



Latin America & The Caribbean



## ***Consideraciones para el Desarrollo de Pagos Abiertos en los Sistemas de Transporte Público en América Latina y el Caribe***

### ***Documento con los Requerimientos Mínimos de:***

- American Express
- MasterCard Worldwide
- Visa Inc.

Centro de Excelencia de SCALA

*Fecha de Publicación: Julio 2015*

**Smart Card Alliance Latino América – SCALA**

Local # 7 – Edificio 237

Tecno parque – Ciudad Del Saber

Ciudad de Panamá, República de Panamá

[www.sca-la.org](http://www.sca-la.org)

## ***Acerca de SCALA – Smart Card Alliance Latino América***

SCALA – Smart Card Alliance Latino América es un capítulo del Smart Card Alliance, una asociación sin fines de lucro, imparcial, que impacta múltiples industrias, la cual trabaja para estimular la comprensión, interoperabilidad, convergencia, evolución, y la adopción innovadora de aplicaciones de la tecnología de tarjeta de circuito integrado (ICC) en los Estados Unidos, América Latina, y el Caribe. SCALA logra sus objetivos a través de proyectos específicos como: *Programas Educativos, Centro de Excelencia, Investigaciones de Mercado, Promociones de Casos de Éxito, Hojas de Ruta, Recursos en Línea, Relaciones en industrias afectadas y foros abiertos*, manteniendo a sus afiliados conectados con líderes de la industria y el pensamiento innovador.

Smart Card Alliance funge como la voz única de la industria para los temas relacionados con las tarjetas con circuito integrado y componentes relacionados, liderando las conversaciones de la industria sobre el impacto y el valor agregado de esta tecnología en las Américas.

Para obtener más información sobre SCALA visite: [www.sca-la.org](http://www.sca-la.org)

O Smart Card Alliance visite: [www.smartcardalliance.org](http://www.smartcardalliance.org)

Derechos de Copia © 2015 Smart Card Alliance, Inc. Todos los derechos reservados, la reproducción o distribución de esta publicación, en cualquier forma está prohibida sin la previa autorización del Smart Card Alliance. Smart Card Alliance ha realizado su mejor esfuerzo para conseguir, pero no puede garantizar, que la información descrita en este reporte es exacta a la fecha de publicación. El Smart Card Alliance no garantiza que la información de este reporte sea exacta, que se encuentre completa o que sea adecuada.

# TABLA DE CONTENIDO

<b>1</b>	<b>INTRODUCCIÓN</b>	<b>4</b>
1.1	OBJETIVO	4
<b>2</b>	<b>ANTECEDENTES DE LOS SISTEMAS DE COBRO</b>	<b>5</b>
2.1	DISPOSITIVOS SIN PREPAGO	5
2.2	DISPOSITIVOS CON PREPAGO	5
2.3	TARJETAS CON BANDA MAGNÉTICA	5
2.4	TARJETAS INTELIGENTES (“SMART CARDS”)	5
2.4.1	<i>Tarjetas con contacto</i>	5
2.4.2	<i>Tarjetas sin contacto</i>	6
2.4.3	<i>Tarjetas híbridas</i>	6
2.4.4	<i>Tarjetas de Doble Interfaz</i>	6
2.5	BOTÓN O COSPEL ELECTRÓNICO	6
2.6	NFC (NEAR FIELD COMMUNICATION)	6
<b>3</b>	<b>REPASO GENERAL EMV</b>	<b>7</b>
3.1	EMV, SIN CONTACTO Y NFC	7
3.1.1	<i>EMV Sin Contacto (contactless)</i>	7
3.1.2	<i>EMV y los Pagos Móviles con NFC</i>	8
<b>4</b>	<b>SISTEMAS PROPIETARIOS EN TRANSPORTE</b>	<b>9</b>
4.1	MIFARE	9
4.2	CALYPSO	9
4.3	FELICA	10
4.4	CIPURSE	10
<b>5</b>	<b>CONSIDERACIONES PARA PAGOS ABIERTOS SIN CONTACTO EN TRANSPORTE PÚBLICO</b>	<b>12</b>
5.1	REQUERIMIENTOS DE LAS TARJETAS	12
5.1.1	<i>Requerimientos mínimos para Tarjetas de la marca Visa</i>	13
5.1.2	<i>Requerimientos mínimos para Tarjetas de la marca MasterCard</i>	14
5.1.3	<i>Requerimientos mínimos para Tarjetas de marca American Express</i>	14
5.1.4	<i>Requerimientos mínimos para Tarjetas de otras Marcas</i>	15
<b>6</b>	<b>BENEFICIOS DE LOS ESTÁNDARES ABIERTOS</b>	<b>16</b>
6.1	SEGURIDAD	16
6.2	BANCARIZACIÓN	16
6.3	REDUCCIÓN DEL TIEMPO DE TRANSACCIÓN	16
6.4	DISPONIBILIDAD DE LA INFORMACIÓN DE LAS TRANSACCIONES	16
6.5	INTEROPERABILIDAD	17
6.6	EFICIENCIA	17
<b>7</b>	<b>CONCLUSIONES</b>	<b>18</b>
<b>8</b>	<b>RECONOCIMIENTOS POR LA ELABORACIÓN DE ESTA PUBLICACIÓN</b>	<b>19</b>
<b>9</b>	<b>BIOGRAFÍA</b>	<b>20</b>

# 1 Introducción

La especificación EMV<sup>1</sup> define los requerimientos técnicos para las tarjetas bancarias con microcircuito integrado y para la infraestructura de terminales punto de venta (POS) que las acompañan.

Una gran mayoría de instituciones financieras alrededor del mundo emiten tarjetas bancarias EMV para empresas y consumidores. Más de 1,620 millones de tarjetas EMV han sido emitidas globalmente y más de 23.8 millones de terminales POS ya aceptan tarjetas EMV. (EMVCo, Q4 2012)

El propósito principal de incluir un chip en una tarjeta bancaria es almacenar de manera segura la información de los clientes, proteger los datos almacenados en el chip contra modificación no autorizada y reducir el número de transacciones fraudulentas que son resultado de falsificación, pérdida y robo de las tarjetas. En adición al chip de contacto, múltiples emisores emiten tarjetas con capacidad sin contacto para ofrecer mayor velocidad y conveniencia a sus clientes.

Utilizar tarjetas inteligentes sin contacto para el transporte público es el siguiente paso natural en la evolución de esta tecnología. Operadores de sistemas de transporte público en diversas partes del mundo han adoptado ya, o se encuentran en proceso de adoptar, sistemas de pago abierto.

Mientras que los sistemas tradicionales de pago electrónico en transporte público solo pueden ser utilizados en ambientes cerrados sin permitir interoperabilidad entre diferentes ciudades o modos de transporte, los pagos abiertos permiten el uso de tarjetas bancarias que cuentan con la capacidad de pagos sin contacto permitiendo la interoperabilidad entre diferentes sistemas.

Los pagos electrónicos en el transporte público proveen una mayor eficiencia operativa, una reducción importante en el costo del manejo de efectivo, y un aumento en la seguridad de los pasajeros.

## 1.1 Objetivo

El objetivo de este documento es educar a los lectores de la cadena de valor acerca de los componentes, requerimientos mínimos, y los beneficios del uso tarjetas bancarias para la creación de pagos abiertos en un sistema de transporte público de América Latina y el Caribe.

---

<sup>1</sup> Los fundadores originales de la organización que mantiene los estándares EMV fueron Europay, MasterCard, y Visa — es debido a esto que se utiliza el acrónimo “EMV.” Mayor información sobre las especificaciones puede ser encontrada en la página web <http://www.emvco.com>.

## **2 Antecedentes de los Sistemas de Cobro**

A través de los años la tecnología ha avanzado a niveles inigualables creando conexiones, y facilitándolas, en torno a las necesidades de las personas. Debido a su versatilidad, ha evolucionado siempre con la finalidad de mejorar y hacer de su uso algo más fácil y eficiente. Con esto en mente, la tecnología se ha adaptado a las necesidades de las personas en todo el mundo y su existencia nunca había sido tan importante para el día a día de las mismas.

El camino que las varias formas de pago han trazado con el pasar de los años y las mejoras en la tecnología son marcadas con las exigencias que han estado creciendo constantemente. A continuación se presentan los diferentes modelos utilizados a través de los años para acelerar el proceso de pago y garantizar la seguridad a sus usuarios.

### **2.1 Dispositivos sin prepago**

Esta forma de pago es la más básica que se encuentra en el mercado, cuya existencia y uso permanece aún con los grandes avances que hay para sustituir su uso. Esta forma de pago está formada por las monedas y los billetes. Ha sido y sigue siendo una forma de pago en América Latina desde su creación.

### **2.2 Dispositivos con prepago**

En busca de encontrar una forma más eficiente de realizar transacciones monetarias apareció el uso de las tarjetas Edmondson, por el inglés Thomas Edmondson, convirtiéndose en la primera forma de prepago. Caracterizadas por su creación en los años 1840 para su empleo en los ferrocarriles. Esta forma de pago constaba de unas tarjetas de cartón con la fecha del viaje impresa al momento de emisión, después del pago correspondiente, se hicieron muy populares alrededor de todo el mundo siendo utilizadas hasta 1990. En Latinoamérica su uso inicio con los ferrocarriles en Argentina conocidos como Ferrocarriles Argentinos, en el año 1947.

### **2.3 Tarjetas con banda magnética**

El uso de formas de pago que no utilicen dinero directamente (prepago) incitó a la aparición de las tarjetas con banda magnética. Estas fueron implementadas en el transporte público, por London Transit Authority, en el sistema de tren en Londres a principios de los años sesenta. Y también fueron implementadas a nivel bancario a principios de los años setenta, después de la creación de los estándares internacionales (ISO 7811).

### **2.4 Tarjetas Inteligentes (“Smart Cards”)**

Hay dos categorías principales para los tipos de tarjetas con circuito integrado, también conocidas como tarjetas inteligentes o “smart cards”, estas son: las tarjetas con memoria y las tarjetas con microprocesadores. La primera contiene componentes integrados que poseen una memoria similar a una banda magnética, mientras que la segunda cuenta con un microprocesador que tiene un sistema operativo completamente desarrollado donde el chip es capaz de realizar funciones muy avanzadas.

En la actualidad existen dos tipos primarios de interfaz para las tarjetas inteligentes, estos son: de contacto y sin contacto. Estos términos describen cómo se comunica el chip con su lector para la transferencia de información. Las tarjetas inteligentes pueden funcionar con un solo tipo de interfaz o combinar ambas, a continuación se presentan, brevemente, los diferentes tipos de tarjetas que existen en el mercado basado en las interfaces antes mencionadas.

#### **2.4.1 Tarjetas con contacto**

Constan de tarjetas cuyo chip es visible y necesitan de un puerto donde la información pueda ser leída para que se realice la conexión.

## **2.4.2 Tarjetas sin contacto**

Cuentan con un microchip integrado capaz de almacenar datos y programas. También son capaces de comunicarse por medio de Radio Frecuencia (RF) donde se transmite la información y en la cual no es necesario un puerto para la comunicación, a diferencia de las Tarjetas de Contacto

## **2.4.3 Tarjetas híbridas**

Estas tarjetas cuentan con dos chips. Esto es debido a que un chip permitirá la transferencia de datos a través de la interfaz de contacto mientras que el otro chip lo hará mediante la interfaz sin contacto. Es muy importante destacar que en estas tarjetas los chips no se conectan ni se comunican entre ellos.

## **2.4.4 Tarjetas de Doble Interfaz**

Este tipo de tarjeta soporta ambas interfaces, de contacto y sin contacto, lo que significa que cuenta con un chip visible que puede ser conectado a un puerto lector para enviar la información de la tarjeta o la misma puede ser realizada por medio de Radio Frecuencia.

## **2.5 Botón o Cospel Electrónico**

Dispositivo de contacto que se caracteriza por solo contener un código de identificación único por tarjeta y usuario, que realiza el débito con la máquina al leer el código, por lo que no almacena dinero. Este método es especialmente atractivo debido al poco riesgo que se tiene con la pérdida de la tarjeta, solo se tiene que notificar para cancelar el código y no hay pérdida de dinero.

## **2.6 NFC (Near Field Communication)**

Tecnología que se centra en el uso masivo de los móviles para facilitar muchas de las tareas del diario vivir. Esta nueva innovación, que está creciendo en los últimos años, es el pago por medio del teléfono inteligente que consiste de una tecnología de corto alcance y alta frecuencia. Esta tecnología es compatible con la que utilizan las Tarjetas de Doble Interfaz.

### 3 Repaso General EMV

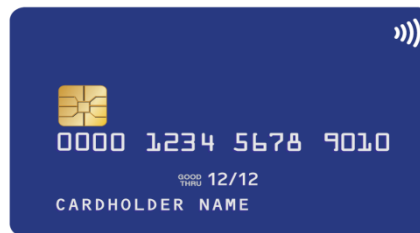
La tecnología de tarjetas inteligentes utiliza un microprocesador de circuito integrado seguro y lo incorpora dentro de una forma de pago (form factor). La forma de pago utilizada más comúnmente es la tarjeta; sin embargo llaveros, tarjetas microSD, adhesivos (stickers), teléfonos móviles con capacidad de NFC, y más recientemente los dispositivos usables (wearable devices), pueden acomodar la misma tecnología. Para su uso, el microcircuito generalmente se alimenta de la energía del dispositivo lector por lo que requiere del mismo para poder funcionar, en el caso de las tarjetas o dispositivos de contacto la energía es provista directamente por una conexión física con el lector y en el caso de tarjetas o dispositivos Contactless y/o Dual Interface la energía es provista a través de la onda de Radio Frecuencia enviada por el lector.

Para pagos con tarjetas bancarias en comercios la interface con el lector puede ser interfaces de contacto, sin contacto, o ambas. Las tarjetas de contacto se comunican con el lector mediante una placa de contactos. La placa debe entrar en contacto con el terminal, generalmente mediante un lector de inserción donde se introduce la tarjeta.

Para los sistemas de pagos abiertos en transporte público se requiere el uso de tarjetas de interface doble y para los terminales siempre se requieren lectores sin contacto (contactless).

Las tarjetas de interface doble (dual-interface cards) combinan ambas tecnologías (contacto y sin contacto) e incluyen una antena que se comunica con el lector mediante radio frecuencia (RF).

El Gráfico 1 muestra una tarjeta típica de interface doble: la placa de contacto es la placa dorada que se observa en la parte izquierda de la tarjeta y el símbolo en la parte superior derecha indica la capacidad de pago sin contacto. La antena generalmente no es visible en la mayoría de las tarjetas.



**Gráfico 1: Tarjeta inteligente EMV de Interface doble**

#### 3.1 EMV, Sin Contacto y NFC

Las tarjetas bancarias (crédito, débito o pre-pago) sin contacto (contactless) con marca de alguna de las banderas de pago deben estar basadas en el protocolo de comunicación sin contacto ISO/IEC 14443.

##### 3.1.1 EMV Sin Contacto (contactless)

Las especificaciones EMV proporcionan la base para los pagos sin contacto EMV, pero no especifican toda la funcionalidad de la aplicación de pago.

Las banderas de pago pueden implementar los pagos sin contacto EMV para funcionar tanto en ambientes en línea como fuera de línea (cada uno con requerimientos y desafíos específicos). Típicamente se requiere tarjetas con DDA (Dynamic Data Authentication) o CDA (Combined Data Authentication) para un primer nivel de seguridad entre la tarjeta y el terminal y posteriormente se utiliza el criptograma EMV para validar en línea la autenticidad de una tarjeta y de la transacción.

El soporte del criptograma EMV requiere ajustes en la red para transportar los datos adicionales que son requeridos para la autenticación en línea, igual que con las transacciones de contacto EMV.

El flujo de las transacciones sin contacto EMV para cada una de las banderas de pago varía de acuerdo al grado de funciones de administración de riesgo y al tipo de criptograma de autenticación que es implementado en la aplicación de pago sin contacto.

Los múltiples enfoques independientes hacia los pagos sin contacto EMV, ha requerido que los terminales POS sean aprobados por cada una de las banderas de pago. EMVCo ha reconocido la necesidad de estandarización y ha desarrollado una hoja de ruta común para terminales sin contacto. En la fase 1, EMVCo está creando un grupo combinado de especificaciones del terminal

para las cuatro especificaciones de las banderas de pago y administrará las pruebas y aprobaciones de los kernels para transacciones sin contacto de acuerdo a estas especificaciones.

### **3.1.2 EMV y los Pagos Móviles con NFC**

Un área donde se espera crecimiento en el futuro es el uso de la Comunicación de Corto Alcance o *Near Field Communication* (NFC) en teléfonos móviles habilitados para pagos sin contacto.

La tecnología NFC es un estándar de comunicación wireless que permite el intercambio de datos entre dispositivos que se encuentran a unos pocos centímetros de distancia uno del otro.<sup>2</sup> Los teléfonos móviles habilitados para NFC incorporan un microcircuito o chip (conocido como elemento seguro) que le permite a los teléfonos almacenar una aplicación de pago e información de la cuenta del cliente para utilizar dicha información como una tarjeta virtual de pago. Más recientemente se han definido estándares que permitirán también el uso de información de la cuenta almacenada en la nube (HCE – Host Card Emulation).

Las transacciones NFC entre un teléfono móvil y un terminal POS utilizan el estándar de protocolo de comunicación ISO/IEC 14443 que ya es utilizado actualmente para las tarjetas sin contacto de crédito y débito EMV, por lo que se puede aprovechar la infraestructura de aceptación de tarjetas para los teléfonos móviles con NFC.

Los teléfonos habilitados para NFC podrán contener una o más aplicaciones de pago y cuentas de diferentes emisores. La especificación NFC no define o especifica la aplicación de pago. Las aplicaciones de pago deberán basarse en las especificaciones de la marca o bandera de pago para la región del mundo donde dicha tarjeta virtual sea utilizada. En toda América Latina, se deberá utilizar una aplicación de pago sin contacto que soporte transacciones EMV. Esto les permite a los clientes utilizar sus teléfonos habilitados para NFC para pagos en la red de terminales sin contacto de crédito y débito EMV existente.

EMVCo ha estado muy activo en la definición de la arquitectura, especificaciones, requerimientos y procesos de aprobación para soportar los pagos sin contacto en móviles.

---

<sup>2</sup> Para mayor información sobre NFC, vea la página web del NFC Forum en <http://www.nfc-forum.org>. El NFC Forum define las especificaciones para la comunicación de etiquetas NFC y de los lectores, pero no define especificaciones para aplicaciones de pago.



## 4 Sistemas Proprietarios en Transporte

La tecnología para desarrollar las tarjetas inteligentes ha estado en las manos de cierta cantidad de compañías, cada una cumpliendo con sus propias necesidades y estándares que cree son los que busca el mercado. Las tecnologías líderes mundiales de tarjetas sin contacto en transporte son: Mifare, Calypso, FeliCa y CIPURSE

### 4.1 MIFARE

Tarjeta inteligente sin contacto y de memoria protegida, cuyo microprocesador integrado está dividido internamente en pequeños sectores y bloques de seguridad para el almacenaje de la información del usuario. Las tarjetas Mifare funcionan con una antena y tienen un espacio de almacenaje variable, dependiendo del número de sectores y bloques que contenga. Funciona cuando la tarjeta se acerca a un lector y una transferencia cifrada entre ambas comunicaciones ocurre, posteriormente, se envía un código de identificación de conexión, como confirmación, para dar acceso a los bloques de información contenidos en la tarjeta. Dentro de los tipos de tarjetas Mifare que se encuentran en el mercado tenemos:

MIFARE Classic, MIFARE Plus, MIFARE DESFire y SmartMX. (Mifare, 2014).

- ❖ MIFARE Classic: Lanzado en 1995, el CI MIFARE Classic 1K fue el primer producto que pudo ser colocado en una tarjeta inteligente sin contacto ISO y, con su bobina compacta, permitió una producción de muy alto volumen. En la actualidad, millones de CI MIFARE Classic 1K son usados en todo el mundo en un sin fin de aplicaciones diferentes, desde transporte público, cobro de peaje y parquímetros; hasta el acceso a estacionamientos y el pago en estaciones de gasolina. Para expandir la funcionalidad de los CI MIFARE Classic 1K existentes se desarrolló el CI MIFARE Classic 4K. Este ofrece un tamaño de memoria significativamente incrementado, lo que lo convierte en una solución apta para las tarjetas de múltiples aplicaciones.
- ❖ MIFARE Plus: ofrece una mayor seguridad y desempeño en cobro automático de tarifas (AFC) y control de acceso. El mismo incluyó el Estándar de Cifrado Avanzado (AES) y una ruta de migración para las implementaciones MIFARE Classic existentes.
- ❖ MIFARE DESFire EV1: Es una tarjeta inteligente que utiliza criptogramas con algoritmos: DES, 3DES, 3K3DES y AES. La misma es orientada a múltiple aplicación en esquemas de transporte, medios electrónicos gubernamentales o aplicaciones de verificación de identidad.

MIFARE ha sido aceptada en la mayoría de los países de América Latina y el Caribe con una recepción positivamente por los usuarios del transporte público. Algunos ha decidido actualizar su sistema de medios de pago en transporte de MIFARE Classic a MIFARE Plus.

### 4.2 CALYPSO

Calypso es una tarjeta inteligente sin contacto, cuyas especificaciones fueron creadas por la organización Calypso Network Association (CNA), que se utiliza para el transporte público masivo mundialmente, y que funciona con la tecnología del microprocesador integrado. Consiste de un conjunto de especificaciones técnicas que describen una transacción sin contacto, rápida y segura, entre una terminal y un dispositivo portátil. Entre los dispositivos portátiles en que se pueden utilizar esta tecnología están las Tarjetas Inteligentes (Smart Card), Tarjetas JAVA sin contacto, Near Field Communication (NFC), entre otras.

Inició en 1990 con un grupo de operadores de transporte europeos de Bélgica, Francia, Alemania, Italia y Portugal, que decidieron desarrollar una tecnología abierta para todos los dispositivos portátiles que se requieren para operar sistemas de peaje (ticketing) de transporte.

Después de diez años de investigación por parte de la compañía INNOVATRON lograron, con éxito, la creación de la tecnología inteligente de tarjetas sin contacto adaptada a muchos mercados, incluyendo el transporte público. Con más de 52 millones de tarjetas y 260 000 lectores en el comienzo de 2010.

El desarrollo de la aplicación de cobro de peaje (ticketing) de Calypso se basa en las normas internacionales: ISO / IEC 14443 (Tipo B), que define la señal de radio y protocolo para una transmisión de inducción a 13,56 MHz. Para las tarjetas de interfaz dual, ISO 7816 (1-3) describe las características físicas y las señales electrónicas y protocolos de transmisión de tarjetas de circuitos integrados. También es compatible con la tecnología NFC (Tipo 4 Tag).

### **4.3 FELICA**

Reconocidas por su alto nivel de seguridad, las tarjetas FeliCa IC han sido introducidas por los operadores de transporte público en los países de Asia desde 1994. Consisten de tarjetas inteligentes con circuito integrado sin contacto que debido a su alto nivel de seguridad es usada en una gran variedad de formas. Transporte público, pagos electrónicos, tarjetas de acceso son algunas de las formas en donde FeliCa es usada.

Las tarjetas FeliCa IC se utilizan como boletos para el transporte público en todo Japón. Desde la primavera de 2013, 10 tipos diferentes de tarjetas de tránsito IC se convirtieron interoperables en todo Japón lo que significa que, más sistemas de transporte pueden ahora aceptar más operadores de tarjetas que nunca. Las tarjetas IC también se pueden utilizar como dinero electrónico en un número creciente de tiendas. La creación de Sony, ha sido aceptada positivamente en el sistema de transporte de Hong Kong y en otros países de Asia como Taiwán, Bangladesh y Tailandia.

La tarjeta FeliCa es la primera tarjeta inteligente sin contacto del mundo certificada por la norma ISO / IEC 15408 EAL4, que garantiza la seguridad y la fiabilidad del sistema FeliCa. FeliCa comunica con una frecuencia estándar de 13,56 MHz a una velocidad de 212 kbps o 424 kbps y soporta el acceso simultáneo de hasta 8 bloques (cada bloque es de 16 bytes).

Algunos de sus servicios son encontrados en:

- La tarjeta Suica del East Japan Railway (boleto y dinero electrónico)
- BitWallet, Inc's. Edy, dinero electrónico en Japón
- La tarjeta Octopus en Hong Kong (boleto y dinero electrónico).

### **4.4 CIPURSE**

La Alianza Open Standard for Public Transport™ (Estándares Abiertos para el Transporte Público, OSPT™), ayuda a los operadores de transporte, posibilitando la próxima generación de soluciones de recaudación flexibles, seguras y de bajo costo, para una comunidad global. Hace uso de las tarjetas inteligentes y otros sistemas de seguridad para su empleo. Los sistemas que usan el estándar abierto de seguridad, CIPURSE, están dirigidos al servicio del transporte público, recaudación de las tarifas de transporte, y las transacciones relacionadas con los micropagos. Construidas según los estándares aprobados, incluyendo ISO 7816, AES-128, ISO/IEC 14443-4 para asegurar múltiples tipos de pagos,

CIPURSE permite a los usuarios utilizar un solo dispositivo para transporte a lo largo de varios sistemas y lugares.

Los mecanismos avanzados de seguridad de CIPURSE incluyen un protocolo criptográfico único que alienta implementaciones rápidas y eficientes. El protocolo proporciona una protección inherente y robusta ante el análisis diferencial de potencia (DPA : Differential Power Analysis) y el análisis diferencial de fallos (DFA : Differential Fault Analysis).

## **5 Consideraciones para Pagos Abiertos sin Contacto en Transporte Público**

Para facilitar la incorporación de pagos abiertos, es decir pagos con tarjetas bancarias en el sistema de transporte público, la recomendación de Smart Card Alliance Latino América es que el sistema de recaudo implementado proporcione el soporte de los esquemas siguientes:

1. Esquema de “autorización diferida con autenticación dinámica fuera de línea”.

Bajo este esquema, los validadores instalados en los buses verifican la autenticidad de la tarjeta (fuera de línea) utilizando un esquema de autenticación dinámica (DDA) y en un momento posterior, los sistemas centrales realizan en línea la transacción financiera correspondiente. Bajo esta modalidad NO es necesario que los emisores realicen la implementación Full EMV. Este esquema permite garantizar una amplia interoperabilidad global, así como los tiempos mínimos requeridos para obtener la fluidez del pago que es requerido en este tipo de transacciones de la misma manera que se está usando en múltiples sistemas abiertos de transporte público alrededor del mundo, entre otros, el de Londres.

2. Esquema de “autorizaciones fuera de línea cuando sea aplicable en la tarjeta”

Bajo este esquema los validadores instalados en los buses verifican la autenticidad de la tarjeta (fuera de línea) utilizando la autenticación DDA o autenticación CDA y se realiza la aprobación de la transacción en base a los parámetros de riesgos definidos en la tarjeta, y en un momento posterior se envía el cobro al sistema central. Esta modalidad contiene en los contadores fuera de línea de la tarjeta los saldos disponibles y la transacción se autoriza por un monto fijo. Para este esquema es requerido que el procesador de la tarjeta sea un procesador Full con generación de script. Este esquema permite garantizar la disponibilidad de fondos de cada usuario de la misma manera que se está usando en múltiples sistemas abiertos de transporte público alrededor del mundo.

En el diseño y desarrollo de este sistema de recaudo, las características técnicas y la personalización de la tarjeta juegan un papel fundamental para el funcionamiento correcto en todo el ecosistema, es decir, aceptación en los buses, aceptación en los comercios, así como la tarjeta como tal. Es crítico que los bancos se apoyen en las Marcas para garantizar que se sigan y cumplan todos los requerimientos, recomendaciones y mejores prácticas.

Cada Marca tiene ciertos requerimientos técnicos mínimos que en muchos casos son diferentes y que se deben tener en cuenta por los bancos emisores para obtener mejores resultados en el proceso de emisión y desarrollo de tarjetas para el proyecto de transporte público.

A continuación los requerimientos técnicos mínimos que cada marca considera importante tener en consideración para la emisión de tarjetas que sean usadas para pagos con chip de contacto en comercios, pagos sin contacto en comercios y pagos sin contacto en el sistema abierto de transporte público.

### **5.1 Requerimientos de las Tarjetas**

Una de las primeras decisiones que un emisor debe realizar para una implementación de EMV es decidir cuál será la interfaz de tarjeta que utilizará: contacto o interface doble.

Para ofrecer pagos abiertos en transporte público resulta indispensable la utilización de tarjetas bancarias de interface doble. Dichas tarjetas soportan tanto la interface de contacto como la interface sin contacto (contactless) permitiendo la aceptación no solo en comercios sino también en el sistema de transporte público.

### 5.1.1 Requerimientos mínimos para Tarjetas de la marca Visa

De las dos opciones de autorización presentadas en la sección 5 de este documento, Visa requiere que se implemente el esquema de “autorización diferida con autenticación dinámica fuera de línea”. Visa no soporta el esquema de autorización fuera de línea.

Las tarjetas Visa deben cumplir con los siguientes requerimientos:

- Tipo de tarjeta: “dual interface” (contacto y sin contacto)
- Número de Referencia de Aprobación Visa válido
- Tarjeta GlobalPlatform (JavaCard)
- EMVCo ICCN
- Estándar EMV 4.3
- Estándar Common Criteria CC EAL4+
- Protocolo de contacto T0 o T1
- Protocolo sin contacto ISO 14443 tipo A o tipo B
- Especificaciones VIS 1.5 / VCPS 2.1
- Soporte de DDA / fDDA
- Applet VSDC v2.8.1am2s o más reciente
- 16Kb de memoria disponible, EEPROM o Flash
- Antenna Inlay / Module Inductive Coupling Technology (recomendado)

Aunque existe una amplia gama de tarjetas disponibles por múltiples proveedores tecnológicos, Visa puede ofrecer directamente apoyo especializado para algunas plataformas de chip, específicamente:

1. Entrenamientos técnicos y comerciales
2. Mejores prácticas, recomendaciones técnicas y de negocio
3. Generación de perfiles de personalización (para cada uno de los diferentes Productos Visa)
4. Claves de prueba
5. Validación de personalización de las tarjetas de acuerdo al perfil suministrado
6. Certificación de host emisor con tarjetas validadas en el laboratorio Visa

El apoyo especializado mencionado aplica para ciertas plataformas. La lista específica de plataformas se debe obtener por medio de su representante de Visa. En caso que un emisor opte por tarjetas de otras plataformas tecnológicas, podrá solicitar el apoyo correspondiente directamente de sus respectivos proveedores de tarjetas.

Siempre es requerido que el terminal y el adquirente procesen transacciones Full EMV. Para emisores, no es necesario ser Full EMV. Visa puede ofrecer Servicios de Autenticación de Chip y conversión de iCVV para simplificar y agilizar el proceso de implementación para emisores.

### 5.1.2 Requerimientos mínimos para Tarjetas de la marca MasterCard

La recomendación inicial de MasterCard para un proyecto de pagos abiertos se basa en el uso de una solución con autorización de pagos “offline” (fuera de línea). Basado en el uso de tal solución para el sistema de transporte, las tarjetas deberían cumplir con las siguientes especificaciones:

- Tipo de tarjeta: “dual interface” (contacto y sin contacto)
- Compatibilidad con las normas: EMV y ISO 14443
- Aplicación de pago: M/Chip 4 o M/Chip Advance
- Sistema Operativo: Multos o Java
- Criptografía: capacidad CDA (Combined Data Authentication)
- Memoria EEPROM: mínimo de 16K

Tanto los emisores como los adquirentes deben ser capaces de operar en modo “Full Grade” (i.e. host del emisor actualizado para recibir y enviar datos de chip, especialmente para poder “actualizar” los contadores “offline” de la tarjeta)

MasterCard cuenta con un equipo de expertos dedicados a los proyectos de Chip y Contactless en la región. El soporte, proporcionado por dicho equipo, incluye entre otros:

1. Entrenamientos técnicos y comerciales
2. Mejores prácticas, recomendaciones técnicas y de negocio
3. Preparación de perfiles para tarjetas
4. Procesos de certificación completo (tarjetas, terminales, criptografía, host, etc), incluyendo pruebas de punta a punta (end to end).

### 5.1.3 Requerimientos mínimos para Tarjetas de marca American Express

Las tarjetas American Express deben:

- Cumplir con los requerimientos descritos en el manual “American Express Transit Policy for Issuers & Acquirers” en la sección correspondiente a “*Expresspay Transactions at Transit Access Terminals (TATs)*”
- Apoyarse en las definiciones del “Issuer Chip Card Implementation Guide”
- Cumplir con los requerimientos de protocolo de comunicación descritos en el manual “Expresspay 2.0 Communication Layer”
- Cumplir con los requerimientos para las aplicaciones de pago que residen en las tarjetas que se describen en el manual “Expresspay 2.0 Card Specification” para tarjetas de interface sin contacto
- Cumplir con los requerimientos adicionales para las aplicaciones de pago que residen en las tarjetas que se describen en el documento “Expresspay 2.0 Card Specification Dual Interface Addendum”, para tarjetas de interface dual

#### **5.1.4 Requerimientos mínimos para Tarjetas de otras Marcas**

Smart Card Alliance Latino América realizará el mejor esfuerzo para consolidar e incorporar en este documento en el futuro próximo los requisitos de otras marcas de pago.

## **6 Beneficios de los Estándares Abiertos**

Debido a las pocas compañías que tienen la tecnología para implementar estas tarjetas, a nivel de cada país, el costo del mismo es muy alto y muchos de los países que tienen la necesidad no tienen el presupuesto para implementar las tarjetas inteligentes. Hay muchas razones por las cuales crear estándares abiertos es la mejor solución para poder implementar esta tecnología en Latinoamérica, permitiendo con esto un entendimiento común y requerimientos claros que ayuden en la reducción de riesgos y costos en la implementación.

La bancarización que ha retenido a Latinoamérica de crecer económicamente, podría verse influenciada por implementaciones de sistemas de pagos abiertos en el sistema de transporte público. La reducción del tiempo al realizar la transacción monetaria en el transporte público, la seguridad tanto para el gobierno como para los usuarios de tener un control más claro de las transacciones realizadas y por último el control de las autoridades sobre la estandarización de la implementación, son beneficios adicionales del uso de Estándares Abiertos.

### **6.1 Seguridad**

Con la implementación de sistemas abiertos con tarjetas inteligentes, se reduce la utilización de dinero en efectivo, lo que a su vez minimiza los robos tanto a los conductores de autobuses como a los usuarios del sistema de transporte. Adicionalmente, los usuarios cuentan con la seguridad que ofrecen las tarjetas inteligentes, de nivel bancario, al no poder ser clonadas como se hacía anteriormente con las tarjetas con banda magnética u otras tecnologías contactless de menor seguridad.

### **6.2 Bancarización**

Las innovaciones en dinero digital y las herramientas disponibles hoy en el mundo móvil, ofrecen facilidades a la hora de pagar cuentas, comprar y vender productos, enviar y recibir dinero y hacer transferencias bancarias. En Latinoamérica el nivel de bancarización, o la cantidad de habitantes que tienen una cuenta bancaria ha mostrado un constante crecimiento. Aunque no se puede comparar a los niveles de Estados Unidos, Europa o Asia, este indicador para Latinoamérica ha mostrado mejoras en los últimos años. La bancarización agregada puede estar rondando niveles cercanos al 40% de la población en el país más avanzado de América Latina. Esto es un indicador que aún luce como lejano si se compara con los países industrializados, donde el acceso a los servicios financieros puede alcanzar niveles del 97%.

América Latina requiere de mayor acceso a los servicios financieros de parte de más grupos de la población. Este es un requisito para alcanzar economías modernas, competitivas, con menores costos de transacción y mayor grado de formalidad. Esta última, es una condición clave para la obtención de financiamiento fresco y estable, mejores posibilidades de ahorro, mejoramiento de los sistemas tributarios y la calidad de vida de los ciudadanos del país.

### **6.3 Reducción del Tiempo de Transacción**

Al utilizar las tarjetas inteligentes no solo se eliminan la incomodidad de cargar con monedas y billetes para pagar por el pasaje, sino que también desaparece el tiempo que cada usuario tarda en pagar por el servicio. Adicionalmente mejora sustancialmente el control que pueden tener los operadores de transporte sobre las transacciones efectivamente realizadas en sus unidades.

Gracias a la velocidad con la que las tarjetas funcionan y al sistema sin contacto, los usuarios no necesitan sacar la tarjeta de sus billeteras o carteras, basta con acercarlos al lector para que la transacción se realice.

### **6.4 Disponibilidad de la Información de las Transacciones**

De utilizarse los estándares abiertos de esta tecnología los costos de poder implementarla bajarían de manera notoria. Se podría aumentar la seguridad ya que el gobierno podría llevar un mejor control de las



transacciones. Se simplifica la migración a nuevas soluciones eficientes mientras se preserva la inversión en soluciones de recaudación existentes. Más opciones rentables para los clientes: Ofrece soluciones que aumentan el retorno de inversión, bajan los costes de operaciones, y reducen el riesgo.

## **6.5 Interoperabilidad**

Cualquier tarjeta bancaria con las características sugeridas podrá ser utilizada para pagar el transporte, independiente de la ciudad o el operador de recaudo. De igual manera los turistas y/o empresarios que visitan los países con estas características podrán pagar sus pasajes en todo los territorios nacionales con sus propias tarjetas bancarias de sus países de origen, colocando el sistema de transporte al nivel de interoperabilidad de los sistemas financieros y los sistemas de transporte más exitosos del mundo.

## **6.6 Eficiencia**

Una solución de pagos abiertos es más eficiente porque reduce los costos asociados con la gestión de tarjetas, elimina la necesidad de un intermediario para el proceso de recaudación de fondos, lo que permite que el sistema de recaudo sea más sencillo, robusto, y seguro para todos los involucrados en el sistema de transporte, adicionalmente, se reducen las “filas” de pasajeros en centros de recargas.

## 7 Conclusiones

De la amplia gama de opciones en la implementación de tarjetas con chip EMV cada marca de medios de pago cuenta con requerimientos específicos, especialmente cuando se refieren a la implementación de pagos abiertos en un sistema de transporte público.

Este documento lista las características que cada una de las compañías de medios de pago considera clave para la implementación de este tipo de proyectos, lo que proporciona un apoyo muy importante para el desarrollo del proyecto así como el éxito del mismo.

Es importante que el sistema de recaudo sea diseñado con el soporte a los esquemas mencionados para lograr la aceptación de las tarjetas bancarias y así poder aprovechar todos los beneficios de los pagos abiertos en el transporte público.

*Para mayor información sobre los esquemas y oportunidades de Pagos Abiertos en Sistemas de Transporte en América Latina y el Caribe contacte a:*

**Smart Card Alliance Latino América - SCALA**

Local # 7 – Edificio 237

Tecno Parque – Ciudad Del Saber

Ciudad de Panamá, República de Panamá

[www.sca-la.org](http://www.sca-la.org)

Contacto Directo:

+507 317 - 1255

[scala@sca-la.org](mailto:scala@sca-la.org)

## 8 Reconocimientos por la elaboración de esta publicación

Este documento fue desarrollado con el esfuerzo conjunto entre la universidad del Estado de la Florida (Florida State University - FSU) en Panamá y Smart Card Alliance Latino América - SCALA y tiene relación con la creación del Centro de Excelencia de la industria de Tarjetas con Circuito Integrado; en forma tal, que mismo sirva como un recurso imparcial educacional para educar a todos los interesados de toda la cadena de valor en los sistemas de transporte y medios de pagos, en relación a los aspectos importantes para la implementación exitosa de tarjetas bancarias – EMV en transporte público en América Latina y el Caribe.

Las organizaciones que contribuyeron al desarrollo, modificación, y adaptación de este documento para América Latina y el Caribe son: **Advance Card Systems, American Express, Charge Anywhere, Gemalto, Giesecke & Devrient, HID Global, MasterCard Worldwide, NXP Semiconductors, Oberthur Technologies, Safran Morpho, Smartrac Technology, Ultra Electronics – Magicard, Visa Inc., and Watchdata Technologies.**

En una forma especial se reconoce la participación y el apoyo, a los siguientes miembros de SCALA y personas:

- **Carolina Garrón**, Florida State University
- **Ansberto Cedeño**, Florida State University
- **Belkis Barral**, Visa Inc.
- **Diego Noreña**, Visa Inc.
- **Dimas Gomez**, Gemalto
- **Fernando Mendez**, Visa Inc.
- **Pablo Juan**, Giesecke & Devrient
- **Kim Hangoc**, MasterCard Worldwide
- **Solmoraine Guzman**, Smart Card Alliance
- **Edgar Betts**, Smart Card Alliance

### **Acerca de SCALA – Smart Card Alliance Latino América**

SCALA – Smart Card Alliance Latino América es un capítulo del Smart Card Alliance, una asociación sin fines de lucro, imparcial, que impacta múltiples industrias, la cual trabaja para estimular la comprensión, interoperabilidad, convergencia, evolución, y la adopción innovadora de aplicaciones de la tecnología de tarjeta de circuito integrado (ICC) en los Estados Unidos, América Latina, y el Caribe. SCALA logra sus objetivos a través de proyectos específicos como: *Programas Educativos, Centro de Excelencia, Investigaciones de Mercado, Promociones de Casos de Éxito, Hojas de Ruta, Recursos en Línea, Relaciones en industrias afectadas y foros abiertos*, manteniendo a sus afiliados conectados con líderes de la industria y el pensamiento innovador.

Smart Card Alliance funge como la voz única de la industria para los temas relacionados con las tarjetas con circuito integrado y componentes relacionados, liderando las conversaciones de la industria sobre el impacto y el valor agregado de esta tecnología en las Américas.

Para obtener más información sobre SCALA visite: [www.sca-la.org](http://www.sca-la.org)

O Smart Card Alliance visite: [www.smartcardalliance.org](http://www.smartcardalliance.org)

## 9 Biografía

### Websites

1. <http://www.cepal.org/publicaciones/xml/5/10635/lcl1752-p-e.pdf>
2. [http://fido.palermo.edu/servicios\\_dyc/proyectograduacion/detalle\\_proyecto.php?id\\_proyecto=380](http://fido.palermo.edu/servicios_dyc/proyectograduacion/detalle_proyecto.php?id_proyecto=380)
3. <http://www.calypsonet-asso.org/handbook.php?chapter=1&page=003>
4. <http://www.sony.net/Products/felica/>
5. [http://www.osptalliance.org/the\\_standard](http://www.osptalliance.org/the_standard)
6. [http://www.osptalliance.org/the\\_standard/why\\_open\\_standards](http://www.osptalliance.org/the_standard/why_open_standards)

### Libros

Smart Card Alliance. Manual CSCIP. Edición 2012