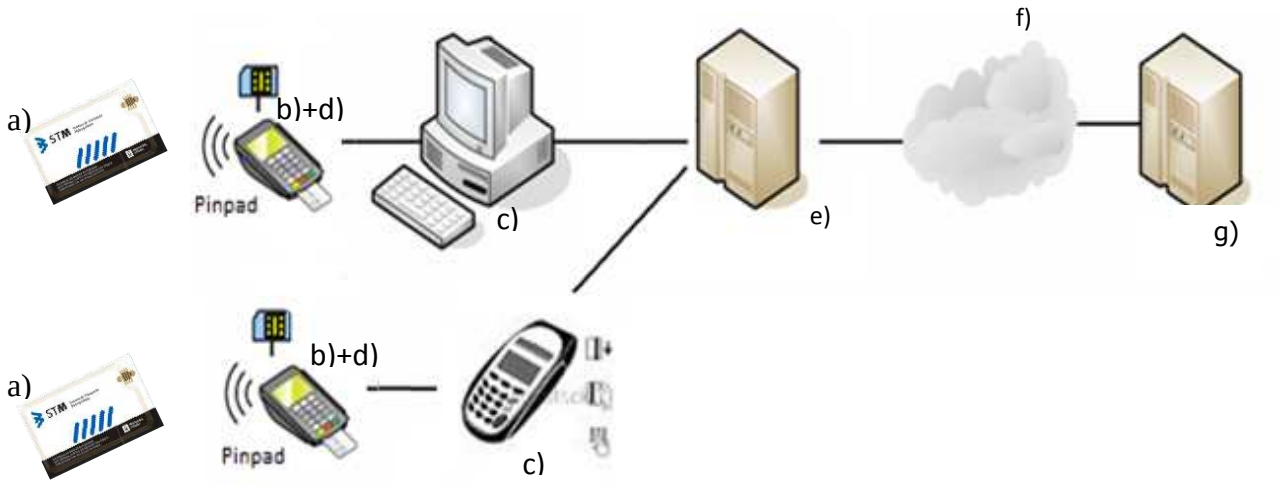
ANEXO TECNICO I

INFRAESTRUCTURA DEL CONTRATISTA

A) PARA LA MODALIDAD de RECARGA PRESENCIAL (PRE-PAGO)

La realización de la venta del crédito se realizará exclusivamente conectado en modalidad on-line con el sistema central del STM, para lo cual dicho sistema provee mecanismos de autorización de la venta mediante servicios web (en adelante Web Services), según la siguiente arquitectura:



A continuación se describen los principales subsistemas incluidos para cumplir con los objetivos propuestos.

a) **Tarjeta chip sin contacto – Tarjeta STM**

Es una tarjeta de chip sin contacto de tecnología Mifare, que contiene todos los datos necesarios para que el usuario pueda operar en el sistema.

b) **Dispositivo Seguro de Recarga STM (DSR_STM)**

Componente de hardware del adjudicatario y homologado por la IM donde corre el aplicativo del STM para las recargas de sus tarjetas. Cuenta con acceso a módulo SAM e interfaz contactless para lectura y escritura sobre tarjetas Mifare.

La tarjeta es accedida exclusivamente por medio del dispositivo DSR_STM, quien presentando las claves adecuadas, es capaz de leer y/o grabar la misma. Es obligatorio el uso de un dispositivo de recarga homologado a los efectos de la realización del servicio solicitado. El dispositivo será provisto por el oferente, debiendo cumplir con las características técnicas del ANEXO II.

c) **PC o POS y Software Cliente**

Es un equipo del oferente que ejecuta un Software Cliente perteneciente al mismo, realiza mediante la utilización del dispositivo b), e invocando a d) y conectado mediante e) a través de f) con los WebServices publicados en g)

d) **Aplicativo de dialogo STM**. Software escrito y compilado por la IM cuya responsabilidad es gestionar la escritura y lectura segura de tarjetas STM. Este software es escrito en ANSI C. Este software debe ser compilado por la Intendencia de Montevideo con el compilador correspondiente.

e) **Sistema Central del oferente** – Es el conjunto de servidores que gestionan y almacenan todos los servicios y datos del oferente.

El contratista deberá proveer una red de puestos de venta interconectados con dicho sistema central.

f) **Red de Enlace** - Enlace dedicado punto a punto entre la infraestructura central del adjudicatario y la de la IM para la transmisión de los datos mediante servicios de Capa 3. Para esta aplicación se deberá contar con redundancia del enlace y tener un ancho de banda en el enlace principal de al menos 512 kbps, el cual estará sujeto a las modificaciones por mejoras que surjan una vez puesta en marcha la aplicación.

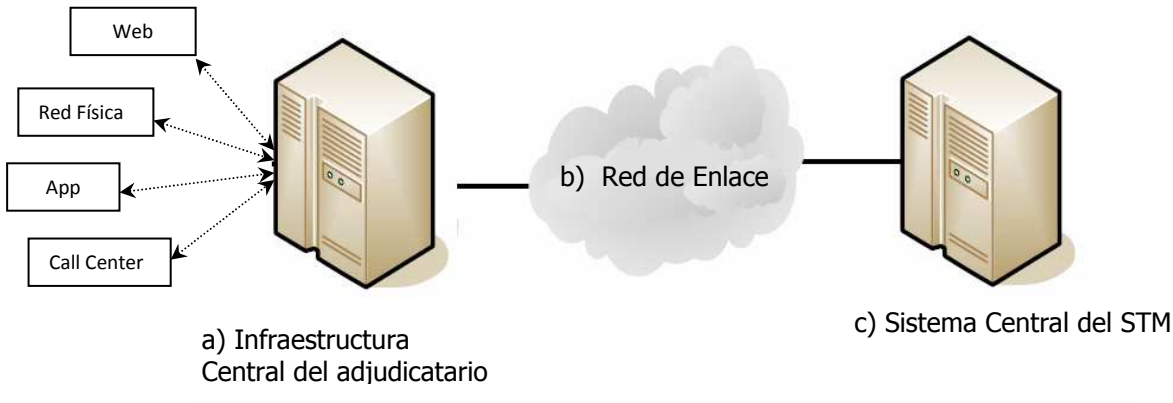
Aquí se requiere:

- Efectuar la Autenticación de todos los mensajes mediante el uso de certificados digitales, los cuales serán emitidos por la Autoridad Certificadora del STM (CA STM)
- Seguridad en la transmisión de los datos requeridos para la transacción, mediante el uso del protocolo SSL (Secure Socket Layer)

g) **Sistema Central STM** – Es el conjunto de servidores que gestionan y almacenan todos los servicios y datos del Sistema de Transporte Metropolitano.

B.i) PARA LA MODALIDAD de RECARGA DIFERIDA (Paso 1)

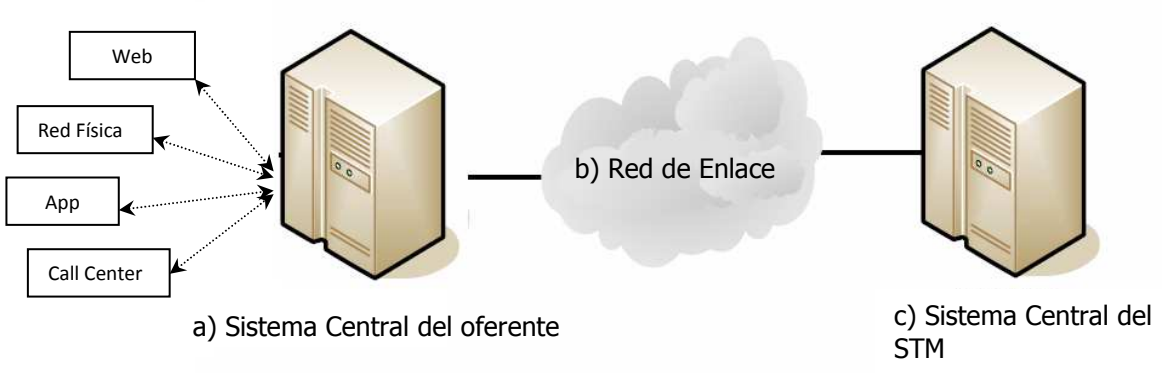
La realización de la venta del crédito se realizará exclusivamente conectado en modalidad on-line con el sistema central del STM, para lo cual dicho sistema provee mecanismos de autorización de la venta mediante Web Services, según la siguiente arquitectura:



B.ii) PARA LA MODALIDAD de RECARGA DIFERIDA (Paso 2)

La transferencia de los créditos previamente comprados se realizará exclusivamente conectado en modalidad on-line con el sistema central del STM, para lo cual dicho sistema provee mecanismos de autorización de la venta mediante Web Services, según la misma arquitectura detallada para la RECARGA PRESENCIAL.

C) MODALIDAD GARANTIA DEL CONSUMO (POST-PAGO)



a) Infraestructura Central del adjudicatario – Es el conjunto de componentes de comunicación y/o servidores que dan soporte a la operativa del adjudicatario.

b) Red de Enlace - Ya detallado en punto f) de A) Modalidad Recarga Presencial.

c) Sistema Central STM – Ya detallado en punto g) de A) Modalidad Recarga Presencial.

ANEXO II

Características Técnicas de los dispositivos DSR_STM

Las siguientes características requeridas constituyen un grupo de requerimientos necesario, pero no necesariamente suficiente, para que un dispositivo o sistema pueda ser considerado como Dispositivo Seguro de Recarga de Tarjetas STM (DSR_STM). No es suficiente debido a que el STM conjuntamente con el proveedor deberá poder homologar la idoneidad de los dispositivos presentados mediante el efectivo desarrollo de un conjunto de pruebas de software que validen dicha idoneidad. El STM podrá solicitar apoyo a organismos de contralor y certificación externos para asegurar la idoneidad, siendo de cargo del oferente los costos de dicha certificación.

- Compatibilidad: PCI PTS 3.0 o superior certificada.
- 1 zócalo SAM mínimo, preferiblemente 2, en zona apropiadamente segura no extraíble fácilmente (norma ISO 7816-2 y 7816-3).
- Antena para tarjetas tipo “contactless” ISO 14443 A tipo Mifare Clasic y Mifare Plus
- Disponibilidad de almacenamiento de al menos 3 claves de 16 bits en zona segura HSM (norma FIPS140-2 Level 3). Deberá contar con mecanismos antitampering, y certificación PCI PTS HSM 2.0 o superior. El proceso de almacenamiento de toda la información segura deberá ser realizado por una empresa que tenga certificación PCI PIN 2.0 o superior.
- SDK para trabajar en ANSI C. Deberá implementar codificación y decodificación Base64 y 3DES. ***El dispositivo deberá poder trabajar con algoritmos criptográficos de forma tal que la clave nunca abandone la zona segura***.

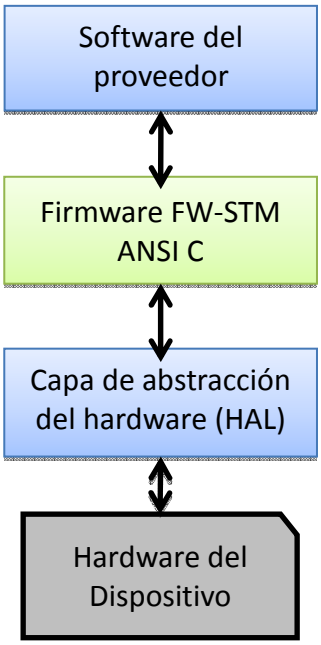
Kit de Desarrollo de Software

El dispositivo deberá contar con apropiadas herramientas de desarrollo (SDK) que permitan trabajar en lenguaje ANSI C y generar objetos y bibliotecas.

El proveedor deberá proporcionar además una capa de abstracción del hardware (HAL), la que expondrá el acceso a ciertas primitivas de uso de hardware, tales como:

- Obtener ID (identificación única) del dispositivo
- Verificar presencia de tarjeta RFID y SAM y obtener identificación única de cada uno
- Ejecutar comandos APDU (norma ISO 7816-4)
- Leer bloque de tarjeta Mifare
- Grabar bloque de tarjeta Mifare

- Manejar las opciones de hardware necesarias para los comandos anteriores (encender/apagar)
- Manejar indicadores LED y sonidos



El STM definirá junto con el proveedor el conjunto de dichas primitivas, teniendo a la vista las características del dispositivo. Las primitivas serán como mínimo las indicadas anteriormente. Esto no excluye la adición de otras primitivas, como podría ser cualquier otro control de hardware que el dispositivo pudiera tener.

Esta capa HAL se definirá por medio de archivos .h; la implementación de estas funciones y su correcto funcionamiento es responsabilidad del proveedor.

El STM cuenta con un firmware en ANSI C que contiene las rutinas que usarán las funciones HAL las cuales expondrán las funcionalidades de la ASTM que el proveedor podrá utilizar.

Además de las características siguientes, se deberá pasar por un proceso de homologación que consiste en la generación por parte del proveedor de un soft para pruebas, con acceso por conexión TCP a fin de verificar en forma atómica el correcto funcionamiento de cada una de las rutinas expuestas por el firmware del STM.

Consideraciones especiales

El STM podrá solicitar ejemplares de muestra de los dispositivos ofrecidos por los oferentes.

En dicho caso, el proveedor deberá aportar también y en forma conjunta a la muestra, todas las herramientas necesarias (SDK, licencias, equipos necesarios) a los efectos de poder realizar las pruebas que se requieran. Asimismo, el proveedor deberá disponer del personal idóneo necesario para que se pueda realizar la evaluación del producto.