T X-509 (ITU-T) y debe ser llevado a cabo de acuerdo con la siguiente figura:

Figura 42 – Infraestructura de llave pública en la red interoperable




## 12.2 Firma de archivos

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 (W3C Recommendation: XML Signature Syntax and Processing (Second Edition), 2008) 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 definido para Esquema de envío de eventos con firma digital

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 una lista 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 el esquema para la lista de revocación de certificados (CRL). Esta está compuesta por las siguientes secciones:

Encabezado de archivo
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 Registrar. |
| **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 compuesta 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 (W3C Recommendation: XML Signature Syntax

and Processing (Second Edition), 2008) 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

# 13 Especificación de los módulos de acceso seguro (SAM)

## 13.1 Introducción

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 la Direccion del Sistema Integrado de Recaudo. Los módulos SAM a ser entregados deben ser usar la tecnología MIFARE SAM AV2 (NXP, P5DF081 MIFARE SAM AV2 functional specification, document number 191732) en modo AV2.

## 13.2 Tipos de SAM

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. La estructura de los SAM y los diferentes tipos de SAM son listados en el documento del Mapping del sistema interoperable. Del mismo modo la forma de obtener el *ConsecutivoSAM* también se describe en ese documento.

## 13.3 Estructura de los SAM

A continuación se describe los distintos tipos de módulos SAM. Dicho contenido incluye las llaves que deben ser almacenadas, la posición y versión en la cual se almacena cada llave dentro del SAM así como el tipo de llaves emitidas por la Dirección del Sistema Integrado de Recaudo.

- SAM de inicialización
- SAM de emisión
- SAM de emisión de medios de pago precargados
- SAM de distribución y recarga de Monedero
- SAM de distribución y recarga de Monedero y Crédito
- SAM de distribución y recarga de BPD
- SAM de distribución y recarga de Monedero, Crédito y BPD
- SAM de uso de productos

# 14 Resumen de los datos que deben ser asignados por el Registrar.

A lo largo del presente documento se han mencionado diferentes campos y valores que deben ser asignados por el Registrar. Este capítulo presenta un resumen de dichos valores y el momento en que deben ser asignados. Todas las versiones de datos de la aplicación interoperable representan una bifurcación en la operación desde el firmware ya que estos cambios representan formas diferentes de operar el mapping o alguna sección del mismo. Esto indica que todas las versiones anteriores del mapping pueden operarse, cada una con sus funcionalidad. Adicionalmente se realiza una discriminación de los datos según la relevancia de los mismos.

## 14.1 Datos relevantes para toda 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 (Comité rector)** | |
| | |

## 14.2 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 del algoritmo de seguridad** | Cada vez que se haga una modificación en |

| | |
|---|---|
| **usado en la aplicación interoperable** | los algoritmos de seguridad de la red 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 |

## 14.3 Datos relevantes para el producto Monedero

| Nombre del dato | Momento de asignación |
|---|---|
| **Identificador del producto Monedero** | Antes de la constitución de la red interoperable o cada vez que el Registrar considere adecuado modificar un valor |
| **Prioridad del producto Monedero** | |
| **Mínimo valor que puede almacenar cada producto** | |
| **Máximo valor que puede almacenar cada producto** | |
| **Días de la semana en los que no se puede usar el producto** | |
| **Número máximo de viajes que se pueden efectuar cada día de la semana** | |
| **Tiempo de passback** | |
| **Passbacks permitidos** | |
| **Tiempo de transbordo** | |
| **Transbordos permitidos dentro del tiempo de transbordo** | |

## 14.4 Datos relevantes para el producto Crédito

| Nombre del dato | Momento de asignación |
|---|---|
| **Identificador del producto Crédito** | Antes de la constitución de la red interoperable o cada vez que el Registrar |
| **Prioridad del producto Crédito** | |

| | |
|---|---|
| **Mínimo valor que puede almacenar cada producto** | considere adecuado modificar un valor |
| **Máximo valor que puede almacenar cada producto** | |
| **Días de la semana en que no se puede usar el producto** | |
| **Número máximo de viajes que se pueden efectuar cada día de la semana** | |
| **Tiempo de passback** | |
| **Passbacks permitidos** | |
| **Tiempo de transbordo** | |
| **Transbordos permitidos dentro del tiempo de transbordo** | |

## 14.5 Datos relevantes para el producto BPD

| Nombre del dato | Momento de asignación |
|---|---|
| **Identificador del producto BPD** | Antes de la constitución de la red interoperable o cada vez que el Registrar considere adecuado modificar un valor |
| **Prioridad del producto BPD** | |
| **Mínimo valor que puede almacenar cada producto** | |
| **Máximo valor que puede almacenar cada producto** | |
| **Días de la semana en que no se puede usar el producto** | |
| **Número máximo de viajes que se pueden efectuar cada día de la semana** | |
| **Tiempo de passback** | |

| | |
|---|---|
| **Passbacks permitidos** | |
| **Tiempo de transbordo** | |
| **Transbordos permitidos dentro del tiempo de transbordo** | |

## 14.6 Datos relevantes para cada emisor de medios de pago

| Nombre del dato | Momento de asignación |
|---|---|
| **Llave del emisor (Llave E)** | Durante el ingreso a la red interoperable |
| **Identificador de la red a la cual pertenece cada entidad** | |
| **Identificador de cada emisor de medios de pago** | |
| **Identificador de cada dispositivo de la red interoperable** | |
| **Identificador de entidad para envío de eventos entre nivel 3-4** | |
| **Versión de la llave de emisión para cada emisor de medios de pago en un I_SAM** | |

## 14.7 Datos relevantes para cada distribuidor de productos

| Nombre del dato | Momento de asignación |
|---|---|
| **Identificador de la red a la cual pertenece cada entidad** | Durante el ingreso a la red interoperable |
| **Identificador de cada distribuidor de medios de pago** | |
| **Identificador de cada dispositivo de la red interoperable** | |
| **Identificador de entidad para envío de** | |

| | |
|---|---|
| **eventos entre nivel 3-4** | |

### 14.8 Datos relevantes para cada prestador de servicio

| **Nombre del dato** | **Momento de asignación** |
|---|---|
| **Identificador de la red a la cual pertenece cada entidad** | Durante el ingreso a la red interoperable |
| **Identificador de cada prestador de servicio** | |
| **Identificador de entidad para envío de eventos entre nivel 3-4** | |

# 15 Referencias


*Anexo 1. Estructura de archivos interoperable en medios de pago Mifare DESFire.* (2015).

(2015). *Anexo 1.* MANUAL DE PROCESOS PARA LA IMPLEMENTACION DEL SISTEMA PAGO ELECTRÓNICO EN EL LOS SISTEMAS DE TRANSPORTE PÚBLICO MASIVO Y COLECTIVO, ASÍ COMO OTRAS MODALIDADES DE TRANSPORTE DE PASAJEROS QUE SE ADHIERAN, EN ÁREAS METROPOLITANAS Y CIUDADES MEDIAS DEL ESTADO DE JALISCO

*Anexo 2. Esquema para envío de eventos.* (2015).

*Anexo 3. Esquema de envío de eventos con firma digital.* (2015).

*Anexo 4. Esquema para la lista de revocación de certificados (CRL).* (2015).

*Anexo 5. Documentos para ejecución de pruebas.* (2015).

*Anexo 6. Estructura de archivos en medio de pago interoperable durante ejecución de pruebas.* (2015).

*Anexo 7. Formatos genéricos para ejecución de pruebas de niveles 3 a 4 y 0 a 4 de la red interoperable.* (2015).

BSI. (2005). *BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements.*

BSI. (2005). *BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists.*

*FIPS PUB 197 Advanced Encryption Standard (AES)*. (Noviembre de 2001). Obtenido de http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

ISO. (2007). *ISO 24014-1 Public transport - Interoperable fare management system - Part 1: Architecture.*

ISO/IEC. (2008). *ISO/IEC 14443-4 Identification cards - Contactless integrated circuit cards - Proximity cards - Part4: Transmission protocol.*

ISO/IEC. (2013). *ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange.*

ISO/IEC. (2011). *ISO/IEC 9797-1 Information technology -- Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher.*

ITU-T. *Recomendación X.509.*

NIST. (2005). *Recomendation for Block Cipher Moder of Operation: The CMAC Mode for Authentication NIST Special Publication SP 800-38 B.*

NXP. (2014). *Data sheet - MF0ULx1 MIFARE Ultralight EV1 - Contactless ticket IC Rev 3.1.*

NXP. (2011). *Data sheet - MF3ICD81 MIFARE DESFire EV1 Rev. 3.6 document number 134036.*

NXP. *P5DF081 MIFARE SAM AV2 functional specification, document number 191732.*

NXP. (2010). *Symmetric key diversifications AN10922 Rev 1.3.*

*W3C Recommendation: XML Signature Syntax and Processing (Second Edition)*. (10 de junio de 2008). Obtenido de http://www.w3.org/TR/xmldsig-core/