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

ENTREGABLE 1
COMPONENTE TECNOLÓGICO DEL MODELO DE INTEROPERABILIDAD

10/12/2018

Contenido

Figuras

Revisiones

Versión	Fecha	Elaborado por	Descripción
2	14/08/2018	GSD+	Atiende las observaciones de EPMMQ con fecha 1 de agosto de 2018
3	09/10/2018	GSD+	Inclusión de análisis y selección de estándares tecnológicos para medios de pago a partir de matriz multicriterio
4	03/12/2018	GSD+	Atiende las observaciones de EPMMQ con fecha 20 de septiembre de 2018

Glosario

Introducción

En el presente documento se presenta una definición de los componentes críticos de las soluciones tecnológicas que constituirán un entorno de interoperabilidad para el sistema integrado de recaudo (SIR) del SITM-Q. Se presenta una recomendación para la tecnología de medio de pago que se utilizará para el SIR, se presenta el diseño de alto nivel del sistema de gestión global y se especifican detalles del banco de pruebas desarrollado para validar las especificaciones técnicas que se hacen para los medios de pago y equipos del SIR.

Se incluye como documento anexo, el Manual de Normatividad Técnica que se utilizará para la implementación del SIR del SITM-Q. Este manual contiene especificaciones técnicas de los medios de pago y de los dispositivos que conforman el sistema de recaudo.

El presente documento tiene tres capítulos, así:

Capítulo 1 – Contexto del Sistema Integrado de Transporte Masivo de Quito

En este capítulo, se presenta el conjunto de funcionalidades y requerimientos del SIR en la PLMQ también teniendo en cuenta la posterior actualización de los sistemas de recaudo del Metrobús, del sistema Quito Cables y de los Convencionales. Así mismo se enumeran y se profundiza en los requerimientos actuales y posibles requerimientos futuros del SITM-Q.

Capítulo 2 – Selección de la tecnología de los medios de pago

En este capítulo, se presenta un análisis comparativo de estándares tecnológicos de medios de pago, compatibles con el estándar ISO 14443 y ampliamente utilizados a nivel mundial para sistemas de recaudo automático en transporte. Se presenta una comparación de funcionalidad, costos, disponibilidad en el mercado, adopción y proyección en el mercado, adaptación de la tecnología a nuevas tendencias en interoperabilidad (e.g., NFC, HCE). Por último, se lleva a cabo un análisis multicriterio, teniendo en cuenta la información presentada y se recomiendan la adopción de dos estándares tecnológicos para Quito.

Capítulo 3 – Diseño de alto nivel del Sistema de gestión global

Contiene especificaciones de las funcionalidades con las que debe contar el Sistema de Gestión Global para ejecutar las funcionalidades de interoperabilidad. Para esto se definen las reglas y procesos operacionales necesarios para realizar el cálculo de la posición neta de cada SIR en cada periodo de compensación.

Este informe tiene dos anexos:

Anexo 1 – Informe de Banco de pruebas

Con el fin de verificar la validez de la norma técnica, se presentan los resultados de pruebas de laboratorio en las cuales se valida la coherencia y completitud del mapa de memoria, el modelo transaccional, y del modelo de seguridad para la ejecución de

transacciones. Para esto, también se presenta una descripción de los equipos utilizados para las pruebas y se documentan resultados para los dos tipos de medios de pago recomendados (recargable y no recargable).

Anexo 2 – Manual de normatividad técnica

Se presenta un documento técnico que contiene las especificaciones del mapa de datos de los medios de pago, el esquema de seguridad, los casos de uso y el protocolo de pruebas para la infraestructura tecnológica del SIR.

Anexo 3 – Descripción del entorno seguro de emisión de módulos SAM.

Se describe el proceso de generación segura de las llaves de sistema. Posteriormente, se describen los requisitos y procedimientos que deben cumplirse para realizar la emisión segura de los módulos SAM que contengan dichas llaves. Finalmente, se identifican los posibles riesgos del procedimiento y se plantean estrategias de mitigación y solución.

A lo largo de este documento, se mencionarán algunas entidades que harán parte del SIR. A continuación se da una definición preliminar de estas entidades para facilitar la lectura del documento:

- *Cámara de Compensación:* Es la entidad encargada de recibir la información de recaudo de todo el sistema y determinar los montos a compensar para todos los actores involucrados.

- *Operadores de Recaudo:* Son las entidades encargadas de recaudar los pagos que los usuarios realizan para utilizar los servicios del SIT. También están encargados de otorgar acceso a los usuarios válidos del sistema.

- *Empresas Prestadoras de Servicio:* Son las empresas que brindan el servicio de transporte a los usuarios autorizados por los Operadores de Recaudo. Su función es remunerada por los Operadores de Recaudo.

1. Contexto del Sistema Integrado de Transporte Masivo de Quito

Como resultado de la aprobación de la Ordenanza Metropolitana No. 185 por el Concejo Metropolitano de Quito el 19 de septiembre de 2017, que posibilita la implementación de Sistemas Inteligentes de Transporte (SIT) para el SITM-Q, se ha dado lugar a un proceso de consultoría para definir el modelo de interoperabilidad que se utilizará en el Sistema Integrado de Recaudo (SIR) del SITM-Q.

En aras de desarrollar satisfactoriamente este proceso, el DMQ ha establecido los términos de referencia para la contratación del SIR para los subsistemas del Metro, Metrobús-Q, Quito Cables y Convencionales. El primer paso para diseñar un sistema interoperable de recaudo para estos subsistemas consiste en hacer una selección de la tecnología de medios de pago recargables que garantice interoperabilidad entre los

cuatro subsistemas que componen al SITM-Q, independientemente de la fecha de vinculación de cada subsistema al SIR.

Por esta razón, se debe tener en cuenta el conjunto de funcionalidades y requerimientos para la adopción rápida del SIR en la PLMQ, y para la posterior actualización de los sistemas de recaudo del Metrobús, del sistema Quito Cables y de los Convencionales. A continuación, se enumeran algunos de los requerimientos actuales y futuros del SITM-Q:

1. **Tarifas diferenciadas por tipo de usuario**

Según la ordenanza No. 54 del 2 de abril de 2015, los usuarios categorizados como adulto mayor de 65 años, estudiante, discapacitado, y menor de 12 años, reciben un 50% de descuento en la tarifa que se cobra en cualquiera de los sistemas que pertenecen a la red del SITM-Q.

2. **Tarifas diferenciadas por horario**

El Sistema Integrado de Recaudo deberá permitir la definición y modificación de tarifas diferenciadas por franjas horarias, en caso de que en el futuro se deseen implementar tarifas nocturnas o tarifas para horas pico.

3. **Tarifas diferenciadas por tipo y subtipo de modo de transporte**

El Sistema Integrado de Recaudo deberá permitir la definición y modificación de tarifas diferenciadas por subtipos de Metrobús-Q (i.e., Trolebús, Metrobús, Intracantonal, Interparroquial, alimentador, etc.).

4. **Tarifa variable por transferencias**

Teniendo en cuenta que los usuarios tendrán la posibilidad de hacer trasbordos entre subsistemas del SITM-Q éste deberá permitir la definición y modificación de tarifas por transferencia, una ventana de tiempo de transferencias y número máximo de transferencias dentro de la ventana de tiempo.

5. **Tarifa variable por distancia de recorrido**

El medio de pago debe poder adaptarse a esquemas de tarificación variables en función de la distancia recorrida por un usuario. Este esquema puede implementarse inicialmente con el sistema de Metro de Quito y posteriormente con el sistema Quito Cables y Metrobús-Q. Es necesario que los usuarios hagan uso del medio de pago a la entrada y a la salida del sistema para sobrepasar las barreras de seguridad (e.g., torniquetes) y así registrar los puntos de origen y destino para estimar la tarifa. Para el caso del sistema Convencional la implementación de este esquema de tarificación requiere medir la distancia recorrida y los puntos de parada del vehículo haciendo uso de un sistema GPS. Sin embargo, en el caso de los servicios interparroquiales, o para el servicio de bus al aeropuerto, para los cuales las tarifas ya están diferenciadas en función de la distancia, no se requiere de equipos especiales, siempre y cuando haya un único punto de parada final, común para todos los usuarios.

6. **Viaje a crédito**

A los usuarios del SITM-Q se les permitirá acceder a la red aun cuando no tengan saldo suficiente para adquirir un contrato de uso del servicio. Podrán acreditar a su medio de pago un monto que no exceda el valor de un contrato para hacer uso del SITM-Q.

7. **Unidades de saldo en moneda local**

Es necesario que las unidades de saldo almacenadas en el medio de pago estén dadas en centavos de dólar estadounidense (USD).

8. **Compatibilidad de medios de pago recargables con medios de pago esporádicos**

La tecnología debe ser compatible con medios de pago de uso desechable, no recargables destinados para tarifas generales y usuarios esporádicos (e.g., turistas). En primer lugar, debe definirse la tecnología idónea para medios de pago esporádicos y luego, debe garantizarse que ésta sea compatible con la tecnología que se seleccione para medios de pago recargables.

9. **Posible integración con Movilízate UIO (futuro)**

El medio de pago debe ser compatible con la tecnología NFC de dispositivos móviles para la consulta de saldo a través de la aplicación Movilízate UIO.

10. **Posible integración con sistema bancario (futuro)**

La tecnología debe ser compatible con medios de pago bancarios, ya sea con tarjetas híbridas o tarjetas con certificación EMV.

11. **Posible integración de BiciQuito con el SITM-Q (futuro)**

La tecnología que se seleccione para el medio de pago debe poder utilizarse para acceder a los servicios del sistema BiciQuito. Por ende, es necesario que el medio de pago permita guardar información relevante sobre la bicicleta que se alquila a los usuarios, además de almacenar información sobre el propietario y los términos contractuales del préstamo (e.g., duración del préstamo, estado del último préstamo, etc.).

12. **Posible integración de Estacionamientos con el SITM-Q (futuro)**

La tecnología que se seleccione para el medio de pago debe poder utilizarse para realizar el pago de estacionamientos. Por ende, es necesario que el medio de pago permita guardar información relevante sobre el vehículo del usuario, además de almacenar los términos contractuales del uso del estacionamiento (e.g., duración de cada uso del estacionamiento, tarifa aplicable del estacionamiento, etc.).

2. Selección de estándares tecnológicos para medios de pago

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.

2.1 Selección del estándar tecnológico para el medio de pago recargable

2.1.1 Estándares disponibles en el mercado

2.1.1.1 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].

2.1.1.2 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]

2.1.1.3 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.

2.1.1.4 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.

2.1.1.5 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]

2.1.2 Comparación de estándares

2.1.2.1 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.

2.1.2.2 Valoración de los estándares a la luz de cada criterio

2.1.2.2.1 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

2.1.2.2.2 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**

2.1.2.2.3 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

2.1.2.2.4 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**

2.1.2.2.5 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**

2.1.2.2.6 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**

2.1.2.2.7 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**

2.1.2.2.8 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

2.1.3 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.

2.2 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.

2.2.1 Estándares disponibles en el mercado

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 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]

2.2.2 Comparación de estándares

2.2.2.1 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.

2.2.2.2 Valoración de los estándares a la luz de cada criterio

2.2.2.2.1 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 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

2.2.2.2.2 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.

2.2.2.2.3 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**

2.2.2.2.4 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**

2.2.2.2.5 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**

2.2.2.2.6 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

2.2.3 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.

3. Diseño de alto nivel del Sistema de gestión global

3.1. Interoperabilidad y cámara de compensación

La visión del SITM-Q contempla una integración tarifaria y de medios de pago para todos los modos de transporte actuales y futuros de la ciudad. Además, se contempla la prestación de servicios de la ciudad como acceso y uso de bibliotecas, acceso a instituciones educativas y de salud mediante un único medio de pago y acceso. La prestación de los futuros servicios ciudadanos y de transporte será dada por entidades diferentes a los Operadores de Recaudo. Para lograr el objetivo de integración tarifaria y de medios de pago se requiere que todos los Operadores de Recaudo se interconecten a través de una Cámara de compensación. Esta interconexión permite intercambiar la información transaccional de los usuarios entre entidades y así poder remunerar a todas las entidades de forma consistente. La Cámara de compensación, así como los medios de pago unificados son el pilar del concepto de Interoperabilidad de recaudo, donde una unificación de medios de pago y una interconexión estructurada de sistemas garantizan la multiplicidad y diversidad de Operadores de Recaudo y la simplificación de las reglas tarifarias y de acceso para los usuarios. El siguiente diagrama presenta las interconexiones que podría ofrecer la Cámara de compensación en un futuro:

Figura 1. Integración de servicios a la cámara de compensación

Fuente: elaboración propia

3.1.1 Requisitos generales para la compensación

Para la implementación de la cámara de compensación para el SIR del SITM-Q, será necesario definir su arquitectura y las posibles interacciones que pueden darse entre

cada uno de los agentes que hacen parte de la red de compensación. Para esto es posible seleccionar una de las dos arquitecturas que se presentan en esta sección, en las cuales se cuenta con una Cámara de Compensación en la cual se centraliza la información de la red interoperable.

Independientemente de la arquitectura, es necesario que los Operadores de Recaudo acuerden interfaces de comunicación con la Cámara de Compensación, para enviar y recibir información transaccional del sistema de recaudo. Independientemente de las características técnicas de la interfaz de comunicación, se debe respetar y cumplir con el contenido y formato de los archivos de información transaccional detallados en el Manual de Normatividad Técnica. Aunque la ejecución y el correcto desempeño de este proceso están completamente a cargo de los Operadores de Recaudo, la Cámara de Compensación estará en la libertad de supervisar el proceso, y será la encargada de ejecutar los cálculos de compensación para remunerar a los actores de cada uno de los subsistemas de transporte que componen al SITM-Q.

Adicionalmente, será necesario definir un periodo de compensación, el cual corresponde al número de días sobre los cuales se hace el cálculo de las remuneraciones asociadas a interoperabilidad. Para el cálculo de la compensación será necesario remunerar a los actores, por los servicios de venta de medios de pago, aceptación de medios de pago, y recarga.

La Autoridad de transporte, con el apoyo del Comité de Interoperabilidad, tendrá la potestad de definir el definir el costo del medio de pago. Esta misma entidad tendrá la responsabilidad de definir una función de remuneración para determinar la compensación que debe recibir cada uno de los actores. Esta función de remuneración debe tener en cuenta múltiples factores, por ejemplo, número de transacciones de aceptación, valor de comisión por recarga, comisiones asociadas a la interoperabilidad, entre otros.

En general, el periodo de compensación puede dividirse en cuatro etapas:

- ***Etapa 1: Generación de transacciones***
- ***Etapa 2: Envío de transacciones a Cámara de Compensación***
- ***Etapa 3: Cálculo de la compensación y envío de cuentas de cobro***
- ***Etapa 4: Liquidación de las cuentas de cobro***

Es posible que el sistema de recaudo tenga un flotante de dinero no utilizado, correspondiente a los montos depositados en los medios de pago por concepto de recargas que pueden ser considerados como unidades de valor que nunca serán usadas en el sistema debido al abandono por parte del usuario de un saldo remanente en su medio de pago. Un monto se comenzará a identificar como flotante no utilizado luego de un periodo de inactividad total en el medio de pago, acordado entre los actores del SIR (después de la última transacción hecha con el medio de pago), y el manejo del dinero correspondiente a las unidades de valor no utilizadas estará a libertad de la(s) Empresa(s) Prestadora(s) del Servicio que tenga(n) dicho dinero. Una vez se alcance este periodo, la tarjeta con flotante deberá ser bloqueada y no podrá ser usada

Independientemente de la arquitectura del sistema de gestión global, será necesario que el dinero de las recargas de medios de pago, con el cual se otorga acceso a los usuarios, sea recaudado por los Operadores de Recaudo (OR), los cuales pueden operar en múltiples subsistemas del SITM-Q. Es decir, no es necesario que cada Empresa Prestadora de un servicio de transporte tenga un único OR, es posible que un OR atienda a múltiples Empresas Prestadoras de Servicio, o que cada Empresa Prestadora de Servicio sea atendida por un único OR.

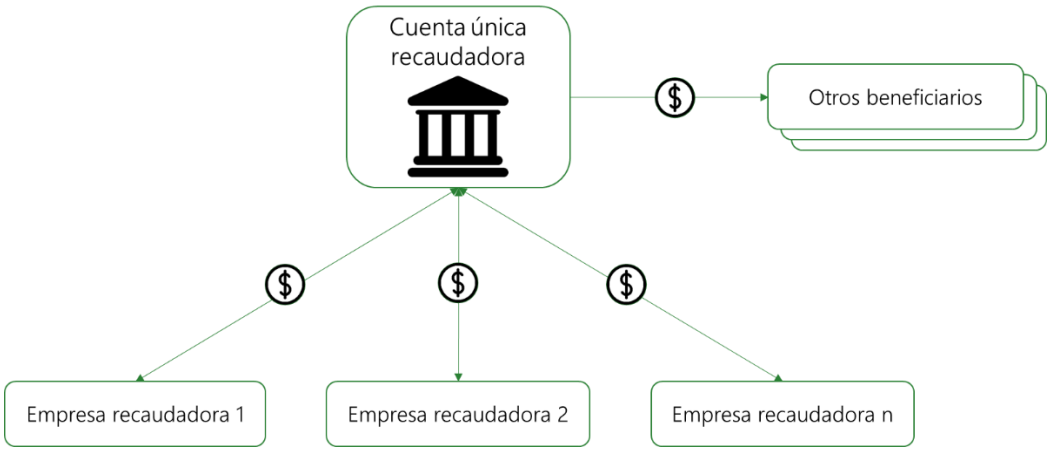
3.1.2 Arquitecturas posibles para el Sistema de gestión global

3.1.2.1 Arquitectura centralizada

La cámara de compensación puede tener una arquitectura centralizada, en la cual, todo el dinero recaudado por las empresas operadoras de recaudo se deposita en una única cuenta de ciudad, la cual puede ser manejada por la entidad reguladora de la Cámara de Compensación, o por una Autoridad de Transporte (e.g., la Municipalidad). La función principal de la entidad reguladora de la Cámara de Compensación es calcular y confirmar la remuneración para cada una de los actores de la red. Basado en esto, la entidad reguladora de la cámara puede efectuar las transacciones de pago para cada uno de los beneficiarios durante un periodo de compensación acordado entre todos los actores de la red (ver Figura 2).

Con esta arquitectura, el manejo del dinero recae en la entidad reguladora de la Cámara de Compensación, como entidad independiente. Por tanto, la confianza de cada actor en el sistema depende únicamente de la confianza en esta entidad. Además, el dinero considerado como flotante queda a disposición de la Autoridad de Transporte, la cual deberá reinvertirlo en el sistema de transporte.

Figura 2. Esquema de cámara de compensación centralizada.



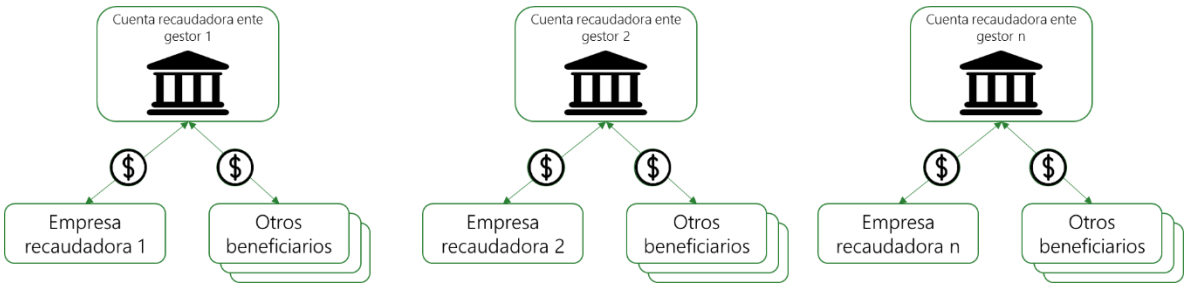
Fuente: elaboración propia

3.1.2.2 Arquitectura descentralizada

La cámara de compensación puede tener una arquitectura descentralizada, en la cual, cada uno de los Operadores de Recaudo de los subsistemas de transporte tiene una

cuenta para depositar los fondos recaudados en su sistema. En este caso, la Cámara de Compensación opera como una entidad encargada de contabilizar la totalidad de las transacciones del sistema y de estimar la remuneración para cada uno de los Operadores de Recaudo. Debido a que no existe una cuenta única de ciudad, la Cámara de Compensación debe estimar los valores de dinero que deben intercambiarse entre las cuentas destinadas a recaudo de cada Operador, para efectuar un cruce de cuentas que permita remunerar apropiadamente a cada actor por sus servicios. El cruce de cuentas debe estimarse de modo que se minimice el número de transacciones entre Operadores de Recaudo.

Figura 3. Esquema de cámara de compensación descentralizada.



Fuente: elaboración propia

Con esta arquitectura, el manejo del dinero recae en diferentes entes gestores involucrados en la red. Por tanto, la confianza de cada actor en el sistema depende de que exista confianza con todos los entes gestores. Además, el dinero considerado como flotante queda a disposición estos entes particulares.

3.1.3 Tabla comparativa de arquitecturas para el Sistema de gestión global

Teniendo en cuenta las características de las arquitecturas anteriormente descritas, se desarrolló la siguiente tabla comparativa, con el objetivo de asistir en la selección del modelo a utilizar en el SITM-Q.

	Arquitectura Centralizada	**Arquitectura descentralizada**
Control de flujo de dinero	Los flujos de dinero son controlados y supervisados por la Autoridad de Transporte, y ejecutados por la entidad reguladora de la Cámara de Compensación. Se requiere alto nivel de confianza en la entidad reguladora.	Los flujos de dinero son controlados y supervisados por la Autoridad de Transporte, y ejecutados por el ente gestor de cada subsistema. Se requiere confianza en cada uno de los demás entes gestores.

Complejidad	Menor número de transacciones, debido a que todos los actores se relacionan con una única cuenta de ciudad.	Mayor número de transacciones, ya que debe haber transacciones de compensación entre todas las cuentas de los entes gestores.
Rentabilidad del flotante	La rentabilidad del flotante es administrada y aprovechada por la Autoridad de Transporte.	Las rentabilidades del flotante son administradas y aprovechadas por particulares.
Autonomía en gestión de pagos de los subsistemas	Cada subsistema debe seguir lineamientos definidos por la Autoridad de Transporte.	Cada subsistema es libre de elegir su esquema de gestión de pagos.

Fuente: Elaboración propia

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] Common Criteria, Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 4, 2012.

[9] ISO/IEC, ISO/IEC 14443-1 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics, 2016.

[10] ISO/IEC, ISO/IEC 14443-2: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface, 2016.

[11] ISO/IEC, ISO/IEC 14443-3: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision, 2011.

[12] ISO/IEC, ISO/IEC 14443-4: Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol, 2016.

[13] CNA, Calypso Specification Rev. 3.1 Ref: 060708-CalypsoAppli, Editado por Spirtech, 2013.

[14] Global Platform, Card Specification v.2.3, 2015.

[15] CNA, Calypso Handbook - Ref: 100324-CalypsoHandbook-11, 2010.

[16] NXP, «Registered Partners,» 2018. [En línea]. Available: https://www.mifare.net/en/.

[17] Spirtech, Stored Value Guidelines, 2016.

[18] Calypso, Calypso Security White Paper, Ref: 080131-CalypsoSecurity, Spitech, 2012.

[19] NXP, Data sheet - MF3ICD81 MIFARE DESFire EV1 Rev. 3.6 document number 134036, 2011.

[20] Calypso, Calypso vs. EMVCo CL L1 Specifications v1.00, Galitt, 2007.

[21] Gemalto, «Contactless EMV cards,» Octubre 2017. [En línea]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/fs-contactless-EMV-cards.pdf.

[22] Calypso, Application Downloading, Trusted Labs, Spirtech, 2011.

[23] NXP, NXP J3D081_M59_DF, and J3D081_M61_DF Secure Smart Card Controller Rev. 2, 2013.

[24] Calypso, Calypso Host Card Emulation Application Version 1.2, Ref: 141113-CalypsoHCEApplication, Spirtech, 2016.

[25] Spirtech, «Secure Application Module SAM-C1,» 2018. [En línea]. Available: http://spirtech.com/docs/Products/SAM-C1/en/SamC1-v1.pdf.

[26] NXP, P5DF081 MIFARE SAM AV2 functional specification, document number 191732.

[27] Calypso, Security Architecture and Key Ceremony - 170202-KeyArchitecture-10, SNCF, 2018.

[28] CNA, «Calypso Networks Association - Membership,» 2018. [En línea]. Available: https://www.calypsonet-asso.org/content/membership.

[29] ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013.

[30] ABIresearch, «ABI Research Forecasts Global Contactless Ticketing Shipments to Top 460 Million in 2017,» Feb 2017. [En línea]. Available: https://goo.gl/igfGrx.

[31] ISO/IEC, ISO/IEC 7816-4 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013.

[32] Arjo Systems (HID Global), SOMA ATLAS - User Manual Calypso Specification Rev. 3.1 v. 1.2, 2016.

[33] ISO/IEC, ISO/IEC 9798-2 Information technology — Security — Part 2: Mechanisms using symmetric encipherment algorithms, 1999.

[34] Gemalto, «Gemalto Calypso G1,» 2018. [En línea]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/transport-celego-calypso.pdf.

[35] HID Global, «MIFARE DESFire EV1 Credentials,» 2010. [En línea]. Available: https://www.hidglobal.com/sites/default/files/resource_files/mifare-desfire-ev1-card-ds-en.pdf.

[36] Concejo del Municipio del DMQ, Ordenanza Metropolitana 0201 del 8 de febrero de 2018, Quito, 2018.

[37] Concejo del Municipio del DMQ, Ordenanza Metropolitana No. 54 del 2 de abril de 2015, Quito, 2015.

[38] ISO/IEC, ISO/IEC 7816-5- dentification cards -- Integrated circuit cards -- Part 5: Registration of application providers, 2004.

[39] BSI, BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements, 2005.

[40] BSI, BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists, 2005.

[41] ISO, ISO/DIS 8601-1: Data elements and interchange formats— Information interchange— Representation of dates and times—, 2016.

[42] Calypso, Secure Application Module SAM-C1: 101010-SamCalypso-16, Spirtech, 2018.

[43] BSI, BS EN 1545-1 Identification card systems. Surface transport applications. Elementary data types, general code lists and general data elements, 2005.

[44] BSI, BS EN 1545-2 Identification card systems. Surface transport applications. Transport and travel payment related data elements and code lists, 2005.

[45] ITU-T, Recomendación X.509.

[46] «W3C Recommendation: XML Signature Syntax and Processing (Second Edition),» 10 junio 2008. [En línea]. Available: http://www.w3.org/TR/xmldsig-core/.

[47] E. Barker y N. Mouha, SP 800-67 Rev. 2: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017.

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

[49] 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.

[50] 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.

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

[52] 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/.

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