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

SELECCIÓN DE ESTÁNDARES TECNOLÓGICOS PARA MEDIOS DE PAGO DEL SISTEMA INTEGRADO DE TRANSPORTE PÚBLICO DEL DISTRITO METROPOLITANO DE QUITO

GSD+
EXPERTOS EN TRANSPORTE

10/10/2018

Contenido

1. Introducción

Garantizar la interoperabilidad a nivel tecnológico en un sistema de recaudo requiere la definición detallada de varios elementos. Uno de estos elementos es el estándar tecnológico del medio de pago. El estándar generalmente define la estructura base del medio de pago, sobre la cual es posible crear una o varias aplicaciones de pago electrónico. La mayoría de estos estándares se crean tomando como base normas técnicas internacionales, entre las que se encuentran la ISO/IEC 14443 y la ISO/IEC 7816.

Es necesario escoger un estándar tecnológico para garantizar la interoperabilidad entre sistemas de recaudo provistos por diferentes integradores. Solo de esta manera se puede asegurar que los integradores no desarrollarán elementos propietarios que luego harán imposible la integración con sistemas y componentes provistos por terceros. Ejemplos de esta buena práctica se encuentran en nuestra región, en ciudades como Sao Paulo, Buenos Aires y Ciudad de México, todas las cuales han escogido un estándar tecnológico que garantiza la interoperabilidad entre sistemas provistos por diferentes integradores. Otros ejemplos en el mundo incluyen Oslo, Reino Unido, Francia, Alemania, por nombrar solo algunos.

La selección de un estándar tecnológico para el medio de pago no implica cerrarse a un proveedor específico. Actualmente existen varios estándares tecnológicos que permiten y fomentan la existencia de múltiples proveedores de chips y tarjetas. Estos proveedores certifican un producto específico el cual implementa el estándar. Esto implica que un integrador tecnológico o un operador de recaudo podrá escoger entre múltiples proveedores que se acogen a un estándar tecnológico.

A continuación, presentamos un análisis multicriterio y nuestra recomendación para la selección de un estándar tecnológico para los medios de pago recargables y otro para los medios de pago no recargables del sistema integrado de transporte público del Distrito Metropolitano de Quito.

2. Selección del estándar tecnológico para el medio de pago recargable

2.1. Estándares disponibles en el mercado

2.1.1. MIFARE DESFire EV2

MIFARE DESFire EV2 corresponde al circuito integrado más reciente, desarrollado por NXP Semiconductors para medios de pago sin contacto, el cual tiene como propósito establecer y garantizar altos estándares de confiabilidad, interoperabilidad y escalabilidad para soluciones de transporte y múltiples servicios de ciudad. Su lanzamiento se hizo en el año

2016, durante la conferencia IT-TRANS, en Karlsruhe, Alemania. Su principal ventaja frente a otras tecnologías anteriormente desarrolladas por NXP, consiste en la flexibilidad que ofrece su estructura de archivos multi-aplicación, organizada de manera jerárquica en aplicaciones y archivos, para la implementación de diferentes servicios en el mismo medio de pago. La velocidad de comunicación para un medio de pago de la familia DESFire es de 848 kbps y tiene una capacidad de memoria de datos EEPROM variable que puede ser de 2/4/8 KB EEPROM.

MIFARE DESFire EV2, a diferencia de MIFARE DESFire EV1, ofrece algunas opciones adicionales, como MIsmartApp, que permite al operador llevar a cabo la venta de espacio en el medio de pago a terceros para la instalación de sus aplicaciones, sin necesidad de compartir su master key. De igual forma, para DESFire EV2 es posible definir múltiples *keysets* por aplicación y se permite la creación de archivos compartidos entre aplicaciones [1].

2.1.2. MIFARE Plus

El producto MIFARE Plus de NXP Semiconductors, ha sido la primera de las alternativas MIFARE en implementar criptografía AES para la comunicación con los equipos de lectura. La primera versión de este producto fue anunciada en el año 2008 y, desde entonces, ha estado en constante evolución. El estándar tecnológico MIFARE Plus contempla cuatro modelos diferentes: MIFARE Plus S, MIFARE Plus SE, MIFARE Plus X y MIFARE Plus EV1.

Este estándar tecnológico fue desarrollado como una evolución de la familia MIFARE Classic, incorporando una serie de mejoras adicionales necesarias, en términos de seguridad. Su estructura de archivos, basada en una subdivisión por bloques y sectores, es compatible con la tecnología MIFARE Classic. Esto ha facilitado el proceso de migración de Classic a Plus para diferentes redes interoperables de transporte. Las características de cifrado y algunas opciones de seguridad adicionales, como el Proximity Check y el Transaction MAC, dependerán del nivel de seguridad en el cual se encuentre configurado el medio de pago i.e. SL0, SL1, SL3 o SL1SL3. [2]

2.1.3. CIPURSE

El estándar CIPURSE fue formalmente definido por la organización OSPT (Open Standard for Public Transportation) Alliance en el año 2010. La OSPT Alliance es una organización sin ánimo de lucro, abierta a proveedores tecnológicos, operadores de transporte, agencias de gobierno, integradores de sistemas, fabricantes de dispositivos móviles, consultores y otros, quienes interactúan entre sí y trabajan conjuntamente por el desarrollo del estándar CIPURSE. La última versión del estándar, introducida en el año 2012, fue diseñada como un estándar multi-aplicación de arquitectura modular, basado en una serie de perfiles de aplicación específicos. Estos perfiles, clasificados de acuerdo a los casos de uso del medio de pago, son: CIPURSE T, CIPURSE S y CIPURSE L. Por su parte, CIPURSE hace uso del algoritmo AES 128, como método de cifrado. En la actualidad, el estándar CIPURSE es implementado sobre chips fabricados por Infineon Technologies AG.

2.1.4. Calypso

Calypso es un estándar internacional para medios de pago electrónico sin contacto, que fue originalmente propuesto por operadores de transporte de once países diferentes, entre ellos, Francia, Bélgica, Alemania, Italia y Canadá. Calypso surgió en el año 1993, como producto de una sociedad entre el operador de transporte de París RATP y la compañía francesa *Innovatron*. El primer caso de implementación de la tecnología Calypso ocurrió en el año 1996 y, desde entonces, su aplicación se ha hecho extensiva en varios países.

La versión 3.2, que corresponde a la más reciente del estándar Calypso, presenta una estructura de datos multi-aplicación, que contempla la integración de múltiples servicios de transporte y de ciudad. Esta tecnología de medios de pago presenta altos estándares de seguridad y cuenta con un óptimo nivel de soporte, basado en la conformación de la CNA (Calypso Networks Association), una asociación sin ánimo de lucro, que reúne diferentes operadores de transporte, consultores y fabricantes con experiencia en la implementación de la tecnología Calypso. La CNA se encarga de promover el estándar Calypso y de establecer una red de soporte conjunta para la aplicación del mismo.

2.1.5. EMV

EMV (Europay Mastercard Visa), inicialmente desarrollado durante los años 1993 y 1994, es un estándar de medios de pago basado en la tecnología chip&PIN i.e. el uso de un elemento seguro (*Certified Silicon chip*) y un código PIN usado por el titular de la tarjeta para garantizar la seguridad de sus transacciones de pago. La propagación de estándar EMV se encuentra cimentado en tres ejes: primero, como una solución segura frente al riesgo de fraude en transacciones; segundo, el titular de la tarjeta puede hacer uso de la misma en todo el mundo, gracias a la arquitectura global EMV; tercero, la industria bancaria ha acordado incentivos para migrar toda la infraestructura de pagos bancarios a EMV.

En términos de seguridad, el método de autenticación EMV DDA (Dynamic Data Authentication) ofrece altos estándares de seguridad y cuenta con certificación *Common Criteria* EAL4+ y EAL5+. El estándar EMV soporta transacciones con medios de pago con contacto y sin contacto, permitiendo nuevas aplicaciones, como las “combi-cards”, que ofrecen múltiples servicios, e.g. Pagos bancarios y Transporte. El éxito de su implementación como solución para transporte público se encuentra, necesariamente, relacionado con el índice de bancarización de la región en cuestión. Por esta razón, es usual encontrar aplicaciones el estándar EMV como solución paralela a otros métodos de pago para los sistemas de transporte público. [3]

2.2. Comparación de estándares

2.2.1. Criterios y pesos asignados

Se han tenido en cuenta una serie de criterios fundamentales para la comparación y selección de un estándar tecnológico. De igual forma, con base en experiencias previas de

diseño e implementación de tecnologías para sistemas interoperables de transporte, se han definido pesos específicos para cada criterio, con el objetivo de llegar a una valoración global para cada tecnología. Cada uno de estos criterios ha sido valorado en una escala de 1 a 5, siendo 5 el puntaje más alto.

- **Costos (20%):** Criterio que define el costo unitario por tarjeta para cada una de las tecnologías, así como las diferencias sustanciales que puede haber entre los costos de toda la plataforma de implementación para un sistema con la tecnología del medio de pago respectiva.
- **Seguridad (15%):** Para el criterio de seguridad se han tenido en cuenta tres ítems de evaluación fundamentales. Primero se consideran los tipos de algoritmos de cifrado soportados por cada una de las tecnologías y la longitud de las llaves usadas. Por otro lado, el nivel de seguridad, de acuerdo con la certificación *Common Criteria*. Finalmente, se considera la capacidad de generar MAC (*Message Authentication Code)* para la protección de la información transmitida.
- **Posibilidad de realizar pagos con dispositivos móviles (10%):** Criterio relacionado con las alternativas hardware y software ofrecidas por cada uno de los estándares tecnológicos, para realizar pagos con dispositivos móviles.
- **Posibilidad de integración con pagos bancarios (10%):** Este criterio se relaciona con la posibilidad de integración de aplicaciones para pagos bancarios para cada una de las tecnologías valoradas.
- **Existencia de múltiples proveedores (10%):** Criterio que se encuentra asociado a la multiplicidad de proveedores a nivel de chip y de tarjeta para cada tecnología. Se define si para cada uno de estos niveles existen múltiples proveedores o un único proveedor.
- **Soporte (10%):** Criterio relacionado con la red de soporte ofrecida por cada uno de los estándares tecnológicos, a nivel de consultas, experiencias de implementación, capacitación y entrenamiento en la tecnología de medios de pago respectiva.
- **Posibilidad de crear múltiples aplicaciones en el medio de pago (10%):** Se refiere a la capacidad de soportar un estructura de datos multi-aplicación, con el objetivo de integrar servicios de transporte y de ciudad en el medio de pago.
- **Casos de éxito en transporte público (15%):** Criterio que describe los casos de éxito en sistemas de recaudo para transporte público en la implementación para cada una de las tecnologías.

2.2.2. Valoración de los estándares a la luz de cada criterio

2.2.2.1. Costos

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta MIFARE DESFire EV2 es de US$ 0.95.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta MIFARE Plus es de US$ 0.71.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta Calypso es de US$ 0.94.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta CIPURSE es de US$ 0.66.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta EMV es de US$ 1.60.

El costo de la plataforma tecnológica para todos los estándares es similar, excepto para el caso de EMV, cuyos equipos de lectura y componentes del sistema central tienen un mayor costo, debido al costo de las certificaciones requeridas para estos equipos y el requerimiento de cumplimiento con estándares PCI de seguridad.

Asignamos un puntaje de 5 unidades a CIPURSE, dado que es la alternativa con el precio más bajo. A EMV le asignamos un puntaje de 1 unidad, ya que es el de mayor costo. Para MIFARE DESFire EV2, MIFARE Plus y Calypso asignamos el puntaje mediante una función lineal.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
3.4	4.6	**5**	3.4	1

2.2.2.2. Seguridad

El puntaje en seguridad se asigna con base en tres subcriterios: estándares de cifrado soportados, nivel de seguridad según Common Criteria y mecanismos para garantizar la

integridad de los datos. Otorgamos a cada uno de los estándares tecnológicos un puntaje de 1 a 5 en cada subcriterio y luego ponderamos los puntajes asignando a cada uno de los primeros dos subcriterios un peso de 40% y un peso de 20% al último subcriterio.

Algoritmos de cifrado:

- MIFARE DESFire EV2 soporta los algoritmos de cifrado simétricos DES, 2KDES, 3KDES y AES de 128 bits. No soporta algoritmos asimétricos.

- MIFARE Plus soporta los algoritmos de cifrado simétrico Crypto 1 y AES de 128 bits. MIFARE Plus no soporta algoritmos de cifrado asimétrico.

- Calypso soporta los algoritmos de cifrado simétrico DES, DESX, TDES y AES de 128 bits. No soporta algoritmos de cifrado asimétrico.

- CIPURSE soporta el algoritmo de cifrado simétrico AES-128. CIPURSE no soporta algoritmos de cifrado asimétrico.

- EMV, soporta algoritmos de cifrado simétrico como AES de 128, 192 y 256 bits y algoritmos asimétricos, como RSA y SHA.

En este subcriterio asignamos 5 puntos a EMV por soportar algoritmos de cifrado asimétricos, con RSA y SHA, y simétrico, con AES de 192 y 256 bits. Esto es, permite claves de seguridad más extensas que las de los demás estándares. Se asignan 4 puntos a los demás estándares por soportar AES de 128 bits, un algoritmo moderno y robusto. Es importante anotar que todos los algoritmos soportados, a excepción del Crypto 1 de MIFARE Plus, son algoritmos robustos y que garantizan un adecuado grado de seguridad para la aplicación de recaudo en transporte.

Nivel de seguridad de Common Criteria:

Respecto al nivel de seguridad, según la certificación *Common Criteria*, se encuentran en el mercado disponibles implementaciones de los estándares MIFARE DESFire EV2, MIFARE Plus (EV1), CIPURSE, Calypso y EMV, en chips que alcanzan el nivel CC EAL5+ que es el puntaje más alto otorgado por Common Criteria. Por tanto, para este subcriterio, se da un puntaje de 5 unidades a todos los estándares evaluados.

Integridad de datos

Todos los estándares tecnológicos evaluados permiten el cálculo de MAC (Message Authentication Code), para la protección de la información intercambiada entre los medios de pago y los equipos de campo. Por esta razón, se asigna un puntaje de 5 unidades a todos

los estándares evaluados. El puntaje ponderado para el criterio de seguridad queda entonces como se muestra en la siguiente tabla:

Subcriterio	Peso	MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
Algoritmos de cifrado	**40%**	4	4	4	4	5
Certificado de Common Criteria	**40%**	5	5	5	5	5
Integridad de datos	**20%**	5	5	5	5	5
Puntaje ponderado	**100%**	4.6	4.6	4.6	4.6	**5**

2.2.2.3. Posibilidad de realizar pagos con dispositivos móviles

- Con MIFARE DESFire es posible implementar pagos con dispositivos móviles a través de herramientas de NXP como MIFARE2GO y MIFARE4MOBILE.

- Con MIFARE Plus es posible implementar pagos con dispositivos móviles a través de la herramienta de NXP MIFARE2GO.

- Con Calypso es posible implementar pagos con dispositivos móviles empleando el applet Java de Calypso embebido en un elemento seguro y siguiendo las guías de la CNA para la implementación de Host Card Emulation.

- Con CIPURSE es posible mediante la implementación de HCE, usando tokenización.

- Las tarjetas EMV cuentan con la posibilidad de ser emuladas en teléfonos inteligentes mediante el uso de NFC.

Se otorga un puntaje de 5 a todas las tecnologías, teniendo en cuenta que todas ellas permiten pagos con dispositivos móviles. La siguiente tabla indica el puntaje otorgado a cada alternativa para este criterio.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
5	5	5	5	5

2.2.2.4. Posibilidad de integración con pagos bancarios

- Para MIFARE DESFire es posible crear una tarjeta dual interface que contenga tanto la aplicación MIFARE DESFire como la aplicación para pagos bancarios EMV. Sin embargo, en este momento se debe utilizar un chip SmartMX, de NXP, toda vez que no está disponible la emulación de MIFARE DESFire para otros chips. Lo anterior, limita el universo de tarjetas disponibles en el mercado que permitan la implementación de esta funcionalidad.

- Para MIFARE Plus es posible crear una tarjeta dual interface que contenga tanto la aplicación MIFARE Plus como la aplicación para pagos bancarios EMV. Sin embargo, en este momento se debe utilizar un chip SmartMX, de NXP, toda vez que no está disponible la emulación de MIFARE Plus para otros chips. Lo anterior, limita el universo de tarjetas disponibles en el mercado que permitan la implementación de esta funcionalidad.

- Para Calypso es posible crear una tarjeta dual interface que contenga tanto la aplicación Calypso como la aplicación para pagos bancarios EMV. En este caso, la CNA desarrolló un applet Java Card, el cual puede ser instalado en la mayoría de tarjetas inteligentes que cuenten con este sistema operativo. El applet puede convivir sin inconvenientes con una aplicación financiera dentro de una tarjeta de interfaz dual. Esto brinda flexibilidad en la selección de posibles proveedores de tarjetas.

- Para CIPURSE, algunos proveedores como IDEMIA (antes Oberthur) han certificado productos de interfaz dual para aplicaciones financieras con OSTP Alliance. Sin embargo, en este momento se debe utilizar un chip Infineon, toda vez que no está disponible la emulación de CIPURSE para otros chips. Lo anterior, limita el universo de tarjetas disponibles en el mercado que permitan la implementación de esta funcionalidad.

- Las tarjetas EMV han sido diseñadas desde un principio para realizar pagos bancarios, teniendo en cuenta los requerimientos del sector financiero y los procesos asociados a la autorización de una transacción bancaria.

Calypso y EMV tienen un puntaje de 5 unidades para este criterio, considerando la multiplicidad de proveedores asociada a la integración de pagos bancarios. Asignamos a los

estándares tecnológicos MIFARE DESFire, MIFARE Plus y CIPURSE un puntaje de 4 unidades, considerando la limitación en la disponibilidad de chips para implementar esta funcionalidad.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
4	4	4	**5**	**5**

2.2.2.5. Existencia de múltiples proveedores

- Asignamos a MIFARE DESFire un puntaje de 3 unidades, ya que, si bien hay múltiples proveedores de tarjetas, existe solamente un proveedor para los chips.
- Asignamos a MIFARE Plus un puntaje de 3 unidades, ya que, si bien hay múltiples proveedores de tarjetas, existe solamente un proveedor para los chips.
- Asignamos a Calypso un puntaje de 5 unidades, ya que, para este estándar, existen múltiples proveedores de tarjetas y de chips.
- Asignamos a CIPURSE un puntaje de 3 unidades, ya que, si bien hay múltiples proveedores de tarjetas, existe solamente un proveedor para los chips.
- Asignamos a EMV un puntaje de 5 unidades, ya que, para este estándar, existen múltiples proveedores de tarjetas y de chips.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
3	3	3	**5**	**5**

2.2.2.6. Soporte

- Para el estándar MIFARE DESFire, NXP ofrece múltiples alternativas de soporte, como MICommunity, foros, sesiones de entrenamiento y Webinars. NXP programa sesiones presenciales en diferentes países de Latinoamérica, Norteamérica y Europa, con el objetivo de brindar formación intensiva en las tecnologías que desarrolla.

- Al igual que para MIFARE DESFire, para el estándar MIFARE Plus, NXP ofrece múltiples alternativas de soporte, como MICommunity, foros, sesiones de entrenamiento y Webinars. NXP programa sesiones presenciales en diferentes países de Latinoamérica, Norteamérica y Europa, con el objetivo de brindar formación intensiva en las tecnologías que desarrolla.

- Calypso cuenta con la CNA (Calypso Networks Association), como red de soporte integrada por operadores de transporte, fabricantes y consultores con amplia experiencia en la implementación de este estándar, factor que permite compartir experiencias entre los diferentes integrantes, colaborar de manera dinámica para el mejoramiento del estándar y realizar consultas sobre casos de éxito, para lograr mejoras en la implementación. Calypso también ofrece la posibilidad de programar sesiones de entrenamiento en sitio, bajo previa solicitud.

- CIPURSE ofrece soporte a través de la OSPT Alliance (Open Standard for Public Transportation), no obstante se observa que la documentación disponible para este estándar es menos abundante y de más difícil acceso que para el caso de los otros estándares considerados. OSPT Alliance también ofrece cursos sobre su tecnología.

- EMV ofrece soporte a través de vinculación a la asociación EMVco, que cuenta con abundante documentación sobre el estándar y ofrece cursos de capacitación en diferentes partes del mundo.

Asignamos un puntaje de 5 unidades a MIFARE DESFire, MIFARE Plus, Calypso y EMV por su robusta oferta de soporte y un puntaje de 4 unidades a CIPURSE, toda vez que la documentación disponible para este estándar es más limitada.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
5	**5**	4	**5**	**5**

2.2.2.7. Posibilidad de crear múltiples aplicaciones en el medio de pago

- MIFARE DESFire permite crear diferentes aplicaciones en el mismo medio de pago, personalizando cada aplicación con estructuras de archivos diferentes y llaves específicas. Así mismo, este estándar permite la creación de diferentes tipos de archivos, como archivos planos, cíclicos, lineales y de respaldo.

- MIFARE Plus permite la creación de diferentes aplicaciones, de acuerdo con la organización del mapa de memoria y considerando el almacenamiento máximo de

la tarjeta. Sin embargo, como la estructura de almacenamiento viene heredada de MIFARE Classic, la flexibilidad para crear diferentes archivos y contar con archivos de respaldo se pierde.

- Calypso permite crear diferentes aplicaciones en el mismo medio de pago, personalizando cada aplicación con estructuras de archivos diferentes y llaves específicas. Así mismo, este estándar permite la creación de diferentes tipos de archivos, como archivos planos, cíclicos, lineales y de respaldo.

- CIPURSE permite crear diferentes aplicaciones en el mismo medio de pago, personalizando cada aplicación con estructuras de archivos diferentes y llaves específicas. Así mismo, este estándar permite la creación de diferentes tipos de archivos, como archivos planos, cíclicos, lineales y de respaldo.

- EMV permite crear diferentes aplicaciones en el mismo medio de pago, personalizando cada aplicación con estructuras de archivos diferentes y llaves específicas. Así mismo, este estándar permite la creación de diferentes tipos de archivos, como archivos planos, cíclicos, lineales y de respaldo.

En conclusión, otorgamos un puntaje de 5 unidades a MIFARE DESFire, CIPURSE, Calypso y EMV, dado que tienen las mismas características de flexibilidad para la creación de múltiples aplicaciones, y un puntaje de 4 para MIFARE Plus, dado que permite crear varias aplicaciones, pero no presenta una estructura de datos tan flexible e intuitiva como los demás estándares.

MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
5	4	**5**	**5**	**5**

2.2.2.8. Casos de éxito en transporte público

- El estándar tecnológico MIFARE DESFire ha sido implementado en los sistemas de recaudo en el transporte público de ciudades como Londres, Madrid, Oslo, Vancouver, Los Ángeles y Shanghái. La tecnología DESFire es la más recomendada por NXP para la implementación de nuevos sistemas de recaudo electrónico debido a su estado de desarrollo técnico y de seguridad.

- El estándar tecnológico MIFARE Plus ha sido implementado en varias ciudades como una solución rápida que ofrece NXP al problema de seguridad que presentaron las

tarjetas MIFARE Classic. La implementación de MIFARE Plus actualmente existe en ciudades como Sao Paulo, Buenos Aires, Viena, Washington, Belgrado, Moscú y San Petersburgo. Sin embargo, en varios de estos casos, la tarjeta está operando en modo emulación de MIFARE Classic.

- Durante más de 15 años de experiencia, las soluciones Calypso se han implementado en 25 países y 125 ciudades, sin ningún inconveniente en términos de fallas técnicas o de seguridad. Entre los casos más importantes de implementaciones Calypso para recaudo en transporte público, se encuentran: Israel, Ciudad de México, París, Bruselas, Venecia, Estrasburgo, Turín y Montreal.

- El estándar CIPURSE cuenta con un número menor de implementaciones específicas en transporte público. Para el 2017, solamente existían 7 implementaciones realizadas satisfactoriamente, y algunas de ellas no eran de recaudo electrónico en transporte público, sino de control de acceso en edificios y tiquetes para eventos [4].

- Existen muy pocos casos de aplicación del estándar EMV como solución pura para el recaudo de sistemas de transporte público. Los casos más conocidos de implementación de este estándar en transporte público son Londres y Chicago. No obstante, para estos casos, EMV se ha implementado como un estándar tecnológico secundario, en complemento de estándares tecnológicos como los otros mencionados en este documento.

Asignamos a los estándares MIFARE DESFire, MIFARE Plus y Calypso un puntaje de 5 unidades para este criterio, considerando los múltiples casos de implementación con éxito para cada uno de ellos. A CIPURSE le asignamos un puntaje de 3 unidades, dado que cuenta con escasas referencias en transporte público. Al estándar EMV le asignamos un puntaje de 1 unidad, considerando que no ha sido aplicado como solución principal para sistemas de transporte público.

MIFARE DESFire EV2	**MIFARE Plus**	**CIPURSE**	**Calypso**	**EMV**
5	**5**	3	**5**	1

2.2.3. Resultados del análisis multicriterio

La siguiente tabla presenta la matriz multicriterio y los resultados del análisis teniendo en cuenta las justificaciones expuestas en la sección anterior.

		MIFARE DESFire EV2	MIFARE Plus	CIPURSE	Calypso	EMV
Criterio	**Peso**	**Puntaje**	**Puntaje**	**Puntaje**	**Puntaje**	**Puntaje**
Costos	20.00%	3.4	4.6	5	3.4	1
Seguridad	15.00%	4.6	4.6	4.6	4.6	5
Pago con celulares	10.00%	5	5	5	5	5
Pagos bancarios	10.00%	4	4	4	5	5
Múltiples proveedores	10.00%	3	3	3	5	5
Soporte	10.00%	5	5	4	5	5
Multi-aplicación	10.00%	5	4	5	5	5
Casos de éxito en transporte público	15.00%	5	5	3	5	1
Total	**100.00%**	**4.32**	**4.46**	**4.24**	**4.62**	**3.6**

Fuente: Elaboración propia

En nuestro análisis multicriterio, Calypso obtiene el mayor puntaje, seguido por los estándares tecnológicos MIFARE Plus y MIFARE DESFire. Recomendamos, con base en este análisis, se adopte el estándar tecnológico Calypso para el desarrollo de los medios de pago recargables en el sistema interoperable de recaudo de Quito.

3. Selección del estándar tecnológico para el medio de pago no recargable

Los medios de pago no recargables están diseñados para usuarios esporádicos que no usan el sistema de transporte público de forma regular. Este medio de pago se venderá con un saldo precargado, no se podrá recargar y se desechará cuando su saldo se agote.

Existen tres estándares tecnológicos adecuados para este propósito: CIPURSE move, Calypso Light Application y MIFARE Ultralight. A continuación presentamos una breve reseña de cada uno de estos estándares, los criterios y pesos para su evaluación, y el análisis multicriterio para comparar estos tres estándares.

3.1. Estándares disponibles en el mercado

3.1.1. MIFARE Ultralight EV1

El estándar tecnológico MIFARE Ultralight EV1 [5] hace parte de la última generación de productos de NXP para tiquetes inteligentes de papel y tarjetas, de bajo costo y aplicaciones de gran escala. Su misión es reemplazar a los tiquetes tradicionales de papel, banda magnética y de código de barras. Sus principales ventajas son:

- Cuenta con mecanismos anti-clonación y de protección de escritura del medio de pago.
- Su capacidad de memoria es suficiente para las aplicaciones de transporte público.
- Tiene tres contadores que permiten almacenar información de saldo.
- Es compatible con otros medios de pago recargables.
- Cuenta con mecanismos de lectura y escritura rápida, protegidos con contraseña configurable.

3.1.2. CIPURSE Move

CIPURSE move es una alternativa para medios de pago sin contacto de uso esporádico y de bajo costo. Es una solución robusta en términos de seguridad, que permite el almacenamiento seguro de llaves AES-128 y permite llevar a cabo un proceso de autenticación mutua 3-pass AES-128. A su vez, es posible crear hasta tres archivos elementales configurables en la aplicación CIPURSE. [6]

Dentro de los mecanismos de seguridad, se contempla el uso de dos llaves AES-128 configurables para la aplicación CIPURSE y el cifrado de la información mediante la generación de MAC (Message Authentication Code) para las transacciones efectuadas.

El estándar tecnológico CIPURSE move ha surgido con el propósito de ser utilizado como medio de pago para viajes sencillos en sistemas de transporte público y como medio para el acceso a eventos, donde se encuentran sus principales aplicaciones hoy en día.

3.1.3. Calypso Light Application

Calypso Light Application (CLAP) fue lanzada en 2017. Diseñada con los usuarios esporádicos en mente, CLAP puede ser implementada en tiquetes de papel de bajo costo y en otros objetos portables, como un teléfono móvil con NFC (Near-Field Communication) y un reloj inteligente con un componente *contactless* embebido.

En cuanto a las características tecnológicas del estándar, CLAP contempla un proceso de autenticación mediante sesión segura y un mecanismo de ratificación, al final de las transacciones, para la confirmación de la ejecución exitosa de las mismas. Las llaves usadas por CLAP son tres llaves TDES de 112 bits y, para el intercambio de información entre el objeto portable y el equipo lector, se lleva a cabo el cálculo de un MAC, para garantizar la integridad del mensaje. La estructura de datos, por su parte, se basa en la aplicación CLAP, compuesta por una serie de archivos o *Elementary Files* (EF), los cuales pueden ser lineales, cíclicos o contadores, y se encuentran organizados por registros. [7]

3.2. Comparación de estándares

3.2.1. Criterios y pesos asignados

Para la comparación de los estándares tecnológicos de medios de pago no recargables, consideramos los criterios de costo, seguridad,existencia de múltiples proveedores, soporte, memoria de datos y casos de éxito.

- **Costos (30%):** Criterio que define el costo unitario por tarjeta para cada una de las tecnologías, así como las diferencias sustanciales que puede haber entre los costos de toda la plataforma de implementación para un sistema con la tecnología del medio de pago respectiva.
- **Seguridad (10%):** Para el criterio de seguridad hemos tenido en cuenta dos aspectos. El método de autenticación usado por cada estándar y la disponibilidad de MAC para garantizar la integridad de la información transmitida.
- **Existencia de múltiples proveedores (15%):** Criterio que se encuentra asociado a la multiplicidad de proveedores a nivel de chip y de tarjeta para cada estándar.
- **Soporte (20%):** Criterio relacionado con el soporte ofrecido para cada uno de los estándares tecnológicos, incluyendo documentación, disponibilidad de redes de operadores, capacitación y entrenamiento en el estándar tecnológico.
- **Memoria de datos (5%):** Este criterio está relacionado con el tamaño de la memoria de datos disponible en el medio de pago no recargable.
- **Casos de éxito en transporte público (20%):** Casos de éxito para cada uno de los estándares.

3.2.2. Valoración de los estándares a la luz de cada criterio

3.2.2.1. Costos

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta MIFARE Ultralight EV1 es de US$ 0.22.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta CIPURSE move es de US$ 0.25.

- Para un volumen de compra de 500.000 tarjetas, en blanco y puestas en fábrica del proveedor, el costo unitario promedio por tarjeta CLAP es de US$0.50.

El costo de la plataforma tecnológica es similar bajo todos los estándares tecnológicos considerados.

Asignamos un puntaje de 5 unidades a MIFARE Ultralight EV1, como la alternativa menos costosa para este criterio. Para CLAP asignamos un puntaje de 1 unidad, por ser el estándar de mayor costo. Se asigna un puntaje de 4.57 para CIPURSE, con base en una proyección lineal, teniendo como referencia los puntajes asignados a MIFARE Ultralight EV1 y CLAP.

MIFARE Ultralight EV1	CIPURSE move	Calypso Light Application
5	4.57	1

3.2.2.2. Seguridad

Método de autenticación:

- MIFARE Ultralight EV1 emplea un método de autenticación ad-hoc basado en el uso de un password de 32 bits.

- CIPURSE move utiliza un proceso estándar de autenticación mutua con llaves AES-128.

- Para CLAP utiliza un proceso estándar de autenticación mutua con llaves TDES de 112 bits.

Asignamos un puntaje de 5 unidades a CIPURSE move, por usar un proceso de autenticación mutua, con base en llaves AES-128. Asignamos 4 unidades a CLAP, por contar con un

método de autenticación con llaves TDES y un puntaje de 2 unidades a MIFARE Ultralight EV1, dado que este cuenta con un método de autenticación por password de 32 bits.

Integridad de los datos

- MIFARE Ultralight EV1 no utiliza mecanismos criptográficos para garantizar la integridad de los datos.
- CIPURSE move utiliza un MAC con llaves AES-128, para garantizar la integridad de los datos.
- Para CLAP utiliza un MAC con llaves TDES de 112 bits, para garantizar la integridad de los datos.

Asignamos un puntaje de 5 unidades a CIPURSE move, por emplear un MAC AES para asegurar la integridad de los datos. Asignamos un puntaje de 4 unidades a CLAP, por utilizar un MAC TDES para este mismo propósito. MIFARE Ultralight EV1 recibe un puntaje de 1 unidad, por no contar con ningún mecanismo para garantizar la integridad de los datos.

Subcriterio	**Peso**	**MIFARE Ultralight EV1**	**CIPURSE move**	**CLAP**
Método de autenticación	**80%**	2	5	4
Integridad de los datos	**20%**	1	5	4
Puntaje ponderado	**100%**	1.8	**5**	4

Es importante tener en cuenta que el criterio de seguridad para estos medios de pago no tiene un peso alto, considerando que no serán recargables.

3.2.2.3. Existencia de múltiples proveedores

- Asignamos a MIFARE Ultralight EV1 un puntaje de 3 unidades, ya que, si bien hay múltiples proveedores de tarjetas, existe solamente un proveedor para los chips.

- Asignamos a CIPURSE move un puntaje de 3 unidades, ya que, si bien hay múltiples proveedores de tarjetas, existe solamente un proveedor para los chips.

- Asignamos a CLAP tiene un puntaje de 5 unidades, ya que, para este estándar, existen múltiples proveedores de tarjetas y de chips.

A continuación, se muestran los puntajes para el criterio de multiplicidad de proveedores, para cada estándar tecnológico:

MIFARE Ultralight EV1	CIPURSE move	CLAP
3	3	**5**

3.2.2.4. Soporte

- Para el estándar MIFARE Ultralight EV1, NXP ofrece múltiples alternativas de soporte, como MICommunity, foros, sesiones de entrenamiento y Webinars. NXP programa sesiones presenciales en diferentes países de Latinoamérica, Norteamérica y Europa, con el objetivo de brindar formación intensiva en las tecnologías que desarrolla.

- CIPURSE move ofrece soporte a través de la OSPT Alliance (Open Standard for Public Transportation), no obstante se observa que la documentación disponible para este estándar es menos abundante y de más difícil acceso que para el caso de los otros estándares considerados. OSPT Alliance también ofrece cursos sobre su tecnología.

- Calypso cuenta con la CNA (Calypso Networks Association), como red de soporte integrada por operadores de transporte, fabricantes y consultores con amplia experiencia en la implementación de este estándar, factor que permite compartir experiencias entre los diferentes integrantes, colaborar de manera dinámica para el mejoramiento del estándar y realizar consultas sobre casos de éxito, para lograr mejoras en la implementación. Calypso también ofrece la posibilidad de programar sesiones de entrenamiento en sitio, bajo previa solicitud.

Asignamos un puntaje de 5 unidades a MIFARE Ultralight EV1 y Calypso Light Application, por su robusta oferta de soporte y un puntaje de 4 unidades a CIPURSE, toda vez que la documentación disponible para este estándar es más limitada.

MIFARE Ultralight EV1	CIPURSE move	CLAP
5	4	**5**

3.2.2.5. Memoria de datos

- Asignamos a MIFARE Ultralight EV1 un puntaje de 5 unidades, ya que el tamaño de sus memoria de datos va desde los 48 bytes hasta los 128 bytes, en todos los casos, suficiente para almacenar los datos para la aplicación de transporte de Quito.

- Asignamos a CIPURSE move un puntaje de 5 unidades, ya que el tamaño de su memoria de datos es de 304 bytes, suficiente para almacenar los datos para la aplicación de transporte de Quito.

- Asignamos a CLAP tiene un puntaje de 5 unidades, ya que el tamaño de memoria de datos va desde 48 bytes y aumenta dependiendo del elemento hardware del objeto portable utilizado.

MIFARE Ultralight EV1	CIPURSE move	Calypso Light Application
5	**5**	**5**

3.2.2.6. Casos de éxito en transporte público

- El estándar MIFARE Ultralight ha sido implementado para medios de pago no recargables en los sistemas de recaudo de ciudades como Sydney, Montreal, Moscú, Amsterdam y Venecia. Además de su aplicación en transporte público, este estándar tecnológico ha sido ampliamente implementado para el control de acceso a eventos, el control de ingreso a edificios y a eventos deportivos, entre otros.

- Para el estándar CIPURSE no se logran identificar implementaciones exitosas a la fecha como medios de pago no recargables en transporte público. [4]

- Dado que CLAP ha sido introducido en 2017, no existen casos de implementación a la fecha.

Asignamos un puntaje de 5 unidades a MIFARE Ultralight, ya que es el estándar más utilizado hoy en día para medios de pago de bajo costo en transporte público. Hemos asignado un puntaje de 1 unidad a CIPURSE move y a CLAP, ya que no se identifican a la fecha casos de implementación en sistemas de transporte público.

MIFARE Ultralight EV1	CIPURSE move	Calypso Light Application
5	1	1

3.2.3. Resultados del análisis multicriterio

La siguiente tabla presenta la matriz multicriterio y los resultados del análisis para el medio de pago no recargable, teniendo en cuenta las justificaciones expuestas en la sección anterior.

		MIFARE Ultralight EV1	CIPURSE move	Calypso Light Application
Criterio	**Peso**	**Puntaje**	**Puntaje**	**Puntaje**
Costos	30.00%	5	4.57	1
Seguridad	10.00%	1.8	5	4
Múltiples proveedores	15.00%	3	3	5
Soporte	20.00%	5	4	5
Memoria de datos	5.00%	5	5	5
Casos de éxito en transporte público	20.00%	5	1	1
Total	**100.00%**	**4.38**	**3.57**	**2.9**

Fuente: Elaboración propia

En nuestro análisis multicriterio, MIFARE Ultralight EV1 obtiene el mayor puntaje, seguido por los estándares tecnológicos CIPURSE move y CLAP. Recomendamos, con base en este análisis, se adopte el estándar tecnológico MIFARE Ultralight EV1 para el desarrollo de los medios de pago no recargables en el sistema interoperable de recaudo de Quito.

4. Referencias

[1] NXP Semiconductors, «MIFARE,» May 2018. [En línea]. Available: https://www.mifare.net/wp-content/uploads/2018/05/MIFARE-DESFire-EV2_Product-Flyer_0518_Web.pdf. [Último acceso: 25 September 2018].

[2] NXP Semiconductors, «MIFARE Plus,» 2018. [En línea]. Available: https://www.nxp.com/products/identification-and-security/mifare-ics/mifare-plus:MC_57609. [Último acceso: 25 September 2018].

[3] Gemalto, «Gemalto,» 2018. [En línea]. Available: https://www.gemalto.com/companyinfo/digital-security/techno/emv. [Último acceso: 25 September 2018].

[4] O. Alliance, «Presentation: Introduction to OSPT & CIPURSE,» 2017. [En línea]. Available: http://www.e-transport.ru/sites/default/files/ospt_presentation_final.pptx.

[5] NXP, Data sheet - MF0ULx1 MIFARE Ultralight EV1 - Contactless ticket IC Rev 3.1, 2014.

[6] Infineon, CIPURSE move - SLM 10TLC001L Product Brief, 2016.

[7] Calypso, Calypso specification - Light Application for Portable Objects "CLAP". Version 1.1., 2017.

[8] NXP, «MIFARE4Mobile,» 2018. [En línea]. Available: https://www.mifare4mobile.org/.

[9] O. Alliance, «HCE Based Transport Ticketing Solution Combining CIPURSE™ and Tokenization,» 2017. [En línea]. Available: http://www.osptalliance.org/assets/pdf/HCE_Tokenisation_Jan2017.pdf.

[10] C. N. Association, «CALYPSO HCE SOLUTION FOR NFC DEVICES WITHOUT SECURE ELEMENT,» 2018. [En línea]. Available: https://www.calypsonet-asso.org/content/calypso-hce-solution-nfc-devices-without-secure-element.

[11] NXP, «SmartMX for programmable, high-security, multi-application smart cards,» 2018. [En línea]. Available: https://www.nxp.com/docs/en/brochure/75017515.pdf.

[12] C. N. Association, «THE CALYPSO APPLET,» 2018. [En línea]. Available: https://www.calypsonet-asso.org/the-calypso-applet.

[13] IDEMIA, «OT RELEASES FIRST DUAL INTERFACE PRODUCT MATCHING ALL NEW VISA AND MASTERCARD SPECIFICATIONS FOR US MARKET,» 2016. [En línea]. Available: http://www.oberthur.com/ot-releases-first-dual-interface-product-matching-all-new-visa-and-mastercard-specifications-for-us-market/.

[14] C. N. Association, «THE CALYPSO APPLET,» 2018. [En línea]. Available: https://www.calypsonet-asso.org/the-calypso-applet.