UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CONTROL DE ACCESO A TRAVÉS DE UNA TARJETA (U)SIM

TESIS PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:
CABALLERO ROMERO PAUL

DIRECTOR DE TESIS:

M.I. AURELIO ADOLFO MILLÁN NÁJERA

CIUDAD UNIVERSITARIA, D.F., MÉXICO
MAYO 2014

Agradecimientos

A mi madre, por siempre confiar en mí y darme el aliento necesario para conseguir mis metas.

A mi padre, por todos sus sabios consejos, guía y apoyo incondicional.

A mis hermanos, por ser parte de mi vida, y compartir todos aquellos buenos momentos.

A mi esposa, por ser ese apoyo incondicional y estar siempre conmigo.

A mis amigos, por hacer mi vida más divertida.

A la universidad, por darme todas esas lecciones de vida y darme una formación académica de alto nivel.

A mi asesor de tesis por brindarme su valioso tiempo, asesoría y apoyo.

Prólogo

El presente trabajo tiene como objetivo describir el desarrollo de una tarjeta denominada inteligente, que cuente con alguna aplicación, la cual permita realizar el acceso a algún tipo de transporte público, realizar la compra de algún producto y a su vez ser capaz de realizar la recarga de fondos para la compra del producto.
A lo largo de este trabajo se justificará el uso de la tarjeta inteligente, en este caso en específico la tarjeta (U)SIM.

A continuación se da una breve descripción de los capítulos en los cuales está estructurada esta tesis:

Capítulo 1.- Marco teórico. Contiene los fundamentos teóricos necesarios para poder describir la tecnología GSM, UMTS, así como la descripción de lo que es el control de acceso. Se menciona los principales protocolos de comunicación inalámbrica. A su vez se describe cómo es que se lleva a cabo la actualización remota de una tarjeta (U)SIM.

Capítulo 2.- Análisis. En este apartado se describen las posibles soluciones y alcances de la tarjeta inteligente (U)SIM, así como posibles casos de uso futuros. También se define la forma de trabajo y su metodología de desarrollo.

Capítulo 3.- Diseño e implementación. En este capítulo se explica detalladamente el diseño e implementación de la tarjeta inteligente y su interacción con los sistemas, redes y equipos. De esta manera, se definen las características y funciones generales de la tarjeta inteligente (U)SIM mediante casos de uso. También se describe la manera en que se deben desarrollar las aplicaciones de una tarjeta inteligente (U)SIM, su sistema de archivos y la implementación del protocolo de comunicación inalámbrico.

Capítulo 4.- Pruebas e implantación. Se describe la metodología seguida para probar el correcto funcionamiento de la tarjeta (U)SIM y sus aplicaciones (mediante pruebas unitarias e integrales). Además se explica el proceso de homologación de la tarjeta para poder entrar en producción y que a su vez el operador de red pueda distribuir al usuario final.

Capítulo 5.- Resultados y conclusiones. Por último, se hace un resumen de las características y la funcionalidad de la tarjeta inteligente (U)SIM. Se exponen las conclusiones y los resultados.

Índice

1. Marco teórico.

1.1. Definición de tarjeta inteligente.

Es un dispositivo que contiene un microprocesador capaz de realizar cálculos matemáticos, almacenar y procesar información. Es usada principalmente en los campos de la telefonía móvil y el sistema bancario. En este capítulo se describirán los componentes de las tarjetas de telefonía móvil.

La tarjeta inteligente contiene los siguientes componentes:

CPU
Unidad de proceso central

ROM (No volátil)
Memoria de sólo lectura. Este tipo de memoria es usada para la "hardmask", la cual contiene el sistema operativo, la máquina virtual de Java® y el API de la tarjeta.

EEPROM (No Volátil)
Memoria de sólo lectura programable y de acceso aleatorio que puede ser borrada. Este tipo de memoria es usada por la "softmasks" o "filtros" y son extensiones para el correcto funcionamiento de los componentes de la memoria ROM. Se puede hacer la analogía con el funcionamiento de un disco duro de una computadora. Este tipo de memoria contiene los archivos GSM y algunas aplicaciones.

RAM (Volátil)
Memoria de lectura-escritura semiconductora de acceso aleatorio. Este tipo de memoria se utiliza principalmente para guardar datos utilizados en una sesión, es decir, mientras está encendida la (U)SIM, (datos de localización, por ejemplo) que serán utilizados por las aplicaciones de la tarjeta (U)SIM.

En la figura 1 se representan los elementos principales de la tarjeta (U)SIM:

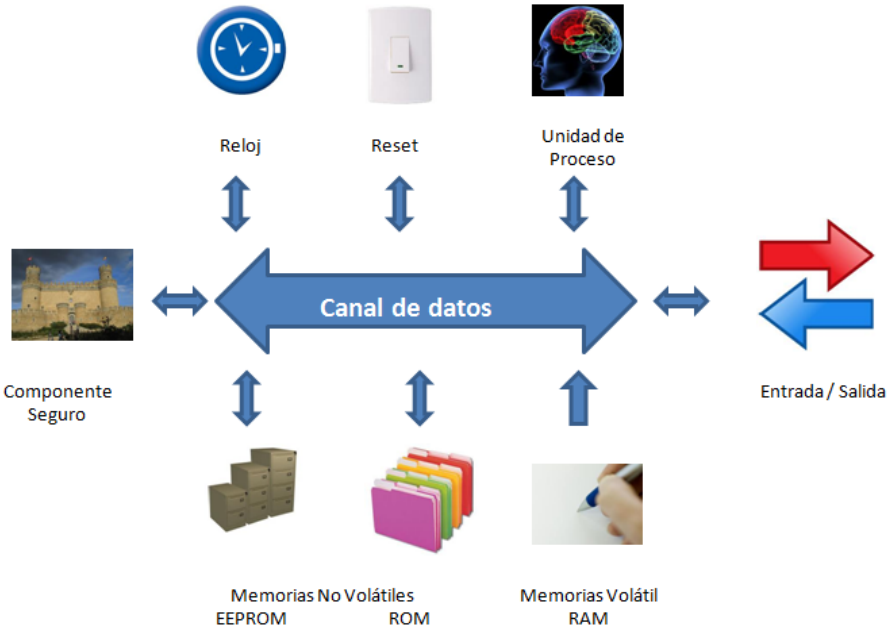


Figura 1. Principales componentes de la tarjeta (U)SIM.

1.2. El Sistema GSM.

La tarjeta inteligente usada en los teléfonos móviles, es llamada "Suscriber Identity Module" (SIM) fue y continúa siendo la pionera en términos de funcionalidad y capacidad de memoria. Esto es en parte debido al uso de las mismas en los teléfonos móviles, con lo cual los costos de manufactura han disminuido en comparación con otro tipo de tarjetas inteligentes, como las tarjetas de pagos electrónicos o aplicaciones médicas.

GSM fue lanzado comercialmente en 1992, se convirtió en el estándar de sistemas de comunicaciones móviles en pocos años. Esto no sólo incluye la transmisión de voz, sino que también la transmisión de datos, principalmente la de envío de la mensajería corta (SMS Send Short Message).

A mediados de 2001, había un total de 400 operadores que adoptaron dicho estándar en 171 países, con más de 565 millones de suscriptores.

La especificación GSM comenzó en 1982 auspiciado por la Conférence Européenne des Postes et Telécommunications (CEPT). El objetivo era generar especificaciones para una red de telecomunicaciones transnacional e interoperable. En el transcurso del tiempo, estos esfuerzos permitieron elaborar un borrador con las especificaciones para

transmisión e interoperabilidad y un ISDN-compatible de un sistema digital de telefonía celular operando en la banda de los 900-MHz. El Groupe Spécial Mobile fue fundado para este propósito, el cual fue llamado GSM. En 1986, la sede de GSM fue establecida en París, a fin de coordinar la generación de especificaciones.

Más tarde también fueron responsables de especificar una gran variedad de pruebas para los componentes del sistema. Desde una perspectiva técnica, fue interesante revisar el número de tecnologías que fueron adoptadas por GSM al tiempo que algunas eran totalmente nuevas y no habían sido probadas. Por ejemplo, la interface aérea usando una combinación de acceso múltiple por división del tiempo con el acceso múltiple por división de frecuencia y la transmisión digital de datos era un territorio totalmente inexplorado para las aplicaciones de las comunicaciones móviles. Estas decisiones llevaron a muchos problemas técnicos, particularmente en la fase de desarrollo, pero actualmente se ve como una decisión afortunada, desde que GSM probó ser un sistema innovador.

La Asociación GSM es un organismo internacional, el cual tiene sus oficinas en Dublín y Londres, para la coordinación de los sistemas de telecomunicaciones. Éste fue fundado en Copenhage en 1987, y es el responsable de los desarrollos y aplicación de los estándares GSM. Representa a más de 500 operadores y proveedores en la industria GSM. En 1989, las especificaciones desarrolladas por varios grupos de trabajo bajo el mando de la sede GSM fueron incorporados en el nuevo instituto fundado el European Telecommunication Standards Institute (ETSI).

En 1990, todas las especificaciones de la fase 1 fueron completadas en un formato aceptable.

En 1998, el Suscriber Identity Module Expert Group(SIMEG) comenzó a trabajar con la especificación de la tarjeta inteligente GSM, la cual es llamada “Suscriber Identity Module” (SIM).

Este grupo fue conformado por representantes de fabricantes de tarjetas, fabricantes de teléfonos y operadores de red. Trabajando bajo la licencia del ETSI, el SIMEG generó las especificaciones para la interface entre la tarjeta inteligente y el teléfono móvil. La especificación obtuvo el nombre de GSM 11.11. En 1994, el SIMEG fue transformado en un nuevo grupo llamado Special Mobile Group 9 (SMG9). El SMG9 llevó el mando de los desarrollos futuros y la revisión de todas las especificaciones de la SIM hasta el año 2000. En el 2000, el SMG9 fue disuelto, y sus responsabilidades fueron divididas en 2 nuevos grupos de expertos. La ETSI Projet Smart Car Platform (EP SCP) es el grupo experto encargado de todos los problemas genéricos en el área de las tarjetas inteligentes, mientras que la 3GPP es el grupo experto relacionado con la interface de aplicación entre un teléfono móvil y la SIM o (U)SIM.

La primera red GSM operando fue mostrada en la Feria de Telecomunicaciones de Génova en 1991. Durante la feria, aproximadamente 11,000 llamadas fueron enrutadas sin

problema alguno. En 1992, el primer sistema GSM fue puesto en servicio regularmente en diversos países de Europa como Dinamarca, Finlandia, Francia, Alemania, Italia, Portugal y Suecia. Al mismo tiempo, había aproximadamente 250,000 suscriptores. También en ese año, el primer "acuerdo de roaming" entre 2 operadores de red fue firmado, y el primer operador de red no Europeo firmo el MoU, lo cual significo la decisión oficial de usar el sistema GSM. Sólo un año después al final del año 1993, el millón de suscriptores fueron dados de alta. En ese año, la primera red GSM1800 comenzó operaciones en la Gran Bretaña. En 1995, la primer red GSM1900 entró en operación en USA, y al final de julio de 1998, los 100 millones de suscriptores GSM fueron dados de alta. A mediados de 2001, había 500 millones de suscriptores en todo el mundo.

1.2.1. Especificaciones.

Un gran número de especificaciones interrelacionadas e interdependientes fueron necesarias para describir totalmente el sistema GSM en términos técnicos. En total, hay aproximadamente 130 especificaciones individuales, con un total de más de 6000 páginas. Para los sistemas GSM los términos "especificación" o "estándar" son usados frecuentemente e indistintamente.

Desde que fueron publicados por la ETSI, los documentos de especificaciones obtuvieron formalmente el estado de estándares. Sin embargo, sus descripciones técnicas son muy estrictas y prácticamente todas las implementaciones están basadas en compatibilidad mutua, lo cual es una característica típica de la especificación. Por esta razón, nos podemos referir al esquema GSM(GSM 11.11), el cual es usado mayoritariamente en los círculos técnicos, el lugar de su correspondiente estándar ETSI(TS 100977), que son idénticos en contenido.

El desarrollo de un sistema GSM ha sido concretado a través de fases. El servicio básico (transmisión de voz, desvío de llamadas, roaming y servicio de SMS) fueron implementados en la fase 1, la cual comenzó en 1992. En la fase 2, la cual comenzó en 1996, servicios suplementarios fueron adicionados, incluyendo conferencias, transferencia de llamadas, y GSM en la frecuencia de los 1800MHz. Esto fue seguido por la Fase 2+, en la cual estos servicios fueron incrementados con las funcionalidades del SIM Application Toolkit, HSCSD y GPRS (además de algunos otros).

Como es usual con las especificaciones, las especificaciones GSM emplean sus propios términos técnicos. Estos términos están precisamente definidos en términos técnicos en varias listas de abreviaturas y glosarios, y son solamente aplicables en el campo GSM. Un resumen es provisto por GSM 1.04 ("abreviaciones y acrónimos"). Debido a este vocabulario técnico, es relativamente difícil para alguien nuevo familiarizarse con GSM, por lo tanto es necesario consultar las explicaciones de las abreviaturas en los contextos adecuados para estudiar las especificaciones.

La especificación que forma las bases del modelo de seguridad GSM en la telefonía móvil se denomina GSM02.17 (“características de la funcionalidad de la SIM”). La especificación más importante de la tarjeta inteligente es el documento GSM 11.11 (“especificación de la interface SIM-Equipo Móvil (SIM-ME)).

La especificación GSM 11.14 (“especificación del kit de herramientas de la SIM al equipo móvil), la cual describe una plataforma segura para los servicios suplementarios de la SIM. Ésta hace referencia a SAT (SIM Application Toolkit), fue publicada en 1996. GSM 11.14 describe a detalle algunas funciones como el manejo de un display, envío de mensaje (SMS) y algunas otras funciones relacionadas a funciones de valor agregado que pueden ser implementadas en la SIM.
La especificación GSM 03.48 establece el mecanismo usado para la transmisión de datos vía aérea (OTA Over The Air). Establece a su vez el mecanismo de administración de archivos RFM (Remote File Management) y aplicaciones RAM (Remote Applet Management).

1.2.2. Arquitectura del Sistema GSM y sus componentes.

Cada red GSM puede ser dividida en 3 subsistemas, los cuales son descritos en términos generales en la especificación GSM 01.02 (“descripción general de una red GSM Pública). Estos tres subsistemas son el subsistema de radio (RSS Radio Subsystem), la Red y el subsistema de switcheo (NSS Network and Switching Subsystem) y el subsistema de operación (OSS Operating Subsystem)
El subsistema de radio está compuesto de los teléfonos móviles, el cual es llamado estación móvil (MS Mobile Station), y un subsistema de estación base (BSS Base Station Subsystem). La estación móvil consta de dos componentes separados, la parte física y la parte lógica, los cuales son llamados equipo móvil (ME Mobile Equipment) y el módulo de identidad del suscriptor (SIM Suscriber Identity Module).

El subsistema de estación base está formado por las estaciones base localizadas en el centro de cada celda. Las funciones de una estación base son establecer contacto con los teléfonos móviles a través de una interface aérea y proporcionar datos a los componentes de alto nivel de la red. Una estación base consiste de una o más estaciones de transmisión/recepción de base (BST Base Transceiver Station) y un controlador de estación base (Base Station Controller BSC). Para la estación de transmisión/recepción de base, típicamente su módulo de recepción tiene ocho canales de 200-kHz, así que teóricamente puede tener ocho canales activos hacia las estaciones móviles. En la práctica sólo siete canales son usados, debido a que un canal es usualmente reservado para comunicaciones administrativas.

Uno, tres o seis módulos transmisores/receptores son usualmente suficientes en una estación base de transmisión/recepción. Una o más estaciones base de

transmisión/recepción están en siendo manejadas por una estación base de control. Una configuración típica consiste en tres estaciones base de transmisión/recepción a 120 grados con respecto a la otra, todas conectadas con la estación base de control. Si una estación móvil se mueve de una región de envío/recepción a una estación base de transmisión/recepción dentro de otra estación base de transmisión/recepción y ambas estaciones de transmisión/recepción están asignadas a la misma estación base de control, la estación base de control puede iniciar independientemente la transferencia después de la señalización de la cual es responsable el centro de switcheo móvil. La transmisión de datos vía interface aérea es cifrada y tiene una taza de transmisión de 13 kbits/s en el modo de transmisión full.

La red y el subsistema de switcheo esencialmente consisten de un centro de switcheo móvil y un registro de localización de visitantes (VLR Visitor Location Register). Un centro de switcheo móvil (MSC) administra múltiples subsistemas de estación de base. Esto forma el enlace entre los subsistemas de estación de base conectados a éste, u a otros centros de switcheo móvil y también redes de telefonía pública. El centro de switcheo móvil es el responsable de configurar, administrar y terminar las conexiones, realizar los cargos de las llamadas y supervisar servicios suplementarios, como el desvío y bloqueo de llamadas y las conferencias. El registro de localización de visitantes (VLR) contiene información acerca de todas las estaciones móviles que están en el rango del centro de switcheo móvil. El VLR también guarda la lista de estaciones móviles que pertenecen a suscriptores de otras redes y se han autenticado en la red del centro de switcheo móvil vía roaming.

El sistema GSM de más alto nivel jerárquico es el subsistema de operación. Éste consiste del centro de operación y el mantenimiento (OMC Operation and Maintenance System), el centro de autenticación (Authentication Center AuC), el registro de localización local (Home Local Register HLR) y el registro de identidad del equipo (Equipment Identity Register EIR). El centro de operación y mantenimiento es el responsable de la operación regular de la red, la administración de los suscriptores y la facturación de las llamadas. El centro de autenticación (AuC) es el componente seguro del lado de la red y de alguna manera es el que habla con su contraparte que es la SIM del lado del equipo móvil. Éste genera y administra todas las llaves y algoritmos necesarios para la operación del sistema, especialmente para la autenticación de las estaciones móviles (por ejemplo la SIM). Otro componente central es el registro de localización local (HLR), el cual contiene todos los datos de los suscriptores, así como los datos de su localización para cada estación móvil. El registro de identidad del equipo (EIR Equipment Identity Register) es el complemento del HLR para estaciones móviles. Éste contiene datos esenciales, tales como los números seriales de todas las estaciones móviles representadas en la red.

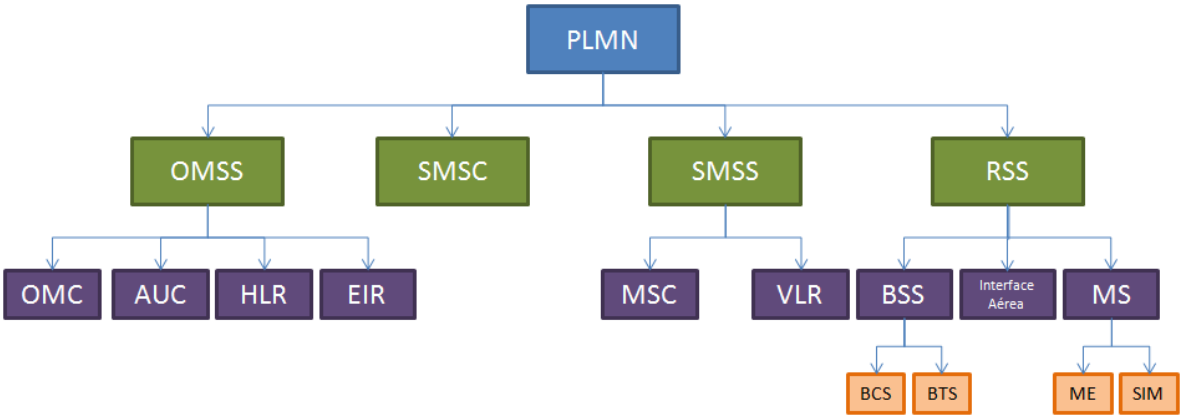


Figura 2. Arquitectura básica del Sistema GSM.

En la figura 2 se muestra la arquitectura básica de un sistema de telecomunicaciones móviles acorde al estándar GSM 01.02. En este ejemplo las bases de datos EIR y HLR están centralizadas. Debido a que muchas características de la configuración PLMN son decididas por los operadores, estas bases de datos podrían estar descentralizadas y distribuidas en algunos MSCs si fuera necesario (por ejemplo debido al alto tráfico de red).

1.3. El Sistema UMTS.

UMTS significa sistema universal de telecomunicaciones móviles (Universal Mobile Telecommunications System), estandarizado por 3GPP, es la tecnología de tercera generación sucesora a GSM y GPRS.

UMTS provee y refuerza el rango de servicios multimedia. Éste ha evolucionado desde su formato básico a través de los desarrollos de HSDPA (High Speed Downlink Packet Access) y HSUPA (High Speed Uplink Packet Access) para proveer una gran capacidad de ancho de banda para soportar los servicios de nueva generación.

El objetivo es ofrecer una banda ancha con una velocidad de acceso de 2Mbps.

La velocidad de transferencia es de 2000kbps

El radio de acceso a redes 3G se hace a través de CDMA (Code Division Multiple Access), en donde:

- Un código único es asignado a cada usuario
- La llamada es bloqueada por este código, nadie más lo puede abrir.
- Todos los usuarios están en la misma banda de frecuencia.
- Este código permite separar a los usuarios.

1.4. Diferencias entre GSM y UMTS.

Mientras que en GSM se utiliza la tecnología de acceso múltiple por división de tiempo (TDMA Time Division Multiple Access) en UMTS se utiliza CDMA (acceso múltiple por división de código). Así pues:

- Un código único es asignado a cada usuario
- La llamada está bloqueada por este código y nadie más puede usar el canal.
- Todos los usuarios están en la misma banda de frecuencias (este código permite separar usuarios)

Además de lo anterior, una tarjeta SIM únicamente puede contener la aplicación SIM, como se muestra en la figura 3.

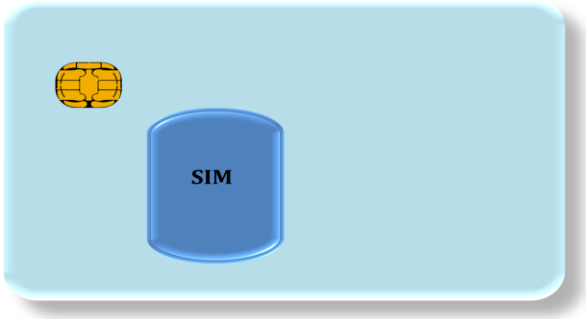


Figura 3. Arquitectura de las aplicaciones de una tarjeta SIM.

Mientras que una tarjeta (U)SIM, puede contener además de las aplicaciones SIM y (U)SIM, otro tipo de aplicaciones como aplicaciones de pagos móviles, control de acceso, aplicaciones de seguridad como PKI, etc. En la figura 4 se muestra un diagrama con la arquitectura de la tarjeta (U)SIM.

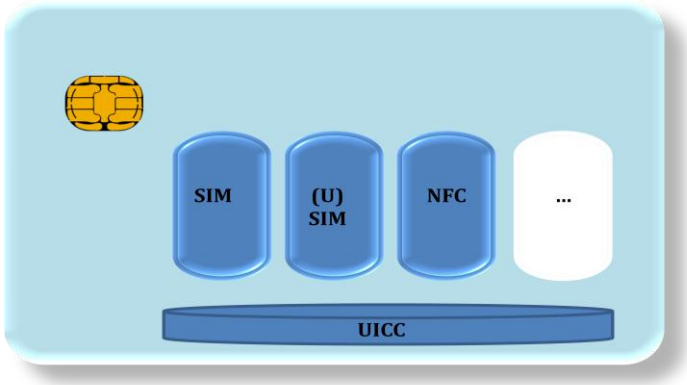


Figura 4. Arquitectura de las aplicaciones de una tarjeta (U)SIM.

La plataforma que permite tener más aplicaciones dentro de una misma tarjeta, es UICC (Universal Integrated Circuit Card).

Otra característica distinta entre GSM y UMTS es la inclusión de la autenticación 3G, basada en el algoritmo Milenage que se describirá en seguida.

1.5. Autenticación 3G.

La autenticación 3G ofrece grandes ventajas con respecto a la autenticación 2G. Entre otras destacan las siguientes:

1. Autenticación mutua (red a (U)SIM y (U)SIM a red)
2. Cálculo de la llave de integridad
3. Cálculo de la llave de confidencialidad.

Dicha autenticación establece algunos de los principios básicos de la seguridad de la información:

- Confidencialidad, pues se establece un canal cifrado con la llave de confidencialidad, la cual cifra la comunicación del suscriptor.
- Autenticidad, al tener cada usuario su propia identidad dada por el IMSI, y su llave de registro a red KI.
- Control de acceso, este enfoque se basa en que el operador se asegura de que existe uno y sólo un usuario que se autenticar en su red. Pues además de las llaves propias de cada tarjeta se tiene un número de secuencia, el cual de no coincidir con el del operador, la suscripción no tiene acceso a la red.

1.5.1. Autenticación mutua (red a (U)SIM y (U)SIM a red).

Este tipo de autenticación se basa en un requerimiento de autenticación y una respuesta de autenticación. En el requerimiento de autenticación el equipo móvil envía el TMSI (IMSI temporal) y/o el IMSI. IMSI es la identidad del suscriptor a nivel internacional. Mientras que en la respuesta de autenticación la red responde con un token de autenticación y un número aleatorio.

La respuesta de autenticación de la red a la (U)SIM contiene los siguientes elementos:

1. AUTN. Token de autenticación. Tiene una longitud de 16 bytes. A continuación se detallan sus componentes.
2. RAND. Número aleatorio. Es un número enviado por la red para autenticar a la (U)SIM, de 16 bytes de longitud y generado con una función aleatoria.
3. KI. Llave secreta. Llave previamente acordada o compartida entre la tarjeta y la red. Su tamaño es de 16 bytes de longitud.

El token de autenticación es verificado por la tarjeta (U)SIM, pues es la respuesta de autenticación enviada de la red a la (U)SIM. Se constituye de los siguientes elementos:

1. *Número de secuencia cifrado con la llave anónima* (SQN $\oplus$ AK de 6 bytes de longitud) Para prevenir ataques de réplica (diferente para cada autenticación). Una lista de SQN es almacenada en la (U)SIM. La llave anónima (AK) es calculada con la llave secreta y el número aleatorio en base a una función f5. Más adelante se detalla la función f5.
2. *AMF* (Authentication Management Field de 2 bytes de longitud). No estandarizado. Podría ser usado para indicar el algoritmo y la llave usada para autenticación.
3. *MAC-A* (Código de autenticación del mensaje 6 bytes de longitud). Sera usado por la (U)SIM para autenticar la red (prueba que la red conoce la llave secreta (Ki))

Autenticación a la red

La tarjeta (U)SIM corre dos verificaciones distintas:

a. Verificador de autenticación. Para autenticar a la red (prueba que la red conozca la llave secreta)
b. Verificador de sincronización. Verifica que no se repita el AUTN para prevenir ataques de réplica.

Verificador de autenticación

La autenticación de la red se hace de la siguiente manera:

- La (U)SIM calcula una AK. Esto lo hace a partir de un número aleatorio (RAND) y la Ki, que son procesados por una función f5.
- La (U)SIM descifra el SQN. Con la llave AK anteriormente calculada haciendo un XOR ($\oplus$)con el SQN (AK $\oplus$ SQN) que fue enviado, se descifra el valor de SQN
- La (U)SIM calcula la MAC-A. Dicho cálculo se hace a partir del SQN, Ki, AMF y RAND. Éstos se generan a partir de una función f1.
- La (U)SIM autentica finalmente a la red haciendo una comparación entre la MAC-A que calculó y la MAC que recibió en la respuesta de autenticación.

En la figura 5 se muestra el diagrama de los vectores de autenticación.

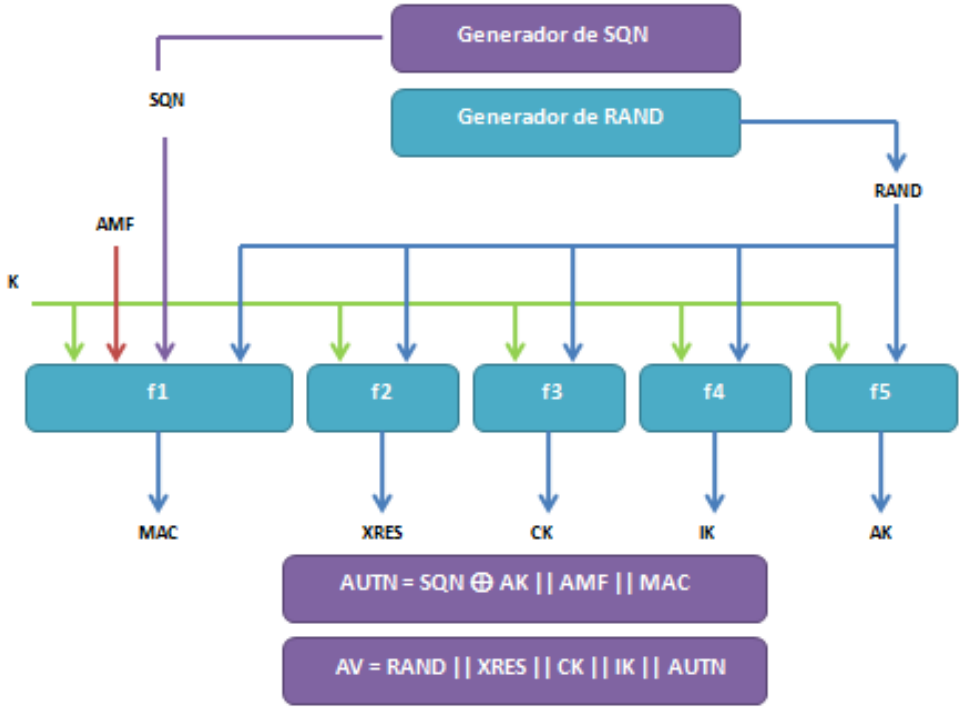


Figura 5. Diagrama de los vectores de autenticación

Verificador de sincronización

Para cada autenticación la red envía un SQN (Sequence Number) incremental a la tarjeta. La tarjeta aplica dos verificaciones antes de aceptar el valor del SQN:

1. Verifica que la SEQ pertenezca al rango de valores delimitados por α y β

2. El SEQ enviado por la red no haya sido recibido antes.

Una vez que se ha realizado un proceso de autenticación de manera exitosa, la (U)SIM y la red compartirán 2 llaves (llave de integridad y llave de cifrado).

Si la sincronización falla, se genera una MAC-S, con los datos de secuencia e índice (SEQ, IND) de la última sincronización valida, la llave secreta Ki, el AMF en ceros y el número aleatorio enviados en la respuesta de autenticación. Estos datos pasan a través de una función f1.

La tarjeta enviará el SQN MS (cifrado) almacenado en el archivo EFSQN a la red. La red podrá re-sincronizar su base de datos y podrá continuar con la autenticación.

NOTAS:

Las funciones para la protección de la confidencialidad e integridad están estandarizadas en el estándar T35.201 y están basadas en el algoritmo “Kasumi”. Dichas funciones son f8 y f9.

Las funciones de seguridad AKA (de acuerdo previo de la llave previa de autenticación), no están estandarizadas pero deben cumplir una serie de requerimientos estandarizados por el estándar TS 33.105. Los estándares 3G proponen el algoritmo Milenage definido en TS35.206 basado en AES. Puede ser customizado por el operador. En este estándar están definidas las funciones f1, f2, f3, f4 y f5.

En la figura 6 se puede observar en resumen la autenticación 3G.

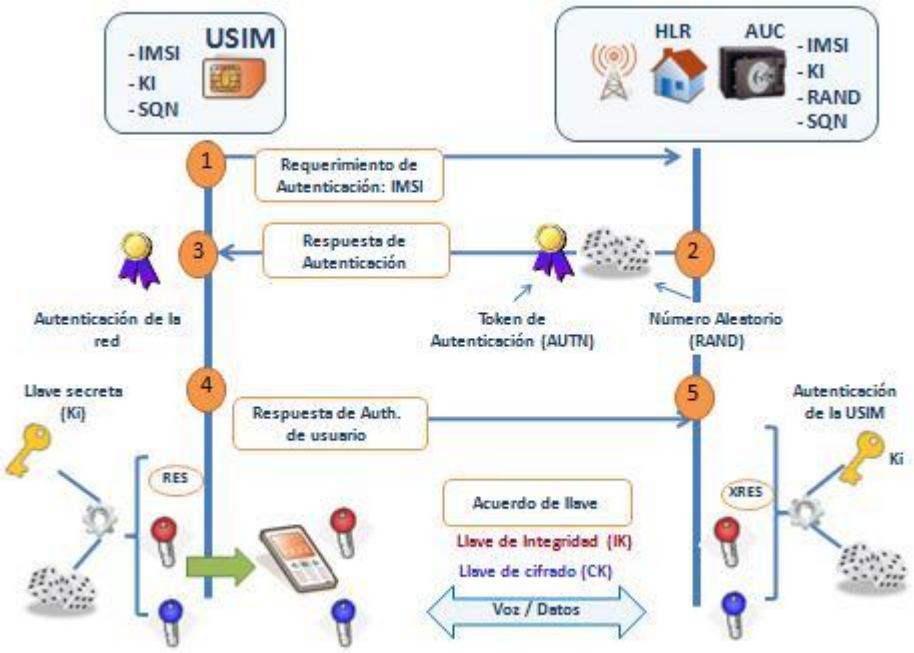


Figura 6. Proceso de autenticación 3G.

1.5.2. Cálculo de la llave de integridad.

La llave de integridad (IK).
Dicha llave se genera a partir de un número aleatorio, la llave secreta Ki a través de una función f4. Más adelante se detalla la función f4. Esta llave será usada para correr una protección en la integridad de la señal de datos.

1.5.3. Cálculo de la llave de cifrado.

La llave de integridad (CK).
Dicha llave se genera a partir de un número aleatorio, la llave secreta Ki a través de una función f3. Más adelante se detalla la función f3. Esta llave será usada para realizar el cifrado de la comunicación de voz y datos.

1.5.4. Algoritmo Milenage.

En el momento en que la (U)SIM conoce la K, RAND, SQN y AMF, ésta puede realizar el algoritmo Milenage y calcular MAC-A, MAC-s, AK, RES, CK e IK. En la figura 7 se muestra un breve resumen del algoritmo Milenage.

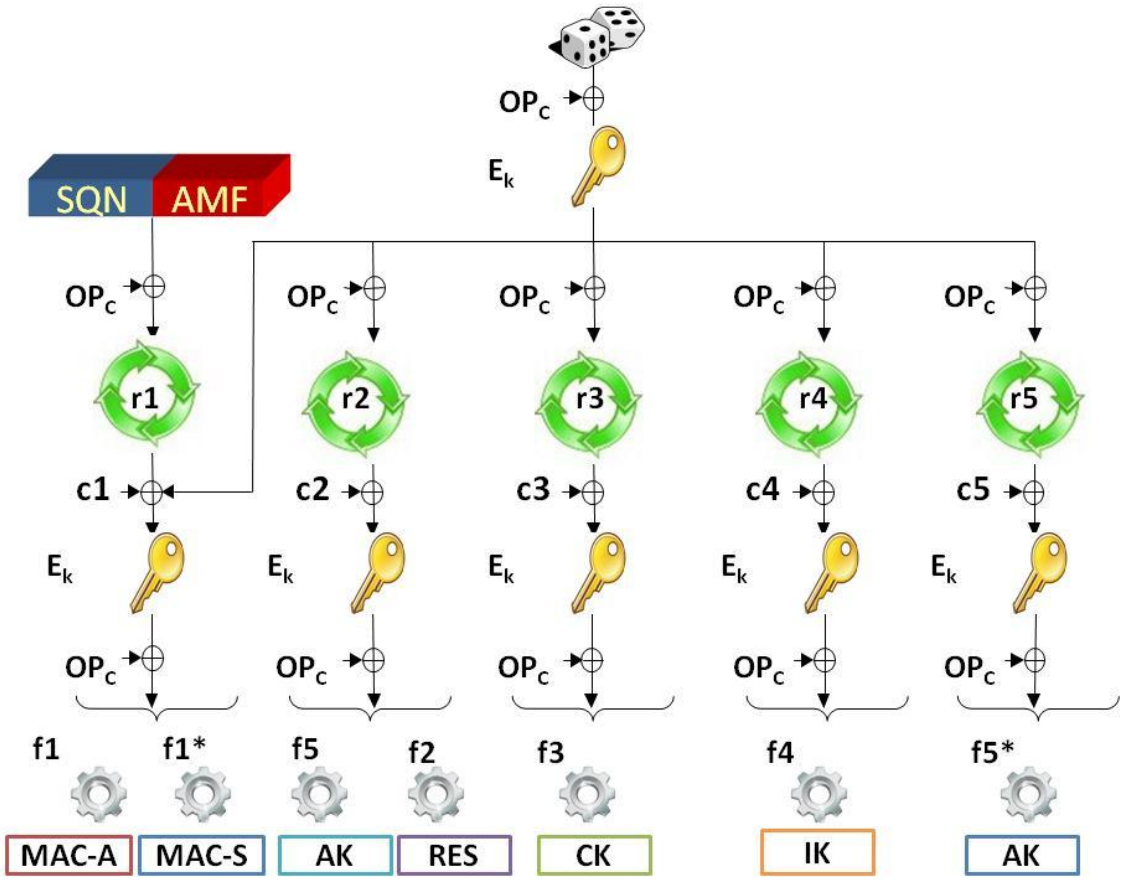


Figura7. Resumen del algoritmo Milenage.

Este algoritmo está basado en el cálculo de las funciones f1, f1*, f2, f3, f4 y f5. Estas funciones serán descritas más adelante.

Diversificación OPC

Se recomienda que esta llave se diversifique fuera de la (U)SIM. La diversificación se hace a partir de una llave OP definida por un operador. Esta recomendación se hace para evitar que la tarjeta (U)SIM almacene la OP, con la cual podrían calcularse las llaves OPC de cualquier otra tarjeta.

Constantes c y r

Es obligatorio que las variables c y r sean diferentes. Se recomienda que c1 tenga paridad par y c2 hasta c5 tengan paridad impar.

Si un operador quiere generar su propio algoritmo puede hacerlo, simplemente debe considerar que los valores de c1-c5 y r1-r5 deben ser distintos. Si se hace de esta manera, los pares (ci, ri) deben ser todos diferentes. Esto tampoco aplica para ci=cj y ri=rj para $i \neq j$. Por ejemplo, no debe existir el caso en que c2=c4 y r2=r4. Adicionalmente se recomienda lo siguiente:

c1 debe tener paridad impar

De c2 a c5 deben tener paridad par.

Estas recomendaciones están establecidas en el estándar ETSI TS135.206.

Funciones f1 f1,f2, f3, f4, f5*

El mecanismo de autenticación y acuerdo de llave requieren de las siguientes funciones:

f0 que genera el número aleatorio.
f1 usada para la autenticación de la red.
f1* re-sincronización del mensaje.
f2 usada para la autenticación del usuario.
f3 para la obtención de la llave de cifrado.
f4 usada para la obtención de la llave de integridad.
f5 obtención de la llave anónima.
f5* para la obtención de la llave anónima para el mensaje de re-sincronización.

Para las funciones f1 a f5* hay un requerimiento que debe cumplirse el cual consiste en que debe ser computacionalmente inviable obtener la llave secreta Ki a partir de las

entradas o salidas. Es por esto que las funciones se apoyan en el algoritmo Rijndael. Ver sección 1.5.4.1 para más detalle del algoritmo Rijndael.

$E[x]_k$ es el resultado de aplicar el cifrado Rijndael a un bloque para la entrada x de 128 bits usando la llave k de 128 bits.

Las entradas de los algoritmos se muestran en las tablas 1 y 2. Mientras que las salidas correspondientes se pueden revisar en las tablas 3, 4, 5, 6, 7, 8 y 9.

Parámetro	Tamaño (bits)	Descripción
KI	128	Llave secreta del suscriptor
RAND	128	Número aleatorio
SQN	48	Número secuencial
AMF	**16**	**Campo administrativo de autenticación (Authentication Management Field)**

Tabla 1. Entradas para las funciones f1 y f1.*

Parámetro	Tamaño (bits)	Descripción
KI	128	**Llave secreta del suscriptor**
RAND	**128**	**Número aleatorio**

Tabla 2. Entradas para las funciones f2, f3, f4, f5 y f5.*

Parámetro	Tamaño (bits)	Descripción
MAC-A	**64**	**Código de autenticación de red**

Tabla 3. Salida para la función f1.

Parámetro	Tamaño (bits)	Descripción
MAC-S	**64**	**Código de resincronización para la autenticación**

Tabla 4. Salida para la función f1.*

Parámetro	Tamaño (bits)	Descripción
RES	64	Respuesta

Tabla 5. Salida para la función f2.

Parámetro	Tamaño (bits)	Descripción
CK	128	Llave confidencial

Tabla 6. Salida para la función f3.

Parámetro	Tamaño (bits)	Descripción
IK	128	Llave de integridad

Tabla 7. Salida para la función f4.

Parámetro	Tamaño (bits)	Descripción
AK	48	Llave anónima

Tabla 8. Salida para la función f5.

Parámetro	Tamaño (bits)	Descripción
AK	48	Llave anónima de re-sincronización.

Tabla 9. Salida para la función f5.*

Las salidas son calculadas de la siguiente manera:

OUT1 = E[**TEMP** ⊕ rot(**IN1** ⊕ **OP**C, **r1**) ⊕ **c1**]K ⊕ **OP**C

OUT2 = E[rot(**TEMP** ⊕ **OP**C, **r2**) ⊕ **c2**]K ⊕ **OP**C

OUT3 = E[rot(**TEMP** ⊕**OP**C, **r3**) ⊕ **c3**]K ⊕ **OP**C

OUT4 = E[rot(**TEMP** ⊕ **OP**C, **r4**) ⊕ **c4**]K ⊕ **OP**C

OUT5 = E[rot(**TEMP** ⊕ **OP**C, **r5**) ⊕ **c5**]K ⊕ **OP**C

Las salidas correspondientes a cada una de las funciones son:

Salida ***f1*** = MAC-A, donde MAC-A[0] .. MAC-A[63] = **OUT1**[0] .. **OUT1**[63]
Salida ***f1**** = MAC-S, donde MAC-S[0] .. MAC-S[63] = **OUT1**[64] .. **OUT1**[127]
Salida ***f2*** = RES, donde RES[0] .. RES[63] = **OUT2**[64] .. **OUT2**[127]
Salida ***f3*** = CK, donde CK[0] .. CK[127] = **OUT3**[0] .. **OUT3**[127]
Salida ***f4*** = IK, donde IK[0] .. IK[127] = **OUT4**[0] .. **OUT4**[127]
Salida ***f5*** = AK, donde AK[0] .. AK[47] = **OUT2**[0] .. **OUT2**[47]
Salida ***f5**** = AK, donde AK[0] .. AK[47] = **OUT5**[0] .. **OUT5**[47]

1.5.4.1. Algoritmo Rijndael .

Rijndael está compuesto de una serie de rondas que transforman la entrada en la salida. Un resultado intermedio es llamado “estado”.

En la tabla 10 se representa el “estado”, mismo que puede ser visto como un arreglo de 4x4 bytes (128 bits en total).

$a_{0,0}$	**$a_{0,1}$**	**$a_{0,2}$**	**$a_{0,3}$**
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

Tabla 10. Representación de un “estado”.

En la tabla 11 se representa la llave cifrada, misma que también puede ser vista como un arreglo de 4x4 bytes (128 bits en total).

$k_{0,0}$	**$k_{0,1}$**	**$k_{0,2}$**	**$k_{0,3}$**
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Tabla 11. Representación de la llave cifrada.

Rijndael toma como entrada los bytes de texto plano P_0, P_1, … , P_{15} y bytes de la llave K_0, K_1, … , K_{15} y entrega como salida bytes de texto cifrado C_0, C_1, … , C_{15}. Los bytes de texto plano son mapeados en bytes de estado de la siguiente manera $a_{0,0}$, $a_{1,0}$, $a_{2,0}$,, $a_{3,0}$, $a_{1,0}$, $a_{1,1}$, … y los bytes de la llave $k_{0,0}$, $k_{1,0}$, $k_{2,0}$,, $k_{3,0}$, $k_{1,0}$, $k_{1,1}$, … , $k_{3,3}$ Al final de la operación de cifrado, el texto cifrado es extraído del estado tomando los bytes de Estado en el mismo orden.

Consiste en la realización de las siguientes operaciones:

- La adición de una llave de ronda inicial
- 9 rondas, numeradas del 1-9, cada una de las cuales consiste de:

- Una transformación de un byte por medio de una sustitución
- Una transformación de un corrimiento de fila
- Una transformación mezcla de columna
- Una adición de una llave de ronda

- Una ronda final (ronda 10) que consiste de:

- Una transformación de un byte por medio de una sustitución
- Una transformación de un corrimiento de fila
- Una adición de una llave de ronda

La transformación por medio del byte de sustitución

La transformación del byte de sustitución es un byte de sustitución no lineal, operada en cada uno de los estados independientemente. La sustitución se da por medio de la caja-S que está ilustrada en figura 8.

En la tabla 12 se puede observar el arreglo de entrada a la caja-S.

$a_{0,0}$	**$a_{0,1}$**	**$a_{0,2}$**	**$a_{0,3}$**
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

Tabla 12. Arreglo de entrada a la caja- S

En la tabla 13 se puede observar la transformación aplicada al arreglo de entrada, mediante la caja-S.

$b_{0,0}$	**$b_{0,1}$**	**$b_{0,2}$**	**$b_{0,3}$**
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Tabla 13. Arreglo de salida de la caja- S

Por lo tanto, para cada elemento de estado, aplicamos la siguiente fórmula:

$b_{i,\,j}$=caja-S[$a_{i,j}$]

donde $a_{i,j}$ es el valor inicial del elemento en el Estado

y $b_{i,j}$ es el valor de salida del elemento en Estado

Transformación de corrimiento de fila

En la transformación por corrimiento de fila, las filas del estado son cíclicamente corridas a la izquierda por diferentes cantidades. La fila 0 no sufre ningún corrimiento, la fila 1 sufre un corrimiento por 1 byte, la fila 2 sufre un corrimiento por 2 bytes y la fila 3 sufre un corrimiento por 3 bytes.

A continuación se ilustra este tipo de corrimiento:

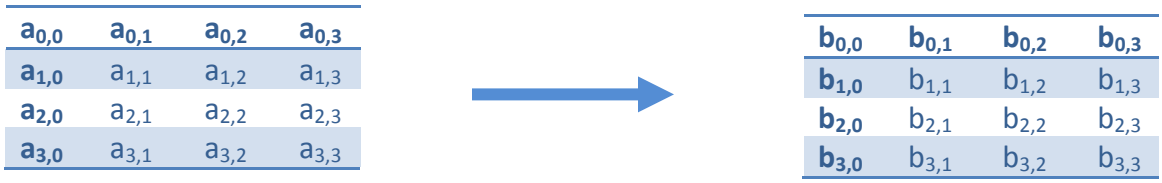
Primera fila (sin corrimiento)

Segunda fila (corrimiento en una unidad)

Tercera fila (corrimiento en dos unidades)

Cuarta fila (corrimiento en tres unidades)

En la tabla 14 se puede apreciar un resumen de la transformación de corrimiento de filas.



a0,0	**a0,1**	**a0,2**	**a0,3**
a1,0	a1,1	a1,2	a1,3
a2,0	a2,1	a2,2	a2,3
a3,0	a3,1	a3,2	a3,3

b0,0	**b0,1**	**b0,2**	**b0,3**
b1,0	b1,1	b1,2	b1,3
b2,0	b2,1	b2,2	b2,3
b3,0	b3,1	b3,2	b3,3

Tabla 14. Transformación de corrimiento de filas.

Transformación mezcla de columna

La transformación de mezcla de columna se aplica a cada columna del estado independientemente. Para la columna j, tenemos lo siguiente:

$$\mathbf{b}_{0,j} = T_2(\mathbf{a}_{0,j}) \oplus T_3(\mathbf{a}_{1,j}) \oplus \mathbf{a}_{2,j} \oplus \mathbf{a}_{3,j}$$

$$\mathbf{b}_{1,j} = \mathbf{a}_{0,j} \oplus T_2(\mathbf{a}_{1,j}) \oplus T_3(\mathbf{a}_{2,j}) \oplus \mathbf{a}_{3,j}$$

$$\mathbf{b}_{2,j} = \mathbf{a}_{0,j} \oplus \mathbf{a}_{1,j} \oplus T_2(\mathbf{a}_{2,j}) \oplus T_3(\mathbf{a}_{3,j})$$

$$\mathbf{b}_{3,j} = T_3(\mathbf{a}_{0,j}) \oplus \mathbf{a}_{1,j} \oplus \mathbf{a}_{2,j} \oplus T_2(\mathbf{a}_{3,j})$$

Donde:

$T_2(\mathbf{a}) = 2*\mathbf{a}$ **si** $\mathbf{a} < 128$

o $T_2(\mathbf{a}) = (2*\mathbf{a}) \oplus 283$ si $\mathbf{a} \geq 128$

y $T_3(\mathbf{a}) = T_2(\mathbf{a}) \oplus \mathbf{a}$.

Por ejemplo:

Si $\mathbf{a} = 63$ entonces $T_2(63) = 126$; $T_3(63) = T_2(63) \oplus 63 = 65$

Si $\mathbf{a} = 143$ entonces $T_2(143) = 5$; $T_3(143) = T_2(143) \oplus 143 = 138$.

En la tabla 15 se ilustra el efecto de la transformación mezcla de columnas en el estado. La mezcla de columnas se aplica en las columnas del estado

$\mathbf{a_{0,0}}$	$\mathbf{a_{0,1}}$	$\mathbf{a_{0,2}}$	$\mathbf{a_{0,3}}$
$\mathbf{a_{1,0}}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$\mathbf{a_{2,0}}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$\mathbf{a_{3,0}}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\mathbf{b_{0,0}}$	$\mathbf{b_{0,1}}$	$\mathbf{b_{0,2}}$	$\mathbf{b_{0,3}}$
$\mathbf{b_{1,1}}$	$b_{1,2}$	$b_{1,3}$	$b_{1,0}$
$\mathbf{b_{2,2}}$	$b_{2,3}$	$b_{2,0}$	$b_{2,1}$
$\mathbf{b_{3,3}}$	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$

Tabla 15. Transformación mezcla de columnas.

La adición de la llave de ronda

Para esta operación una llave de ronda es aplicada al estado por una simple or exclusiva o xor a nivel de bits. La llave de ronda es obtenida de la llave cifrada por medio de la llave Schedule. La longitud de la llave de ronda es igual a la longitud del bloque. En la tabla 16 se ilustra la adición de la llave de ronda.

$\mathbf{a_{0,0}}$	$\mathbf{a_{0,1}}$	$\mathbf{a_{0,2}}$	$\mathbf{a_{0,3}}$
$\mathbf{a_{1,0}}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$\mathbf{a_{2,0}}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$\mathbf{a_{3,0}}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\oplus$

$\mathbf{rk_{0,0}}$	$\mathbf{rk_{0,1}}$	$\mathbf{rk_{0,2}}$	$\mathbf{rk_{0,3}}$
$\mathbf{rk_{1,1}}$	$rk_{1,2}$	$rk_{1,3}$	$rk_{1,0}$
$\mathbf{rk_{2,2}}$	$rk_{2,3}$	$rk_{2,0}$	$rk_{2,1}$
$\mathbf{rk_{3,3}}$	$rk_{3,0}$	$rk_{3,1}$	$rk_{3,2}$

=

$\mathbf{b_{0,0}}$	$\mathbf{b_{0,1}}$	$\mathbf{b_{0,2}}$	$\mathbf{b_{0,3}}$
$\mathbf{b_{1,1}}$	$b_{1,2}$	$b_{1,3}$	$b_{1,0}$
$\mathbf{b_{2,2}}$	$b_{2,3}$	$b_{2,0}$	$b_{2,1}$
$\mathbf{b_{3,3}}$	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$

Tabla 16. Adición de la llave de ronda.

Por lo tanto para cada elemento del estado se tiene:

$\mathbf{b}_{i,j} = \mathbf{a}_{i,j} \oplus \mathbf{rk}_{i,j}$

Donde:

$\mathbf{a}_{i,j}$ es el valor inicial del elemento en el estado
$\mathbf{b}_{i,j}$ es el valor resulte del elemento en el estado

$\mathbf{rk}_{i,j}$ es el byte de la ronda de la llave.

Llave Schedule

Rijndael tiene 11 llaves de ronda, numeradas de 0-10, cada una de un arreglo de bytes de 4x4. Las llaves de ronda son calculadas por la llave cifrada basada en la llave Schedule. La llave de ronda inicial (considerado el cero como la llave de ronda) está formada directamente por la llave cifrada. Esta llave de ronda cero es usada sin alterar para la llave de adición inicial. Las restantes llaves de ronda son usadas en las diez rondas. Cada nueva llave de ronda es calculada por la llave de ronda anterior.

Nota. Es posible correr la llave Schedule ronda por ronda en un requerimiento base y sólo si se usan un total de 16 bytes almacenados en la llave de ronda.

Suponga que rkr,i,j son los valores de rth llave de ronda en la posición (i, j) en el arreglo y ki,j es la llave cifrada cargada dentro un arreglo de 4x4.

Inicialización:

$\mathbf{rk}_{0,i,j} = \mathbf{k}_{i,j}$ para toda **i** y **j**.

Las otras llaves de ronda (r=1 a 10 incluido) son calculadas a partir de la llave previa. Primero la columna 0 es construida:

$\mathbf{rk}_{r,0,0} = \mathbf{rk}_{r-1,0,0} \oplus$ caja-S[$\mathbf{rk}_{r-1,1,3}$] $\oplus$ ronda_const[**r**]

$\mathbf{rk}_{r,1,0} = \mathbf{rk}_{r-1,1,0} \oplus$ caja-S [$\mathbf{rk}_{r-1,2,3}$]

$\mathbf{rk}_{r,2,0} = \mathbf{rk}_{r-1,2,0} \oplus$ caja-S [$\mathbf{rk}_{r-1,3,3}$]

$\mathbf{rk}_{r,3,0} = \mathbf{rk}_{r-1,3,0} \oplus$ caja-S [$\mathbf{rk}_{r-1,0,3}$]

Entonces las restantes tres columnas son construidas en su turno de la columna correspondiente de la llave de ronda previa y su columna previa de la actual llave de ronda. La manera de realizarlo es la siguiente:

$\mathbf{rk}_{r,i,j} = \mathbf{rk}_{r-1,i,j} \oplus \mathbf{rk}_{r,i,j-1}$ para **i**=0,1,2,3 y **j**=1,2,3.

Las diez constantes de ronda son calculadas a partir de las siguientes ecuaciones:

ronda_const[1] = 1
ronda_const[r] = T2(ronda_const[r-1]) r=2,3…,10

son: 1, 2, 4, 8, 16, 32, 64, 128, 27, 54.

La caja-S

En la figura 8 se muestra la representación de la caja-S.

Caja-S [256] = {
99, 124, 119,123,242, 107, 111, 197, 48, 1,103, 43,254,215,171,118,
202,130,201,125,250, 89, 71,240,173,212,162,175,156,164,114,192,
183, 253,147, 38, 54, 63, 247, 204, 52, 165, 229,241,113,216, 49, 21,
4, 199, 35, 195, 24, 150, 5, 154, 7, 18, 128, 226, 235, 39, 178, 117,
9, 131, 44, 26, 27, 110, 90, 160, 82, 59, 214, 179, 41, 227, 47,132,
83, 209, 0, 237, 32, 252, 177, 91, 106, 203, 190, 57, 74, 76, 88, 207,
208, 239,170 ,251, 67, 77, 51,133, 69, 249, 2, 127, 80, 60, 159,168,
81, 163, 64, 143, 146,157, 56, 245,188,182,218, 33, 16, 255, 243,210,
205, 12, 19, 236, 95,151, 68, 23, 196, 167, 126, 61, 100, 93, 25, 115,
96, 129, 79, 220, 34, 42, 144, 136, 70, 238, 184, 20, 222, 94, 11, 219,
224, 50, 58, 10, 73, 6, 36, 92, 194, 211, 172, 98, 145, 149,228, 121,
231, 200, 55,109, 141, 213, 78,169,108, 86, 244,234,101,122, 174, 8,
186, 120, 37, 46,28, 166,180,198, 232, 221, 116, 31,75,189, 139,138,
112, 62, 181,102, 72, 3,246, 14, 97, 53, 87, 185, 134, 193, 29, 158,
225, 248, 152, 17, 105,217,142,148,155, 30,135,233,206, 85, 40, 223,
140, 161, 137, 13, 191,230, 66,104, 65,153, 45, 15,176, 84,187, 22 };

Figura 8. Caja-S.

1.6. Arquitectura de seguridad OSI.

La arquitectura de seguridad OSI, establece los siguientes cinco servicios fundamentales de seguridad de la información:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

1.6.1. Confidencialidad.

Su función es garantizar que la información sólo puede ser accedida por las partes autorizadas. La principal herramienta que implementa confidencialidad es la criptografía.

1.6.2. Autenticación.

Existen diversos tipos de autenticación, podemos considerar los siguientes:

Autenticación de identidad
Consiste en garantizar que los participantes de la comunicación son quien dicen ser. Es decir, es un proceso de identificación de una parte ante las demás, y debe hacerse de una manera incontroversial y demostrable.

Autenticación de origen de datos
Consiste en garantizar la autenticidad del origen de los datos. Que los datos vengan de donde deben venir.

La autenticación se clasifica en tres tipos, de acuerdo a la naturaleza de los elementos en que se basa su implementación:

- Algo que se sabe
- Algo que se tiene
- Algo que se es

Los dispositivos físicos que permiten la autenticación de los usuarios de un sistema contienen información relativa a su dueño o la actividad que pretende realizar. Esta información, además de servir como autenticador, puede ser usada para otros fines, tales como robo de información bancaria. Si estos dispositivos se usan remotamente, se corre el riesgo de que la autenticación del usuario no ocurra, simplemente se autentica el dispositivo, que puede estar en otra manos. Este tipo de dispositivos normalmente son tarjetas de presentación, tarjetas de banda magnética, tarjetas con códigos de barras. Es por esta razón que se han creado las tarjetas con procesador y memoria denominadas tarjetas inteligentes. Estas tarjetas tienen entre sus principales ventajas ser pequeñas y portátiles

Otra clasificación de la autenticación, puede ser:

Directa
En este proceso sólo intervienen las partes interesadas que se van a autenticar.

Indirecta
En este proceso interviene una tercera parte confiable que actúa como autoridad o juez, que avala la identidad de las partes.

1.6.3. Integridad.

La integridad consiste en proteger activos del sistema contra modificaciones, alteraciones, borrado, inserción y en general contra toda acción que atente contra la integridad.

1.6.4. Control de acceso.

El servicio de autenticación está íntimamente relacionado con el control de acceso. Su función es proteger los activos del sistema de accesos y usos no autorizados. Normalmente no utilizan técnicas criptográficas para su implementación. Existen gran número de técnicas y tipos de control de acceso, tales como los modelos específicos de Bell y LaPadula.

1.6.4.1. Antecedentes.

El uso de contraseñas se remonta a la antigüedad: los centinelas que vigilaban una posición solicitaban el "santo y seña" al que quisiera pasar. Solamente le permiten el acceso a aquella persona que conoce la contraseña. En la era tecnológica, las contraseñas son usadas comúnmente para controlar el acceso a sistemas operativos de computadoras protegidas, teléfonos celulares, decodificadores de TV por cable, cajeros automáticos de efectivo, etc. Una computadora puede hacer uso de contraseñas para diferentes propósitos, incluyendo conexiones a cuentas de usuario, accediendo al correo electrónico (e-mail) de los servidores, accediendo a bases de datos, redes, y páginas Web, e incluso para leer noticias en los periódicos (diarios) electrónicos.
El establecimiento de áreas y mecanismos de autenticación, como el anteriormente mencionado de "santo y seña" ha dado origen a lo que hoy se conoce como control de acceso, la cual es la actividad principal de la seguridad informática.

Para poder llevar a cabo un control de acceso, se necesita de un sistema acotado en sus componentes y usuarios. Dicho sistema teóricamente permite a cada componente saber en forma inequívoca con quien está interactuando en algún momento dado. Por lo tanto, el conocimiento es la base del funcionamiento de un sistema seguro, y en cada interacción es posible identificar las partes y garantizar su identidad, basado en los siguientes principios de la seguridad de la información:

- Confidencialidad
- Autenticidad
- Integridad

1.6.4.2. Procedimiento.

Para poder llevar a cabo un control de acceso efectivo, deben llevarse a cabo los siguientes pasos:
Registro
Identificación
Autenticación

Registro
Para poder llevar a cabo un procedimiento de control de acceso que utilice mecanismos de identificación y autenticación, es absolutamente necesario tener un procedimiento de registro. Dicho proceso de registro, dentro de un sistema informático lo convierte en un sistema acotado. En un sistema acotado aquellos elementos que están fuera del inventario, por definición, no forman parte del sistema. Es importante, establecer un sistema que incluya, altas, bajas, cambios y excepciones.

Un ejemplo de este tipo de procedimiento de control de acceso en un edificio corporativo es el siguiente:

Cada una de las empresas da de alta a sus empleados (alta en el registro del sistema).

Cuando el empleado decide separarse de la empresa, debe ser dado de baja del sistema (baja del registro).

Si el edificio tuviese un control de acceso por piso, y la empresa cambia su ubicación dentro del mismo edificio, debe efectuarse una actualización de la información y permitir a los empleados el acceso a su espacio de trabajo (cambio en los registros del sistema).

Si alguna persona quiere acceder al edificio para visitar alguna empresa, es indispensable realizar el registro en la recepción (excepciones en el registro).

Identificación
Durante la fase de registro, el usuario debe realizar el proceso de identificación. Para identificar al usuario se debe de extraer información que permita identificar al usuario de manera única entre la población, número de cuenta, nombre, número de pasaporte, son algunos ejemplos de dicha información.

Mediante esta información es como se localizará al usuario en el registro previamente realizado.

Para evitar la suplantación de identidad, normalmente se colocan mecanismos de seguridad para verificar el vínculo entre los documentos que identifican a la persona y la persona.

Algunos de los mecanismos incluyen, fotografía, firma, huella digital.

Autenticación
Por último se encuentra la autenticación, en la cual el usuario debe depositar o recibir un autenticador (luz verde, gafete de entrada, tarjeta de transporte público).

En algunas ocasiones este dispositivo o dato se considera como evidencia incontrovertible de que el que aparece o porta el dispositivo o dato es el mismo que ha sido registrado. En este punto si el autenticador no es correcto, el servicio solicitado será denegado.

1.6.5. No repudio.

Proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación nieguen haber enviado o recibido un mensaje o haber sido el destinatario de una acción.

Los servicios de no repudio identificados por OSI (Open System Interconnection) son los siguientes:

- No repudio con prueba de origen
- No repudio con prueba de entrega

Para implementar no repudio se utilizan esquemas de llave pública como firmas digitales, pero no se restringe a ellas, también se pueden usar técnicas de cifrado de llave pública y de llave secreta, en esta última, siempre que se utiliza una tercera parte confiable.

1.7. Principios de comunicación inalámbrica.

La comunicación inalámbrica se define como la transferencia de información a una distancia determinada sin el uso de un conductor o cable.

Algunos ejemplos de comunicación inalámbrica:

La TV y el radio trabajan usando un radio de frecuencia de 30 a 300 MHz.

La red GSM usada por los teléfonos celulares. GSM usa una porción de radio frecuencia denominada ultra alta frecuencia o UHG, para la transmisión y recepción de señales. El rango de frecuencia UHF va de los 300 a los 3000 MHz. La banda UHF es también compartida por la TV, Wi-Fi y la transmisión de datos vía bluetooth

Wi-fi que es una tecnología diseñada y optimizada de una red de área local (LAN). Esta provee una extensión de las redes alámbricas para docenas de dispositivos dentro de un rango de 100 metros. La tecnología Wi-fi usa el rango de frecuencias de 2.4 a 24835 GHz. Este rango de frecuencias es compartido por algunos dispositivos como hornos de microondas que pueden generar interferencia. Es por esto que desde 2006, un nuevo rango de frecuencias de alrededor de 5 GHz es usado para Wi-Fi.

RFID (Radio Frecuency Identification) es un método automático de identificación, confiable en el almacenamiento y obtención remota de datos usando dispositivos llamados etiquetas RFID. Una etiqueta RFID es un objeto pequeño que puede ser incorporado en un producto. Las etiquetas RFID contienen chips de silicón para habilitar la recepción y envío de datos a consultas desde un lector RFID. RFID es una comunicación de rango corto lo cual significa que las etiquetas RFID pueden ser sólo leídas a algunos centímetros del lector.

La tecnología Bluetooth fue diseñada para reemplazar los cables de los teléfonos celulares, laptops y otros dispositivos de cómputo y la comunicación de los dispositivos se lleva a cabo en un rango de 10 metros aproximadamente. Este rango de radio frecuencia va de los 2.4 a 24835 GHz.

IrDA es una tecnología de comunicación de rango corto (menos de un metro), es una comunicación de campo visual estándar para el intercambio de datos a través de una luz infrarroja. La interface IrDA es frecuentemente usada en computadoras y teléfonos móviles.

Las tarjetas inteligentes que establecen comunicación a distancia incorporan un microprocesador que se comunica con un lector a través de la tecnología RFID. Algunos ejemplos de la comunicación a distancia de las tarjetas inteligentes son el ISO 14443 y FeliCa, la cual permite un rango máximo de 10 cm en las comunicaciones a distancia.

La tecnología de comunicación inalámbrica da la energía para el flujo entre la tarjeta y la interface del dispositivo sin un contacto físico. Lo que define la tecnología de comunicación a distancia es que sólo el transmisor/receptor esta encendido.

Las técnicas de inducción o transmisión de alta frecuencia son usadas a través de una interface de radio frecuencia.

El principio de la tecnología inalámbrica es que el transmisor/receptor envía energía y datos. El campo magnético pasa por la antena y enciende el dispositivo NFC (campo de comunicación a distancia corta) que puede ser también una tarjeta inteligente o una etiqueta RFID.

En la figura 9, se representa un diagrama con los componentes esenciales de un sistema de comunicación inalámbrica.

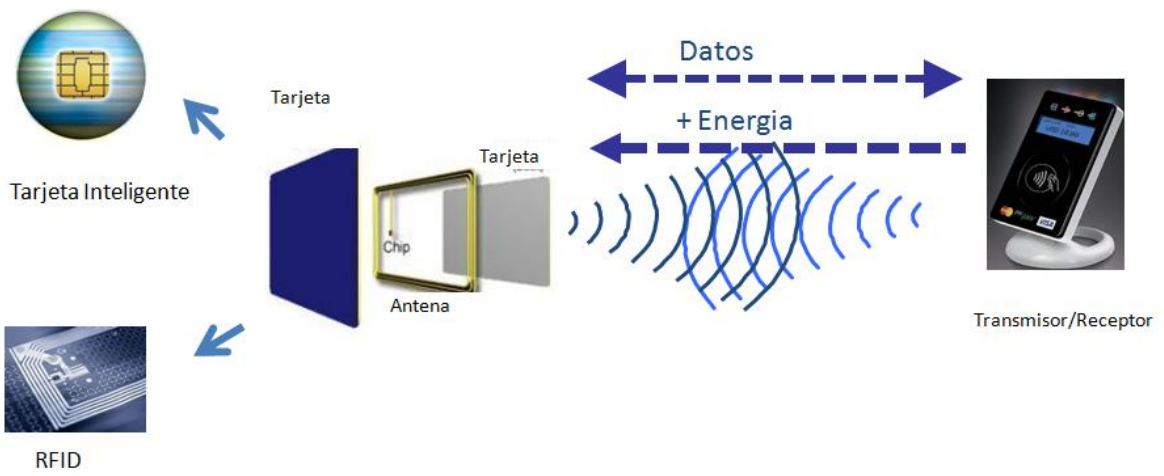


Figura 9. Diagrama de los componentes esenciales de la comunicación inalámbrica.

1.8. RFID.

La tecnología de identificación de radio frecuencia (RFID Radio Frecuency Identification) es un método de identificación automática, basado en el almacenamiento y obtención de datos remotamente usando dispositivos denominados etiquetas RFID.

Las etiquetas RFID son objetos pequeños que pueden incorporarse en algunos productos. Dichas etiquetas contienen chips de silicón capaces de recibir y enviar peticiones desde un lector o escritor RFID.

RFID establece una comunicación en un rango reducido, sin embargo, soporta una distancia mayor para el intercambio de datos que la tecnología de comunicación a distancia (contactless), típicamente son algunos metros.
Los dispositivos RFID normalmente no incluyen memoria de escritura o microcontroladores compatibles con las tarjetas inteligentes con comunicación a distancia.

La identificación de radio frecuencia puede trabajar a diferentes frecuencias. Una frecuencia específica para cada caso de uso, por ejemplo, frecuencias menores a los 125KHz son usadas para las aplicaciones de transporte, mientas que las de altas frecuencias son usadas para control de acceso seguro.

NOTA: Las tarjetas NFC (Near Field Communication) pueden únicamente leer las etiquetas RFID que trabajan a 13.56 MHz debido a que es un estándar NFC.

1.9. Tarjetas inteligentes con comunicación inalámbrica.

La comunicación inalámbrica es una tecnología un tanto madura, tiene alrededor de 10 años de existencia. Se busca el reemplazo de códigos de barras o bandas magnéticas.

Una tarjeta inteligente con comunicación a distancia, es una tarjeta en la cual el chip se comunica con un lector de tarjetas a través de la tecnología de inducción RFID. Estas tarjetas deben ser acercadas a una antena para completar una transacción pero no requieren del contacto con el validador. Éstas son usadas para facilitar transacciones a manos libres, usualmente menores a cinco mil milisegundos, tales como sistemas de transito masivo, donde la tarjeta inteligente puede ser usadas sin siquiera sacarla de una cartera o monedero.

Las tarjetas inteligentes con comunicación inalámbrica operan en un rango reducido de operación, el cual representa algunos centímetros y usa la frecuencia de 13.56 MHz.

Las tarjetas inteligentes con comunicación a distancia contienen un microprocesador el cual hace cálculos, y se comunica en ambos sentidos, tiene una memoria con información y hace uso de las características de seguridad y algunas otras aplicaciones.

1.9.1. Limitantes de las tarjetas con comunicación inalámbrica.

La limitante de las tarjetas (U)SIM con comunicación a distancia es que normalmente ocupan un solo protocolo y soportan un solo tipo de aplicación (por ejemplo pasaporte, transporte y pagos).

Además no es posible modificar la tarjeta con comunicación a distancia vía remota (OTA) y no hay una GUI (interface gráfica de usuario).

La solución escogida para eliminar estas limitaciones es el uso de NFC. Los estándares NFC para la comunicación en un rango de frecuencias limitado para las comunicaciones inalámbricas que permiten el intercambio de datos entre dispositivos a una distancia de 10 cm aproximadamente.

Esto opera en un rango de radio frecuencia de 13.56 MHz. La tecnología es una extensión del estándar de tarjetas con comunicación a distancia ISO 14.443, el cual combina la interface de una tarjeta inteligente y un lector en un solo dispositivo. Un dispositivo NFC puede comunicarse con ambos tarjetas y lectores, así como también con otros dispositivos NFC, y es también compatible con la infraestructura ya existente para el transporte público y pagos móviles.

NFC es principalmente usada en los teléfonos móviles. NFC fue aprobada como un estándar ISO el 8 de diciembre de 2003. Ésta es una tecnología de plataforma abierta estandarizada en el ISO 18.092.

Este estándar especifica los esquemas de modulación, codificación, velocidades de transferencia y los esquemas de la interface de radio frecuencia en los dispositivos NFC, así como la inicialización y condiciones de los esquemas requeridos para el control de colisiones durante la inicialización.

1.10. Los modos de operación NFC.

La tecnología NFC define 2 modos de comunicación denominados activo y pasivo.

En el modo activo, ambos dispositivos generan su propio campo de radio frecuencia para el transporte de datos.

En el modo pasivo, la comunicación se establece a partir del campo de radio frecuencia generado por un dispositivo, mientras que el otro dispositivo usa la modulación de carga

para transferir datos. El protocolo especifica que el inicializador es el dispositivo responsable de generar el campo de radio frecuencia.

La tecnología NFC es principalmente usada por los teléfonos móviles, hay tres principales casos de uso de NFC:

- Emulador de tarjeta, donde el dispositivo NFC se comporta como una tarjeta con comunicación a distancia

- Modo lector donde el dispositivo NFC está activo y lee una etiqueta RFID, por ejemplo de publicidad interactiva

- Modo punto a punto, donde 2 dispositivos NFC se comunican en conjunto e intercambian información.

1.10.1. Modo emulador de tarjeta.

En este modo, los dispositivos NFC se comportan como una tarjeta con comunicación a distancia. Para ser más precisos, el chip NFC en los teléfonos móviles se comporta como una tarjeta con comunicación a distancia en modo esclavo. El lector de radio frecuencia genera el campo de radio frecuencia mientras que el dispositivo NFC usa la modulación de carga para transferir datos.

Todos los comandos APDUs (protocolo de comunicación entre la (U)SIM y el terminal) son enviados por el lector de radio frecuencia.

Este modo es usado para aplicaciones bancarias Paypass o aplicaciones de transporte como Calypso.

Debido a que el modo emulador de tarjeta es un modo de comunicación pasivo, éste trabaja aún si el equipo móvil no tiene batería.

1.10.2. Modo lectura escritura.

En el modo lectura escritura, la tarjeta con la característica de comunicación a distancia en el equipo móvil, actúa como un lector de radio frecuencia en modo maestro enfrente de una etiqueta. Este modo puede ser usado para obtener la información como una URL, número de teléfono, o datos de SMS desde una etiqueta.

Este modo es usado para leer un precio o una referencia, y desplegarlo en la pantalla de un equipo móvil.

1.10.3. Modo punto a punto.

En el modo punto a punto, el chip NFC en el equipo móvil actúa en ambos modos maestro esclavo. Este modo es usado para intercambiar información entre teléfonos

1.11. Los protocolos de comunicación inalámbrica de tarjetas inteligentes.

En la figura 10, se muestran los protocolos de comunicación a distancia utilizados por las tarjetas inteligentes.

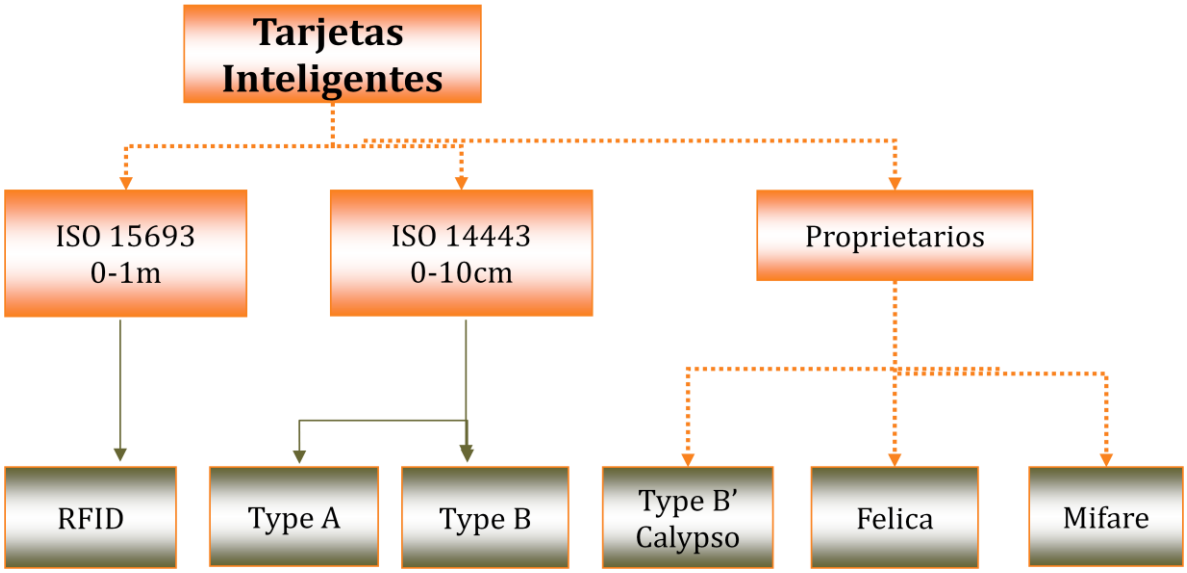


Figura 10. Protocolos de comunicación inalámbrica de tarjetas inteligentes.

ISO 14443 Tipo A

Diseñado por Philips para aplicaciones simples de tarjeta de memoria
Codificación por amplitud
Protocolo Mifare es utilizado por ISO 14443 parte 2 y 3 tipo A

ISO 14443 Tipo B
Diseñado por un grupo de proveedores de equipos móviles y usuarios de aplicaciones para tarjetas inteligentes.
Codificado en modulación

ISO 14443 Tipo B' o Innovatron
Misma Capa física que Tipo B

Capas superiores son propietarias

JISX6319-4
Felica hecha por Sony también llamado tipo C.

EMV Totalmente compatible con el ISO14443 tipo A y B

Los dos principales protocolos de comunicación soportados bajo la serie ISO 14443 son los tipos A y B. Se intento incluir algunos otros sistemas tales como los apéndices Tipo C(Sony/Japón), Tipo D(OTI/Israel), Tipo E(Cubic/USA) y Tipo F(Legic/Suiza) y tipo G(China) pero al final no fueron acepados por el estándar.

1.11.1. Estándares ISO 14443.

ISO 14.443 es una parte de los estándares internacionales para las tarjetas con comunicación a distancia, opera a los 13.56 MHz.
Este estándar ISO establece los estándares de comunicación y protocolos de transmisión entre una tarjeta y un lector, para crear interoperabilidad de los productos relacionados con las tarjetas inteligentes de comunicación a distancia.
La primera parte del estándar define las características físicas
La segunda parte define la interface de radiofrecuencia y la interface de la señal.
La tercera parte define la inicialización y los procedimientos de anticolisión.
La cuarta parte especifica el protocolo de transmisión que establece el intercambio de bloques de datos y sus mecanismos.

Como se ha visto anteriormente, los dos protocolos de comunicación son reconocidos por el estándar ISO, tipo A y B. La principal diferencia entre estos tipos se debe a los métodos de modulación, los esquemas de comunicación que se definen en la parte 2 y el protocolo de inicialización definido en la tercera parte.

Las partes 1 y 3 son suficientes para conocer los estándares ISO. La parte 4 es descrita como una parte opcional dentro de las especificaciones ISO, pero es mandatorio asegurarse su completa interoperabilidad. Los principales clientes requieren una completa compatibilidad de la parte 4 para asegurarse que sus sistemas soportan las diferentes tarjetas de los diferentes proveedores. Un lector debe soportar todas las partes del estándar, así como ambos tipos de comunicación A y B, para recibir la aceptación de compatibilidad ISO.

2. Análisis.

2.1. Situación actual.

En la actualidad existen lectores transmisor/receptor para el control de acceso en algunos transportes públicos, estacionamientos, la renta de algunos accesorios (bicicletas), ingreso a edificios corporativos. Para cada uno de los ejemplos mencionados, los establecimientos emiten su propia tarjeta. Esto se traduce en una gran cantidad de dispositivos para el usuario, y un gasto extra por la emisión de la tarjeta.

Por otro lado, se tienen tarjetas (U)SIM, las cuales tienen la característica de poder ser actualizadas a través de una interface aérea. Estas tarjetas además, tienen una característica llamada portabilidad, es decir, trabajan de la misma manera independientemente del dispositivo móvil. Tienen además, la capacidad de realizar cálculos matemáticos en tiempo real, lo cual permite hacer transacciones únicas.

Dado lo anterior, se tiene como objetivo crear una tarjeta (U)SIM, la cual debe cumplir con los siguientes objetivos:

- Tarjeta que contenga una aplicación para realizar el control de acceso al transporte público.
- Debe tener la capacidad de ser actualizada de manera remota.
- Debe contener la información correspondiente al operador.
- Disponer de una aplicación tipo monedero electrónico recargable.

El operador de red, el cual a su vez llamaremos cliente, asignó la elaboración de la tarjeta desde su análisis hasta su implementación. El equipo de desarrolladores en adelante también se describirá como consultores.

La tarjeta de pruebas será denominada tarjeta de ingeniería, dicha tarjeta puede sufrir modificaciones.
La tarjeta de producción, será denominada tarjeta BAP (buena a producir), dicha tarjeta no debe sufrir ningún cambio, pues ésta es una tarjeta de producción.

2.2. Metodología de desarrollo.

La metodología de desarrollo utilizada para la creación de la tarjeta (U)SIM se describe a continuación (ver figura 11):

- Requerimientos. Se realizan una serie de reuniones entre los encargados de crear la tarjeta (consultor) y el operador, con el objetivo de que ambas partes definan los requerimientos de la tarjeta de ingeniería.
  Esta etapa es de suma importancia debido a que los consultores deben entender las necesidades del cliente para transformarlos en requerimientos.
- Plan de trabajo y cotización. El consultor debe tener una comprensión total de las necesidades del cliente, así como del software, infraestructura y recursos humanos requeridos. Después el consultor debe elaborar un plan de trabajo, en el cual se especifican cada una de las actividades y los tiempos de desarrollo necesarios para la realización de la tarjeta.
  El plan de trabajo y su cotización son entregados al cliente.
- Solicitud de desarrollo. Cuando el cliente acepta el plan de trabajo y su cotización, éste realiza una solicitud de elaboración de tarjeta de ingeniería al consultor. De esta manera se formaliza la aceptación y el inicio del desarrollo del proyecto.
- Elaboración de especificaciones detalladas. El consultor genera un documento denominado NOG(Network Operator Guide), el cual describe detalladamente las características de la tarjeta, así como la funcionalidad de cada una de las aplicaciones.
- Aceptación de las especificaciones. El operador revisa las especificaciones detalladas y se realiza una retroalimentación hasta el momento en el cual ambas partes logran un acuerdo.
  Cabe aclarar, que los cambios en las especificaciones son mínimos, la retroalimentación se realiza para evitar la omisión de características y funcionalidades de la tarjeta. En caso de que los cambios solicitados afecten de manera relevante la estructura y diseño de la tarjeta, se deberá hacer un cambio de alcance y cotización.
- Implementación del sistema. El consultor realiza la tarjeta de ingeniería, misma que debe ser probada por el operador. El operador debe validar toda la funcionalidad de la misma, y en caso de cambios mínimos se pueden realizar en presencia del operador. En caso de cambios mayores, se debe proceder a elaborar una nueva tarjeta de ingeniería acorde a las necesidades del operador. De no recibir la aceptación del operador, no se pueden generar la tarjeta de producción y continuar con las pruebas de tarjeta BAP.
  Se debe validar nuevamente toda la funcionalidad de la tarjeta BAP, en caso de encontrar un error se debe realizar una nueva tarjeta de ingeniería y una nueva BAP.
- Puesta en producción. Una vez que el operador haya dado la aceptación de la tarjeta BAP, se puede proceder a la elaboración de lotes de producción.

- Garantía del proyecto. El operador puede encontrar algún error que no fue perceptible en las pruebas anteriormente mencionadas, en ese caso se puede proceder a una actualización vía OTA (Over The Air).

Figura 11. Metodología de desarrollo

2.3. Requerimientos del usuario.

Tener una tarjeta (U)SIM que cumpla con los siguientes requerimientos:

- Autenticación 3G utilizando el algoritmo Milenage. Las constantes R y C deben ser las variables estándar ETSI 135 TS 206. Estas se colocan en la tabla 17.

Constante	
R1	64
R2	00
R3	32
R4	64
R5	96
C1	00000000000000000000000000000000
C2	00000000000000000000000000000001
C3	00000000000000000000000000000002
C4	00000000000000000000000000000004
C5	00000000000000000000000000000008

Tabla 17. Constantes y variables de rotación definidas por el estándar ETSI 135 TS 206.

La diversificación de la OPC debe realizarse en el centro de personalización con la OP proporcionada por el operador y la llave Ki de autenticación a red. Cada OP debe ser única para cada tarjeta. El algoritmo a utilizarse es el siguiente:

OPC = AES-128 (OP,KI) XOR OP

- El lenguaje que debe tener predefinido la tarjeta (U)SIM debe ser Español
- La tarjeta (U)SIM debe de tener definido un centro de mensajes
- En la tabla 18 se definen los números de servicio, requeridos por el operador.

Identificador	Número
Atención ciudadana	066
Bomberos	116
Cruz Roja	065

Tabla 18. Números de servicio.

La agenda a utilizar debe ser una agenda 2G con 250 registros.
La agenda de números fijos debe contar con 20 registros.
Colocar 10 registros para el almacenamiento de LDN (last number dialed).

En la tabla 19 se muestra la manera en que se pide calcular los códigos de seguridad de la tarjeta.

Código	Número
PIN1	Fijo 1111
PIN2	Aleatorio a 4 dígitos
PUK1	Aleatorio a 8 dígitos
PUK2	Aleatorio a 8 dígitos

Tabla 19. Generación de los códigos de seguridad de la tarjeta.

Además debe contar con una aplicación capaz de realizar las siguientes acciones:
- Permitir el acceso a un sistema de transporte público
- Realizar la compra en una máquina expendedora de café
- Poder consultar y abonar saldo a la tarjeta.
- Comunicación inalámbrica tipo A

2.4. Propuesta y justificación de solución.

Dadas las características anteriormente descritas de la seguridad dentro de la tarjeta (U)SIM, tales como la autenticación mutua, la actualización remota y las condiciones de acceso propias de cada archivo de la (U)SIM ésta es considerada un elemento seguro, capaz de realizar cálculos matemáticos en tiempo real. Por lo tanto, para este trabajo he elegido a la tarjeta (U)SIM como el elemento seguro que se comunica con el equipo móvil.

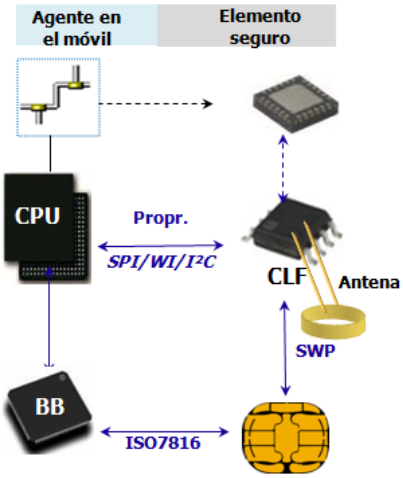


Figura 12. El elemento seguro y su interacción con el equipo móvil

En la figura 12 se observa el elemento seguro (tarjeta (U)SIM) y su conexión dentro del equipo móvil. Es importante destacar las siguientes características de la tarjeta (U)SIM:

- Capacidad de actualizarse remotamente.
- Implementa un protocolo de comunicación inalámbrica.
- Capacidad de soportar más de una aplicación.
- Portabilidad.

Otra característica es que el usuario final tenga un solo dispositivo en el cual pueda tener el control de acceso a algún sistema de transporte, adicionalmente tener un pequeño monedero para realizar la compra de algún producto y además conserve las características de la tarjeta (U)SIM como la recepción y realización de llamadas, el envío de SMS, la agenda de contactos, agenda de número restringidos, etc.

Hoy en día los lectores de tipo transmisor/receptor se han ido incrementando, se tienen por ejemplo en algunas de las autopistas donde se hace un cobro de prepago, en algunos transportes públicos, en algunos accesos a estacionamientos, acceso a edificios corporativos, en algunos restaurantes, etc. Dado lo anterior, es claro que se requiere tener un sistema que homologue todos estos escenarios anteriormente mencionados, lo cual puede ser bastante costoso. Otra manera para resolver este problema es tener una tarjeta que implemente el control de acceso para estos servicios en un mismo elemento, por lo cual el costo de generación de tarjetas es significativamente menor que el de establecer un sistema único para estos elementos, además de poder ser actualizadas de manera remota.

3. Diseño y desarrollo.

3.1. Aplicaciones dentro de la tarjeta SIM.

A continuación se detallan algunos aspectos a considerar en el desarrollo de aplicaciones para una tarjeta (U)SIM.

3.1.1. Administración de los recursos.

En las aplicaciones Java Card, los recursos son limitados debido al tamaño físico del microprocesador (chip). Los desarrolladores deben estar conscientes de este problema y deben también siempre estar alerta en el consumo de recursos.

Por lo tanto se describirán los siguientes puntos:

- Administración de la memoria EEPROM.
- Alojamiento de objetos.
- Administración de la memoria RAM.

3.1.1.1. Administración de la memoria EEPROM.

La memoria EEPROM contiene los siguientes elementos:

Sistemas globales de datos.
Estos datos incluyen por ejemplo los buffers usados como respaldo para la integridad o alguna información global de la misma tarjeta.
La EEPROM en una tarjeta Java contiene los siguientes elementos:

Bytecode
El código para todas las aplicaciones y librerías está almacenado en EEPROM. En muchas aplicaciones incluso, el código consume una cantidad considerable de EEPROM.

Objetos Java
Todos los objetos Java persistentes son almacenados en EEPROM. Esto incluye los objetos que son creados por los applets ROM, así como los applets descargados.

La memoria EEPROM puede estar organizada de diversas maneras:

Una pila larga de código y datos.
En ese caso, el código y los datos son almacenados en la misma área y pueden ocuparla de manera libre, lo cual significa que es la opción más simple para el desarrollador. Sin embargo, en tarjetas con mayor cantidad de memoria, esto representa un incremento significativo en el tamaño de los objetos.

Una pila por código y una pila por dato
Ésta es una solución intermedia que puede ser útil en casos en los cuales toda la memoria no puede ser direccionada como bytecode. Esto es interesante, debido a que el uso de restricciones no es muy poderoso y el sistema usualmente tiene un bajo incremento de los objetos.

Una pila para cada paquete de aplicación
En este caso, una pila dedicada es asignada a cada paquete. Esto puede ser muy práctico, pero la mayor dificultad con este modelo, es que el desarrollador de aplicaciones, tiene que conocer la prioridad de la instalación de la cantidad de espacio que será consumido por los datos de la aplicación.

Finalmente, las herramientas de administración de la memoria EEPROM podrían incluir más o menos técnicas poderosas. En particular hay algunas características que podrían ocurrir como:

Colector de basura
Algunas plataformas incluyen el colector, por ejemplo para la colección de objetos no usados. Sin embargo, esta característica tendría un costo en el futuro cercano.

Administración de la fragmentación
Algunas plataformas incluirán una característica que limita la fragmentación de la memoria cuando los paquetes y los objetos son borrados (ya sea explícito o a través del recolector de basura)

Cuando se desarrollan aplicaciones genéricas (que serán usadas en diferentes plataformas), es una buena práctica no asumir nada acerca del manejo de la memoria EEPROM.

3.1.1.2. Alojamiento de objetos.

Un objeto ocupa espacio de memoria por dos razones principales:

- Espacio para almacenar componentes (campos, arreglos de elementos). Este espacio depende del tipo de componente y será descrito más adelante.
- Sobrecarga de espacio requerido por la administración de memoria del sistema. Esta sobrecarga incluye al menos un encabezado y algunos más, como se explicará más adelante.

El alojamiento de los objetos necesita estar limitado por dos principales razones:

- Hay poca memoria disponible.
- No hay manera de reciclar la memoria para objetos perdidos.

Existen tres posibles estrategias para el alojamiento de los objetos:

- Alojamiento de todos los objetos durante la instalación de un applet. Para applets poco complejos y con una cantidad de datos fijos, ésta es la estrategia más segura. El punto más importante es que la instalación podría fallar si no hay suficiente espacio en la tarjeta para alojar todos los objetos, lo cual hace más simple la recuperación de todo el espacio ocupado por la instancia del applet.
- Alojamiento de todos los objetos durante la instalación y personalización del applet. Para applets un poco más complejos, se debe tener mayor flexibilidad y no es algo razonable alojar todos los objetos durante la instalación del applet. Sin embargo, es común que el alojamiento pueda ser limitado para la fase de personalización (durante la cual todos los objetos son inicializados). La mayor desventaja de esto es que si el applet agota el espacio de memoria al final de la personalización, puede perderse algún espacio de memoria. Otra desventaja es que un comando que aloja objetos podría dejarse disponible al usuario después de terminar la fase de personalización.
- Alojamiento de objetos cuando son requeridos. Esto es bastante peligroso, porque el applet podría agotar el espacio de memoria en cualquier momento. Esto debe ser usado para applets extremadamente abiertos y esto debería ser asociado a precauciones específicas.

3.1.1.3. Administración de recursos en memoria RAM.

Los objetos transitorios son muy prácticos y son usados frecuentemente en los applets por dos propiedades muy interesantes:

- El acceso a los campos es más rápido y no los desgasta (es bastante útil para la información que es modificada en muchas ocasiones, tales como un “archivo actual” o bien un “registro actual”)
- Estos campos son reseteados cuando ocurren algunos eventos, así pueden ser usados para almacenar los estados de seguridad.

Por lo tanto el alojamiento de estos objetos debe ser controlado de manera bastante minuciosa.

En Java Card 2.2 los objetos transitorios deben ser sólo arreglos. A fin de calcular el tamaño ocupado por los arreglos transitorios, las reglas estándar deben ser usadas, con una regla en especial:

El descriptor del objeto debe ser almacenado en EEPROM y los elementos del arreglo son almacenados en RAM. Esto simplifica el cómputo para el tamaño de la memoria RAM a ser consumida.

Existen 2 tipos de objetos transitorios:

BORRADO AL TÉRMINO DE LA SELECCIÓN
Este tipo de objetos son borrados cada vez que se ha terminado la selección del applet. Por ejemplo cuando otro applet es seleccionado o cuando la tarjeta es reseteada.

BORRADO EN RESET
Los objetos transitorios son borrados sólo cuando la tarjeta es reseteada. Esta característica puede ser muy útil cuando un valor necesita ser guardado en 2 selecciones de applet. De hecho, en este tipo de borrado los objetos más usados son objetos que pueden ser compartidos, porque éstos son los únicos que son accesibles cuando el applet es accesado a través de un mecanismo compartido.

3.1.2. Aislamiento de una aplicación.

Cada plataforma de tarjetas Java incluye una implementación de un cortafuegos definida en la especificación del ambiente Runtime de Java Card 2.2. Este cortafuegos asegura un aislamiento entre aplicaciones y plataforma de la siguiente manera:

- Un applet no puede acceder o modificar datos que pertenezcan a otra aplicación o a una plataforma.
- La plataforma garantiza que el applet no puede hacerse pasar por otro applet.

A fin de asegurar que el applet tiene un aislamiento total, los desarrolladores de applets necesitan seguir las siguientes reglas:

No exportar componentes en los applets.
Esta regla quiere decir que está prohibido que un applet esté ligado con alguno otro.

No usar objetos o interfaces compartidas.
Es decir, un applet no debe confiar en objetos compartidos por alguna interface.

3.1.3. Seguridad que debe proveer un applet.

El applet debe proveer su propia seguridad. Estas reglas son las siguientes:

Código de reglas de desarrollo de un applet
La seguridad de la plataforma confía en que el código es correcto. Por lo tanto los desarrolladores deberán asegurarse que la aplicación que se está entregando ha sido generada con la versión correcta usando la versión del código generada con herramientas compatibles, por ej. Java Card 2.2.

Entregable y reglas de un applet
Un proceso de entrega segurizado necesita ser establecido entre el desarrollador y los fabricantes de las tarjetas (U)SIM. Esto se hace con el fin de garantizar la integridad y confidencialidad del código a ser descargado en la tarjeta.

Reglas para la descarga del código de un applet
Las implementaciones de Java Card no implementan un verificador interno. Esto significa que la seguridad interna de la tarjeta confía en el hecho de que el código ha sido verificado fuera de la tarjeta. Si este tipo de validaciones no son realizadas, es posible que se descarguen aplicaciones maliciosas en la (U)SIM.
Esto debe ser evitado a toda costa antes de la emisión. Por lo tanto el fabricante debe definir procedimientos apropiados para la descarga del código, en particular debe realizarse la verificación del código del applet.

3.1.4. Objetos compartidos.

El cortafuego del applet se encarga de controlar la separación entre los diferentes espacios de los objetos, los cuales son llamados contextos. Un contexto está asociado con cada paquete de tal manera que todos los applets de un paquete comparten el mismo contexto. Si la máquina virtual ejecuta un bytecode que ha sido invocado con ciertas condiciones que han sido cumplidas, la máquina virtual ejecuta un cambio de contexto y coloca el contexto actual en la pila. El contexto llamado es restaurado (reinvocado desde la pila) al final de la ejecución del método. El ambiente de ejecución de Java o JCRE(Java Card Runtime Environment) tiene su propio contexto con privilegios específicos.

Cada objeto pertenece ya sea a un applet o a un contexto JCRE. La propiedad de cada objeto creado está relacionada al applet del contexto actual. Un objeto puede ser accesado sólo por su propio contexto, si el último es el que está activo, tal como un mecanismo de prevención para el acceso no autorizado a un objeto. Para habilitar la interacción entre applets, el estándar define el concepto de shareable interface (interface compartida). Esto significa la invocación, desde un contexto, métodos de un objeto que no son propios. Nótese que los campos de otros métodos de un objeto no son accesibles, sólo los métodos definidos en la interface compartida están disponibles a través del cortafuegos. Cuando un método de la interface compartida es invocado, un cambio de contexto ocurre para el contexto del objeto del dueño, bajo control de JCRE. Tal mecanismo permite una comunicación segura inter-applet. Cuando un objeto invoca la interface compartida, esto no significa que todos pueden hacer uso de sus métodos o leer sus datos. Cuando otro objeto quiere acceder a un método compartido (o datos), éste pregunta al dueño para que le dé autorización. Si es aceptado, éste le da al demandante, una referencia al método(o datos) llamado capacidad. Con esta capacidad, los objetos distantes podrán usar el método local.
Cuando un objeto da una referencia a otro objeto en un método local compartido, es imposible cancelarlo.

En la figura 13 podemos ver una representación de intercambio de objetos. En esta representación, el servidor acepta dar una referencia al objeto X para el cliente.

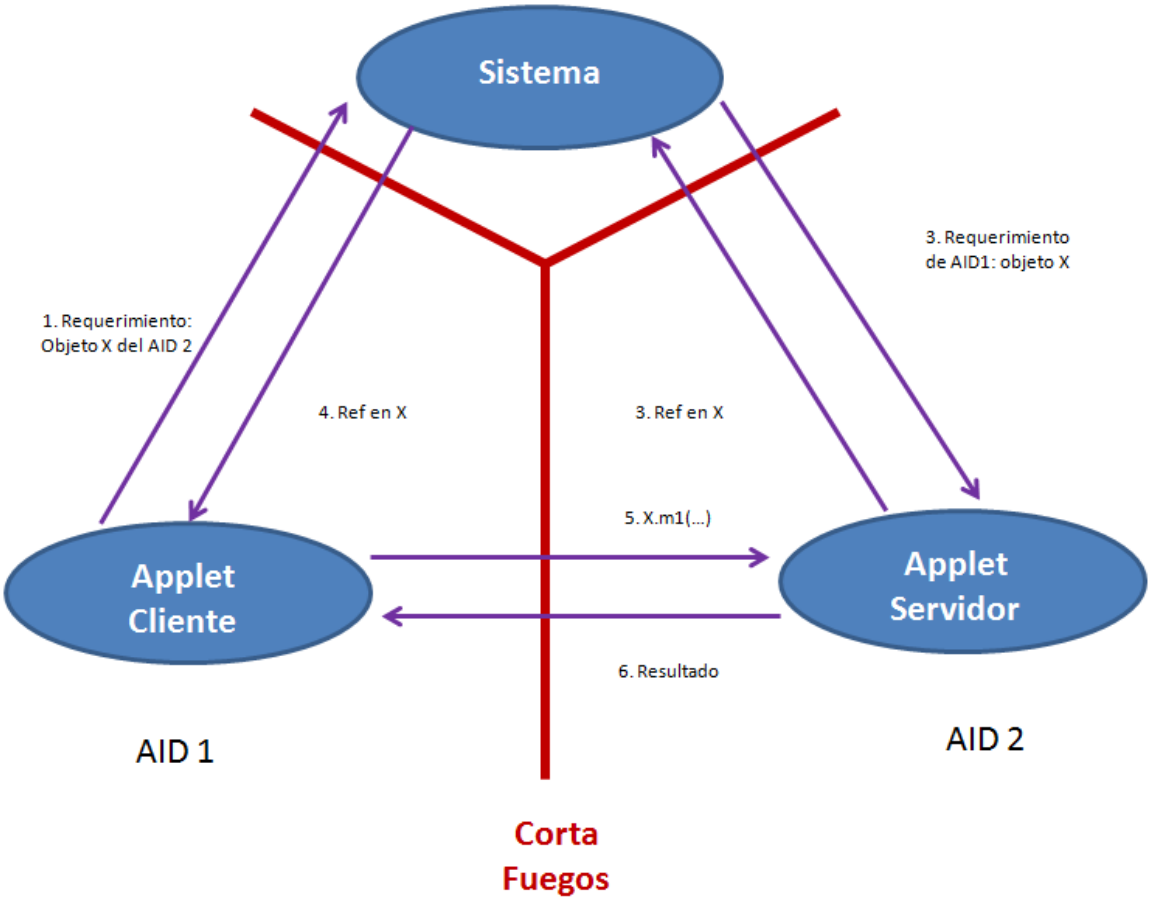


Figura 13. Diagrama de objetos compartidos en las aplicaciones de la tarjeta (U)SIM.

Si el servidor rechazara compartir el objeto X en el tercer intercambio este retornaría un NULL.

El sistema JCRE es muy importante en este protocolo, porque es éste el que autentica al servidor.

3.1.5. Datos compartidos.

Además de los aspectos de seguridad de plataforma y aplicaciones, un tercer aspecto debe ser tomado en cuenta. Todas las dificultades provienen de los datos compartidos dentro de la tarjeta. De hecho, la mayoría de las multiaplicaciones en las tarjetas inteligentes, a fin de tener sistemas que puedan cooperar entre sí y optimizar el uso de memoria, permiten compartir datos y servicios (por ejemplo compartir objetos entre aplicaciones). Además de este punto, hay una necesidad de una tarjeta con una gran política de seguridad para las aplicaciones. Un ejemplo pequeño podría ayudar a aclarar este punto. Cuando un proveedor de aplicaciones A decide compartir (o probablemente vender) algunos datos a un proveedor de aplicación B, éste solicita la garantía al proveedor B, el cual no es capaz de revender estos datos para que estén disponibles a algún otro proveedor. El tratamiento de los datos podría ser una preocupación comercial o de privacidad.

Una política obligatoria de seguridad es necesaria para solucionar el problema de re-compartir los objetos antes mencionados. La política de seguridad debería modelar los flujos de información entre las aplicaciones, las cuales deben reflejar relaciones confiables entre los participantes de un esquema aplicativo. Lo mejor para un sistema de política mandatoria es una política de aplicación multinivel.

Para reforzar esta política de seguridad podría hacerse de manera dinámica con un monitor de referencia (parte del sistema operativo de la tarjeta), el cual es invocado cada cierto periodo de tiempo como una referencia al objeto usado por la máquina virtual, o estáticamente para revisar que todo este correcto en la información del flujo del applet. Esta solución puede ser muy costosa en términos de memoria y tiempo de ejecución pues ambos son críticos en una tarjeta inteligente, ya que cada objeto podría ser etiquetado con su nivel y verificado para su validez implicando esto operaciones de lectura/escritura.

3.1.6. Integración al contexto GSM.

En este punto se tratará de explicar algunas advertencias que se deben de tener en el contexto GSM en específico.

Es importante señalar que se deben aclarar las suposiciones entre las entidades y sus respectivos applets.

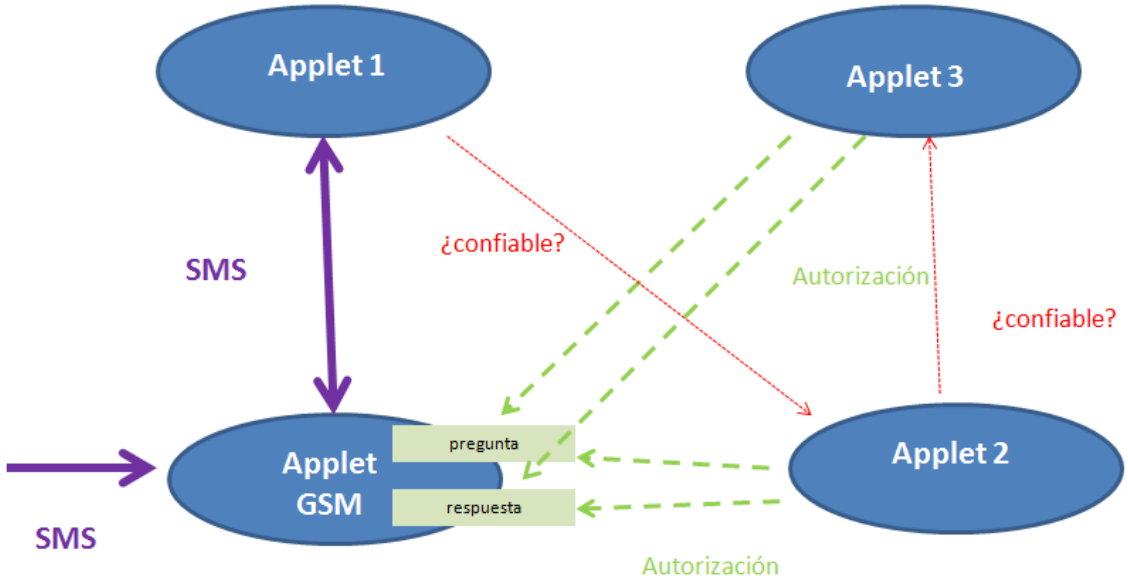


Figura 14. Diagrama relación entre las aplicaciones y el contexto GSM

De acuerdo a la figura 14, cuando un SMS llega al applet GSM, éste está ligado a un applet (applet 1). Los datos son almacenados en dos buffers, uno con privilegios de escritura (para los SMS de respuesta), y otro con privilegios de lectura (para los datos del SMS). Estos dos buffers pueden ser accesados por todos los applets. Así, si el applet 1 da el control a otro applet (applet2), este nuevo applet activo será capaz de leer los datos (problema de confidencialidad) en un buffer y escribir datos (problema de integridad) en el segundo. Si el applet 2 da el control a un tercer applet, este nuevo applet tendrá los mismos privilegios en el mismo buffer. Aquí nos encontramos con una situación crucial. Si un applet tiene que manipular algunos datos confidenciales vía SMS, esto debe ser de una manera muy cuidadosa. Antes de dar el control a otro applet, la situación debe ser analizada.

- Si el segundo applet no es un applet confiable, todos los buffers deben ser limpiados.
- Si el segundo applet es un applet confiable, una nueva pregunta surge ¿se debe dar el control al applet?

Cuando se usan paquetes no formateados, el desarrollador de applets deberá asegurarse que la información sensitiva está cifrada.

Un SMS sin formato no tiene una lista de direcciones. De hecho, todos los eventos suscritos al applet recibirán el paquete. Por lo tanto si el SMS contiene información sensitiva en claro, los diferentes applets podrán recibir el paquete. Por lo tanto si el SMS contiene información sensitiva en claro (sin cifrar), los diferentes applets podrán recibirla.

Con el empaquetamiento basado en el estándar GSM 03.48, nunca se confía en el campo del formato del encabezado para tomar una decisión relacionada con la seguridad y siempre se incluye el campo del tamaño de la seguridad a nivel de datos de usuario.
En el estándar 03.48, sólo los datos protegidos están totalmente cifrados, por lo tanto es muy peligroso usar información en los encabezados (porque podrían no estar cifrados) para tomar una decisión relacionada con la seguridad.

Nunca comenzará ninguna acción basada en el paquete recibido sin antes haberse verificado el SPI. Los bytes que indican los parámetros de seguridad SPI (Security Parameters Indicaton) están contenidos en cada SMS segurizado (basado en el estándar 03.48). Éste codifica las reglas de seguridad aplicadas en los mensajes y las mismas deben ser aplicadas en las respuestas. Después de la recepción del SMS es muy importante analizar los bytes del SPI, y verificar su valor. Todas las verificaciones de seguridad son realizadas por el applet GSM antes de dar los datos al applet destino. Es posible crear SMS con un SPI nulo. Al recibirlo el applet GSM no verificará nada pues el SPI es cero, entonces entregará los datos al applet de destino, si éste no verifica el valor del SPI, no podrá hacer la distinción entre un SMS normal y uno segurizado.

Cuando se generan acciones sensitivas basadas en paquetes, siempre se requiere un nivel máximo de seguridad para este paquete (verificación de contador, un checksum criptográfico y cifrado). Si un applet debe tomar una decisión importante basada en los paquetes, éste requiere un máximo nivel de seguridad para ese paquete.

3.2. Casos de uso.

A continuación un repaso general de las aplicaciones con comunicación a distancia existentes.

El *modo emulador de tarjeta*, que es cuando un dispositivo NFC se comporta como una tarjeta con comunicación a distancia, el cual es usado para aplicaciones bancarias, control de acceso o aplicaciones de transporte. Este es el caso de:

- Emisión de tickets usado por ejemplo en el acceso a los sistemas de transporte público.
- Pagos móviles, usados por ejemplo en pagos con tarjeta de crédito en tiendas o establecimientos mercantiles.
- Control de acceso físico usado principalmente en la casa u oficina.
- Acceso lógico, usado por ejemplo en el acceso a una computadora.
- Aplicaciones de lealtad usadas por ejemplo para dar puntos de recompensa en algún centro comercial.

El *modo punto a punto* es usado para el intercambio de datos entre 2 celulares o entre un celular y una computadora.

El *modo lector*, es usado por los “anuncios inteligentes”, es decir, para acceder a la información de un anuncio, en la parada de autobús o leer etiquetas RFID de carteleras para obtener las descripciones de las películas.

3.3. Arquitectura de la aplicación.

En la figura 15 se muestra la arquitectura del sistema NFC, para el modo emulador de tarjeta.

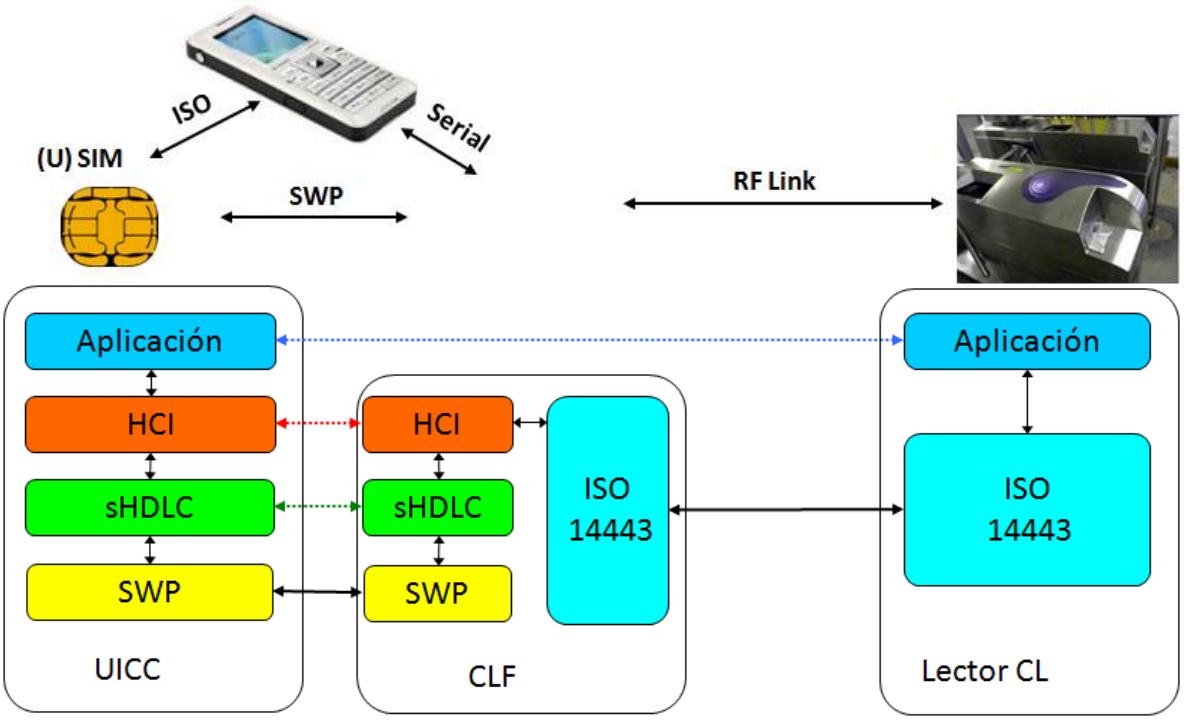


Figura 15. Arquitectura del sistema NFC (modo emulador de tarjeta).

En color naranja se encuentra el protocolo HCI (Host Controller Interface), que pertenece a la capa de red.
En color verde el protocolo sHDLC (Simplified High Level Data Link Control), que pertenece a la capa de enlace de datos.
En color amarillo se encuentra el protocolo SWP (Single Wire Protocol) perteneciente a la capa física.

3.3.1. Arquitectura HCI.

La figura 16 muestra las conexiones del Host Controller o CLF (Contactless Frontend) con otros Host en la capa HCP (Host Controller Protocol), usando mensajes HCI arriba de este para el intercambio de datos.

El CLF activa una o más RF según sea requerido por la UICC (Universal Integrated Circuit Card). La interface HCI tiene una colección de entradas para el intercambio de comandos, respuestas y eventos.

El intercambio de comandos APDU entre la entrada de la tarjeta y la entrada de la tarjeta RF, es hecho sobre el canal de comunicación (Pipe). Estos canales de comunicación (Pipes) son canales de comunicación lógica entre dos entradas (gates)
El estándar HCI define el comportamiento de la entrada dependiendo del tipo de aplicación (véase la figura 16), por ejemplo:

- Aplicación tipo A tales como aplicaciones bancarias, o aplicaciones de lealtad.
- Aplicación tipo B como aplicaciones de transporte, no sólo para la aplicación Mifare. En este caso la comunicación es hecha usando el modo CLT (Contactless tunneling), llamado túnel con comunicación a distancia, que está definido en la especificación técnica 102.613.

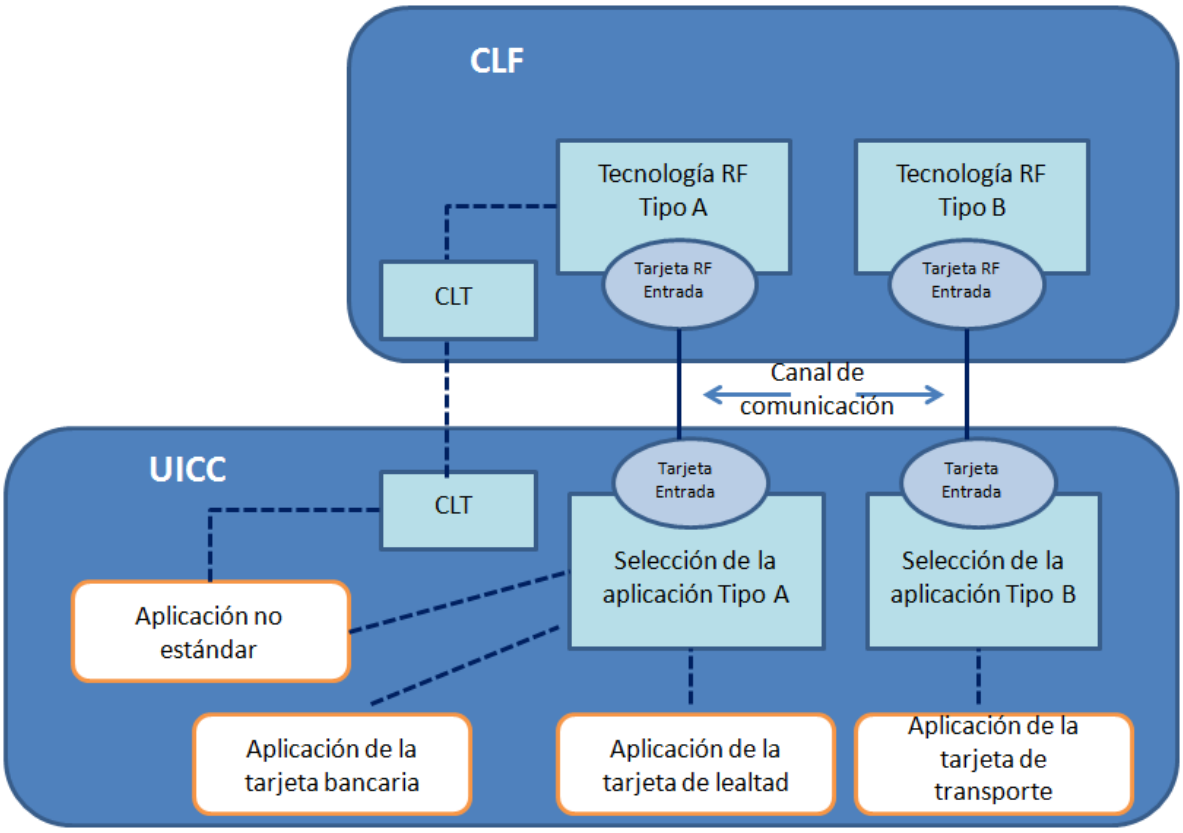


Figura 16. Arquitectura HCI.

3.3.1.1. HCI entradas y servicios.

Una puerta (gate) es un punto de entrada a un servicio que es operado dentro de un servidor.
Un servidor, en la infraestructura HCI (Host Controller Interface), es identificado por el Host Identifier codificado en 1 byte. Además de muchos servidores el sistema contiene siempre un controlador de servidores (Host Controller), el cual es la frontera de la comunicación a distancia que finaliza en el equipo móvil NFC.

El servidor puede ser por ejemplo, la UICC o la terminal.
El protocolo de servidor controlador, llamado HCP (Host Controller Protocol) habilita las entradas (gates) desde diferentes servidores para intercambiar mensajes. En la figura 17 se representa un diagrama del protocolo de servidor controlado.

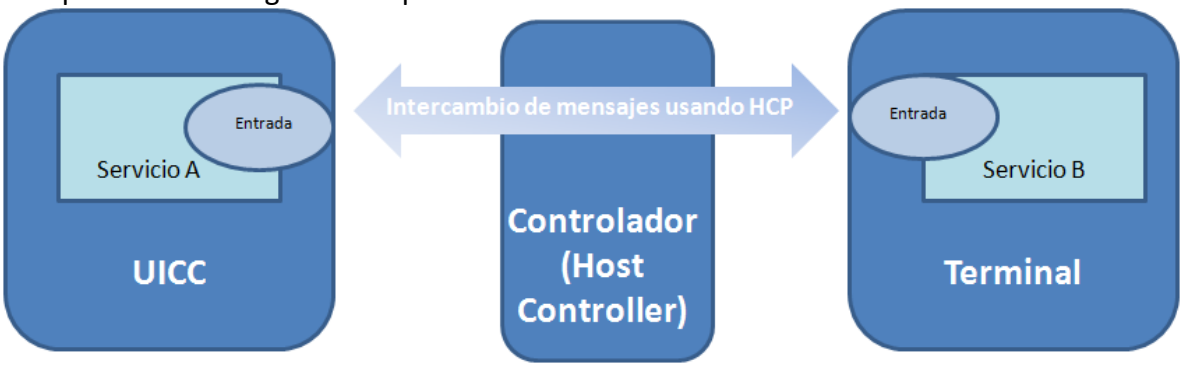


Figura 17. Diagrama HCP, intercambio de mensajes entre la (U)SIM y el terminal.

Existen dos tipos de puertas (gates):
Entradas administrativas (management gates), para la administración de un servidor de red.
Entradas genéricas, las cuales no están relacionadas con la administración de servidores de red. Únicamente los aspectos generales de esas entradas están definidas en el núcleo del HCI.
Una entrada (gate) es identificada por un identificador de entrada que está codificado en un byte y está definido en la especificación 102.622.

3.3.1.2. Canales de comunicación HCI.

Un pipe es un canal de comunicación lógico entre dos puertas (gates), identificado por su identificador codificado a un byte. Existen 2 tipos de pipes, estáticos o dinámicos.

Los pipes estáticos tienen un identificador fijo y está siempre disponible, éstos no necesitan ser creados y no pueden ser borrados. Los pipes estáticos son usados para conectarse a una entrada de servidor para la entrada CLF.

Los pipes dinámicos tienen identificadores alojados por el controlador de servidores. Éstos pueden ser creados y borrados. El estado puede también ser abierto o cerrado y éste permanece persistente aún cuando el servidor está apagado.

3.3.2. SHDLC.

La capa SHDLC (Simplified High Level Data Link Control) es la responsable de la transmisión libre de errores de datos entre nodos de red. Esta asegura que, los datos enviados a la siguiente capa han sido recibidos exactamente como los que se transmitieron. Es decir, consistentes o libres de errores, sin pérdidas y en el orden correcto. También, la capa SHDLC administra el control de flujo, lo cual asegura que los datos son transmitidos tan pronto como el receptor podría recibirlos.
SHDLC asegura una sobrecarga mínima en el manejo del control de flujo, detección y recuperación de errores. Si el flujo de datos se realiza en ambas direcciones, las estructuras de datos por sí mismas llevan toda la información requerida para asegurar la integridad de los datos. En la figura 18 se representa la estructura de datos SHDLC.

El concepto de ventana deslizante, para enviar múltiples estructuras, antes de recibir la confirmación que la primera estructura ha sido recibida correctamente. Esto significa que, los datos podrían continuar el flujo en situaciones donde podría haber intervalos de tiempo que den vueltas, sin detenerse a esperar una confirmación. El tamaño de la ventana deslizante está diseñada para 4 estructuras por default.

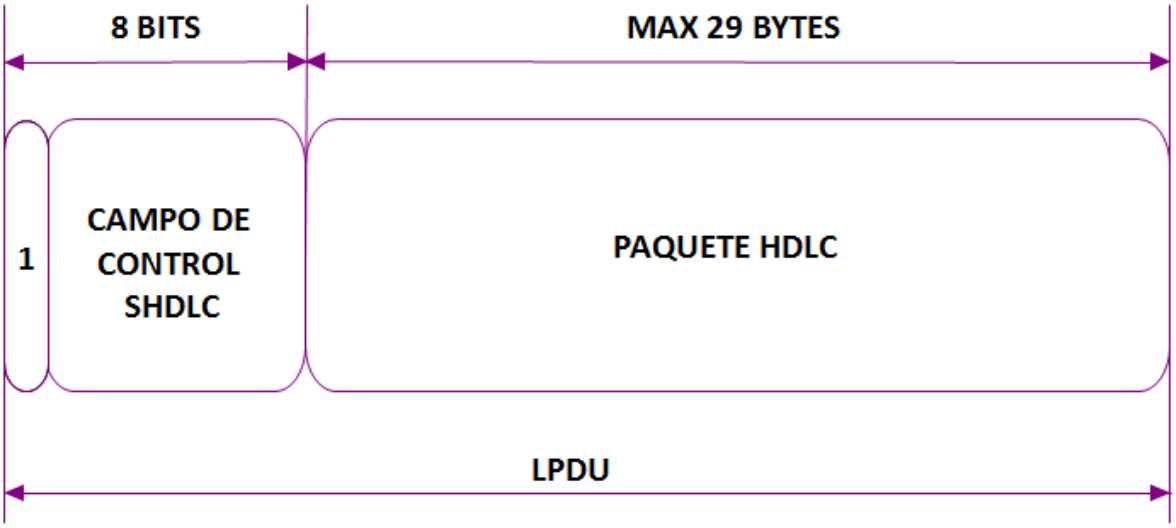


Figura 18. Diagrama SHDLC, estructura de datos para el intercambio de información libre de errores entre nodos de red.

3.3.3. Protocolo SWP.

Se encuentra en la capa física, establece una comunicación full duplex, a una velocidad máxima de 1.5 Mb/s. Los datos, el reloj y el control de los mensajes son enviados en el mismo PIN.

El estándar SWP se basa en la especificación TS 102.221 la cual menciona que el suministro de energía se debe dar a través del equipo móvil en contacto. La energía podría

ser enviada desde el campo de radio frecuencia o la batería y depende de la implementación en el equipo móvil.
El CLF informa a la UICC acerca del estatus de la batería (disponible o no). Esto es la responsabilidad de la UICC ajustar su consumo de acuerdo a los requerimientos estándares. En la figura 19 se indica el PIN dedicado al SWP.

Figura 19. Pines de la (U)SIM incluyendo PIN SWP

3.3.4. Comunicación entre un terminal NFC y la (U)SIM.

Cuando la UICC está encendida, ésta comienza la comunicación SWP hacia el CLF y detecta, vía el intercambio de un ID de sincronización y un ID de sesión, si ésta tuvo una conexión previa al CLF o no. Si la conexión CLF-UICC no fue establecida anteriormente, la UICC configura el CLF con datos individuales de la aplicación, por ejemplo la UID, el tipo de protocolo NFC (por ejemplo ISO 14443 A o B) y otros servicios disponibles vía la interface de comunicación a distancia. De otra manera si la conexión CLF-UICC ya había sido establecida con anterioridad, no se corre un nuevo proceso de configuración, debido a que las conexiones virtuales vía la interface SWP han sido almacenadas.
Si un equipo móvil tiene NFC habilitado y se acerca a una terminal con comunicación a distancia, la secuencia de comunicación es iniciada como se muestra en la figura 20.

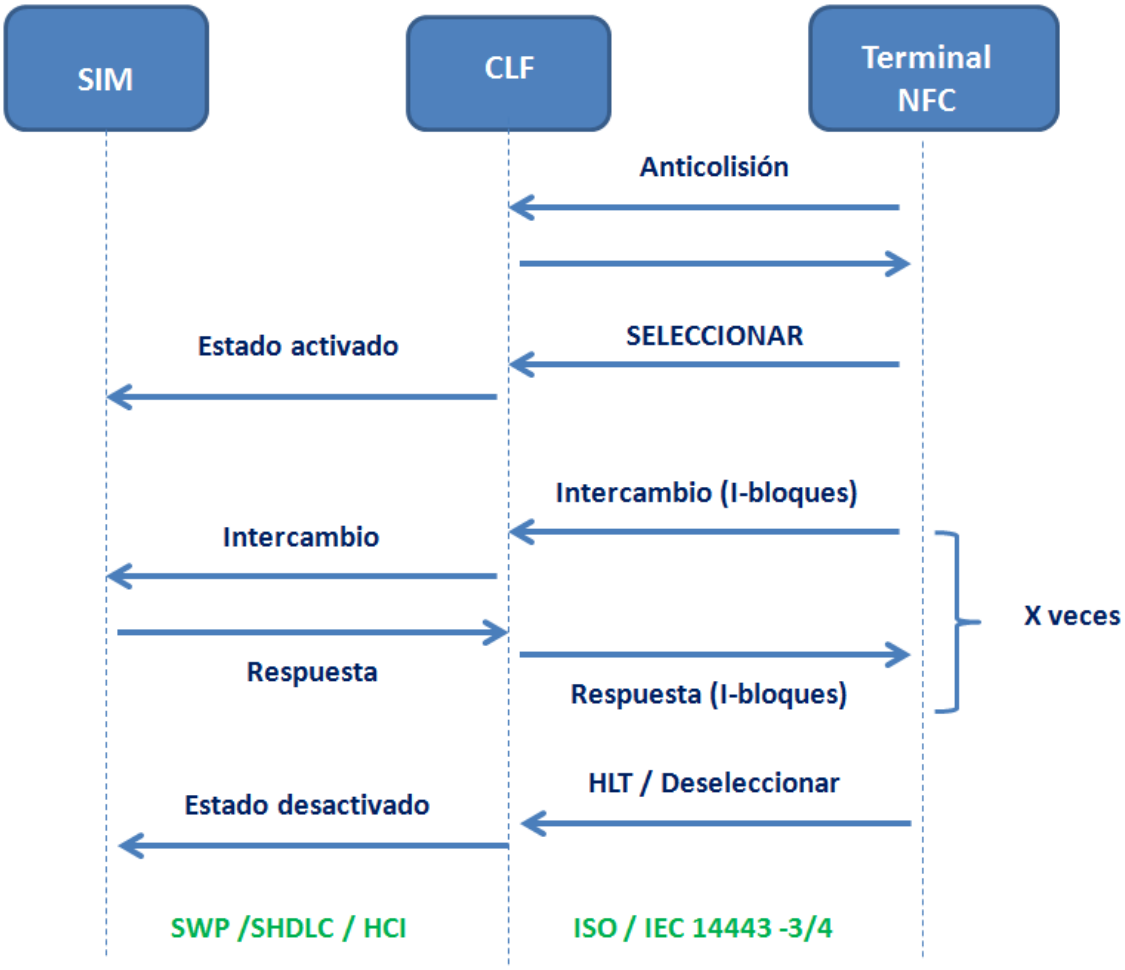


Figura 20. Ciclo de comunicación entre el terminal y la tarjeta (U)SIM a través del CLF

En el modo emulador de tarjeta, la terminal con comunicación a distancia activa el CLF del equipo móvil, el cual despierta a la UICC llevándola al estado de activado.
Después de la activación exitosa de la pila SWP, la terminal es capaz de enviar comandos APDU vía NFC, los cuales son enviados de la UICC al SWP. Los datos de respuesta son enviados a la terminal con comunicación a distancia que pueden después enviar nuevos comandos APDU.
Cuando la comunicación entre la terminal y el equipo móvil es finalizada, la terminal envía un comando para detener o terminal la selección vía NFC, el cual se convierte en el estado de desactivación.

3.3.5. Equipos móviles con NFC.

Un equipo móvil NFC es capaz de comunicarse con un lector/terminal, sin la necesidad de hacer contacto físico.
La comunicación a distancia es tratada por un dispositivo embebido en el equipo móvil, llamado CLF.
El CLF está a cargo de manejar la comunicación ISO 14.443 con el terminal/lector, y sólo esa comunicación. Todos los datos intercambiados con el terminal son después transmitidos a la tarjeta para su ejecución utilizando el protocolo SWP (Single Wire Protocol).

La línea SWP está físicamente conectada a la tarjeta dentro del equipo móvil. El estándar ISO 14.443 describe la comunicación entre el CLF y el manejo del lector/terminal con comunicación a distancia. A continuación se detallarán los elementos que forman parte de las transacciones de comunicación a distancia:

El primer elemento es el "elemento seguro", el cual usualmente es una tarjeta (U)SIM. Dicha tarjeta (U)SIM contiene aplicaciones de comunicación a distancia y un sistema operativo. La tarjeta (U)SIM contiene también embebidos todos los estándares requeridos para la comunicación con las aplicaciones. Esto incluye las capas de comunicación de Global Platform Amendment C, HCI y SWP. La (U)SIM también contiene para cada aplicación sus parámetros de comunicación a distancia, usados durante el protocolo de incialización por el CLF con el lector a comunicación a distancia.

La tarjeta (U)SIM tiene sus 5 contactos regulares, más uno adicional que está conectado al CLF. Esta línea es usada para una comunicación interna con el CLF.
El CLF mencionado con anterioridad, que se puede denominar también NFC chipset, maneja la comunicación ISO con el lector de comunicación a distancia.
Éste es también energizado por el equipo móvil, o podría trabajar también en modo batería apagada, cuando el equipo móvil este apagado. El CLF es encendido en este caso por el campo que está siendo generado por el lector de comunicación a distancia.
La (U)SIM está conecta al CLF por la línea del SWP. En el modo de batería apagada, el CLF está a cargo de proveer la suficiente energía, para que la (U)SIM sea capaz de procesar las transacciones a distancia. El CLF está conectado a una bobina de antena, asegurándose la detección oportuna del campo de radio frecuencia generado por el lector de comunicación a distancia.

En la figura 21 se muestran los elementos anteriormente descritos.

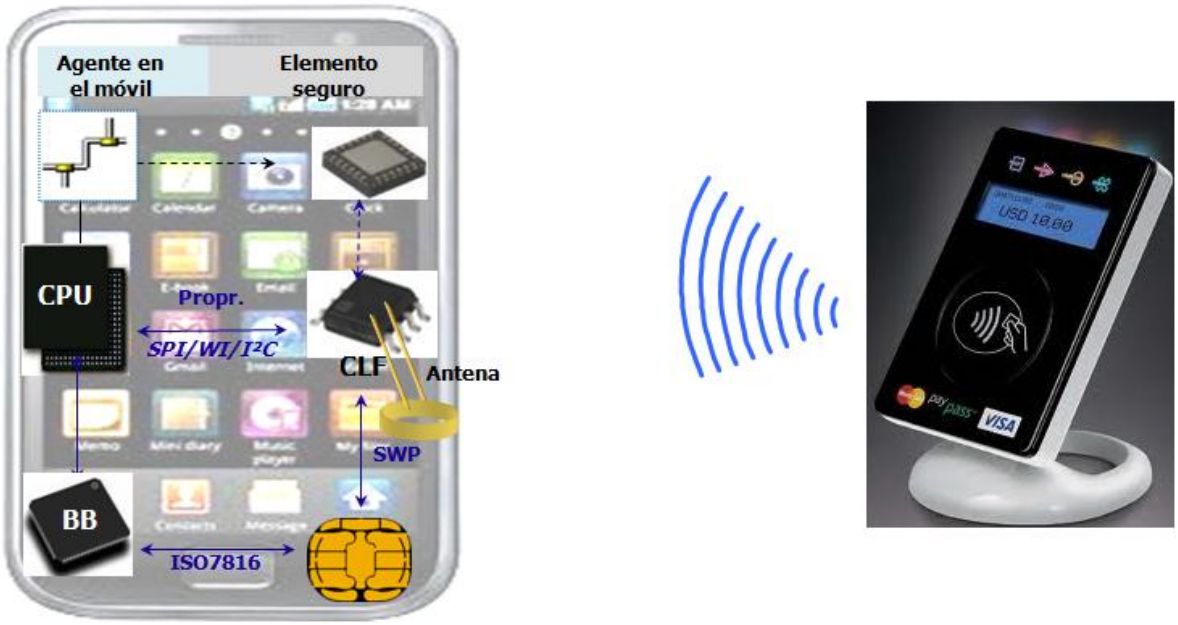


Figura 21. Elementos de un equipo móvil con tecnología NFC

3.3.5.1. Comunicación tipo A.

Todos los pasos son iniciados por el terminal/lector usando los comandos ISO. La fase de la petición es iniciada por el comando denominado REQA que indica que quiere iniciar la comunicación con la tarjeta (U)SIM. La tarjeta (U)SIM envía el ATQA (answer to request). La respuesta contiene el tamaño del identificador de la tarjeta (U)SIM, tamaño que será usado durante el ciclo de anticolisión. La anticolisión es el siguiente paso, y consiste en revisar todas las tarjetas en el campo de radio frecuencia, y seleccionar sólo uno. La tarjeta responde al ciclo de anticolisión con su identificador único denominado UID.

Después el terminal selecciona explícitamente la tarjeta (U)SIM con su UID, usando un comando de selección (SELECT command). Ya se ha comentado de la selección de la tarjeta durante la fase de inicialización de la comunicación a distancia, más no se ha hablado de la selección de una aplicación, la cual podría realizarse cuando comienza la transacción. La tarjeta seleccionada confirma esta selección regresando el acknowledge de selección SAK (Select Acknowledge). El SAK contiene información para determinar si la tarjeta es compatible con la parte 4 de la especificación ISO, o si ésta implementa un protocolo propietario, por ejemplo Mifare. Si la tarjeta es compatible con la parte 4, antes debe ser capaz de comunicarse con el terminal, la tarjeta comienza la etapa de activación, especificada en la parte 4 del estándar. En la figura 22 se representa el protocolo de comunicación tipo A.

La activación es iniciada por el requerimiento del comando ATS (ATS command). La tarjeta responde con su ATS (Answer to Select). El ATS es muy similar al ATR (Answer to Reset) en

el modo de comunicación con contacto. Durante esta activación, el lector/terminal y la tarjeta intercambian y acuerdan sus respectivas configuraciones de comunicación. El terminal podría negociar otras configuraciones, enviando un comando PPS justo después de la activación.
En esta etapa, el lector/terminal y la tarjeta están listos para comunicarse. Éstos intercambian comandos aplicativos y datos, para ejecutar la transacción aplicativa.

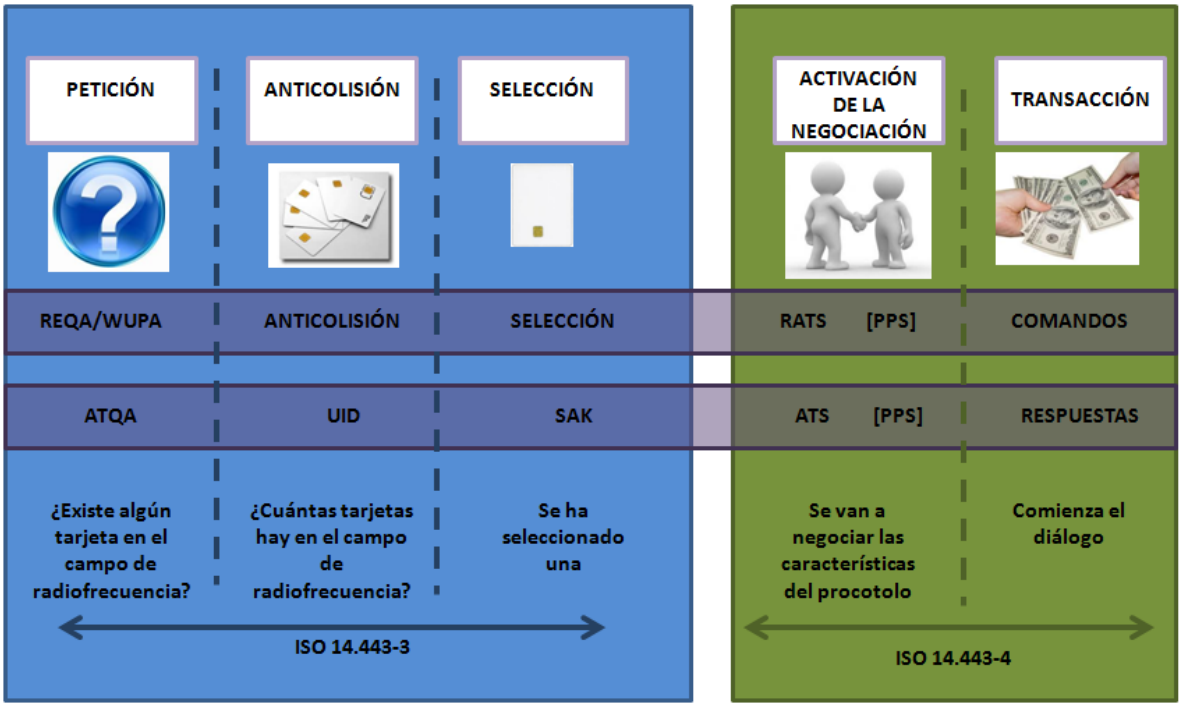


Figura 22. Protocolo de comunicación tipo A

3.3.5.2. Comunicación tipo B.

Para el tipo B, la fase de requerimiento es iniciada por el comando REQB, indicándole que necesita comunicación con la tarjeta. Cualquier tarjeta con chip de proximidad PICC (Proximity Integrated Circuit Card) presente en el campo responderá con su ATQB, o el ATS (Answer to Request). La respuesta contiene el identificador del chip y parámetros adicionales. Como en el tipo A, un proceso de anticolisión es iniciado por el lector/terminal, para revisar si hay varias tarjetas en el campo de radio frecuencia, y elegir uno. Después el terminal selecciona explícitamente la tarjeta con su identificador, usando un comando denominado ATTRIB. La tarjeta seleccionada confirma su selección regresando una respuesta a ATTRIB. En esta etapa, el lector/terminal y la tarjeta están listos para comunicarse. Éstos intercambian comandos aplicativos y datos, para ejecutar la transacción aplicativa. A continuación se muestra el protocolo de comunicación tipo B en la figura 23.

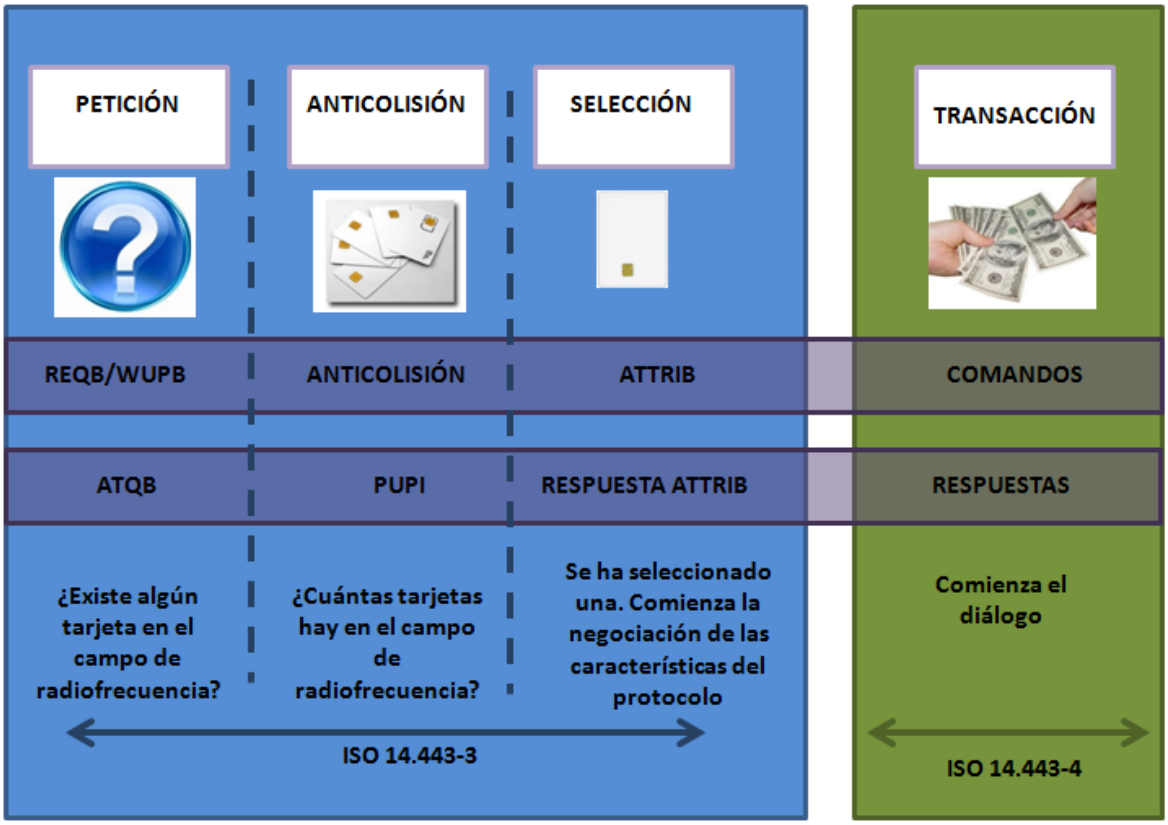


Figura 23. Protocolo de comunicación tipo B

3.4. Actualización de una SIM card vía OTA.

El estándar 3GPP TS 03.48 establece la estructura de los paquetes seguros en un formato general y las implementaciones usando los short message service point to point (SMS-PP)

Establece, además que el intercambio de paquetes de manera segura se debe realizar entre una red GSM, UMTS, etc. y una entidad en la SIM.

La aplicación emisora prepara el mensaje que se enviará a la entidad receptora del mensaje, con la indicación de seguridad que debe aplicarse al mensaje.

La entidad emisora del mensaje prepara el encabezado de seguridad (encabezado de comando) al mensaje de la aplicación. Este después aplica la seguridad requerida a parte del encabezado de comando y a todos los mensajes de aplicación, incluyendo todos los octetos de relleno. La estructura resultante es aquí referida como un paquete de comandos seguro.

Bajo circunstancias normales, la entidad receptora recibe los paquetes de comandos y los ejecuta de acuerdo a los parámetros de seguridad indicados en el encabezado de comando. La entidad receptora subsecuentemente envía el mensaje de aplicación a la aplicación receptora indicándole la seguridad que fue aplicada.

Si todo es correcto en el encabezado de comando, la entidad receptora creará un paquete de respuesta (seguro). El paquete de respuesta consiste de un encabezado de seguridad (encabezado de respuesta) y opcionalmente, datos específicos de aplicación provistos por la aplicación receptora. Tanto el encabezado de respuesta y los datos específicos de aplicación son segurizados con los mecanismos indicados en el paquete de comandos recibidos. El paquete de respuesta se le regresará a la entidad emisora.

En algunas circunstancias la seguridad relacionada al error podría ser detectada por la entidad receptora. En tales circunstancias la entidad receptora tendrá un comportamiento de acuerdo a las siguientes reglas:

1. Nada será enviado a la aplicación receptora,
2. Si la entidad emisora no requiere respuesta (en el encabezado del comando) la entidad receptora descarta el paquete de comandos y ninguna acción posterior es tomada.
3. Si la entidad emisora no requiere una respuesta de la entidad receptora, puede ambiguamente determinar cuál es la causa del error, la entidad receptora creará un paquete de respuesta indicando la causa del error. Este paquete de respuesta será segurizado de acuerdo a la seguridad indicada en el comando de paquete recibido.
4. Si la entidad emisora no requiere una respuesta y la entidad receptora no puede determinar que ha causado el error, la entidad receptora enviará un paquete de respuesta indicando que un error indefinido ha sido detectado. Este paquete de respuesta es enviado sin ninguna seguridad.
5. Si la entidad receptora recibe un encabezado de comando no reconocible, el paquete de comando será descartado y no se tomará ninguna otra acción.

En la figura 24 se muestra la arquitectura general para realizar una actualización vía interface aérea.

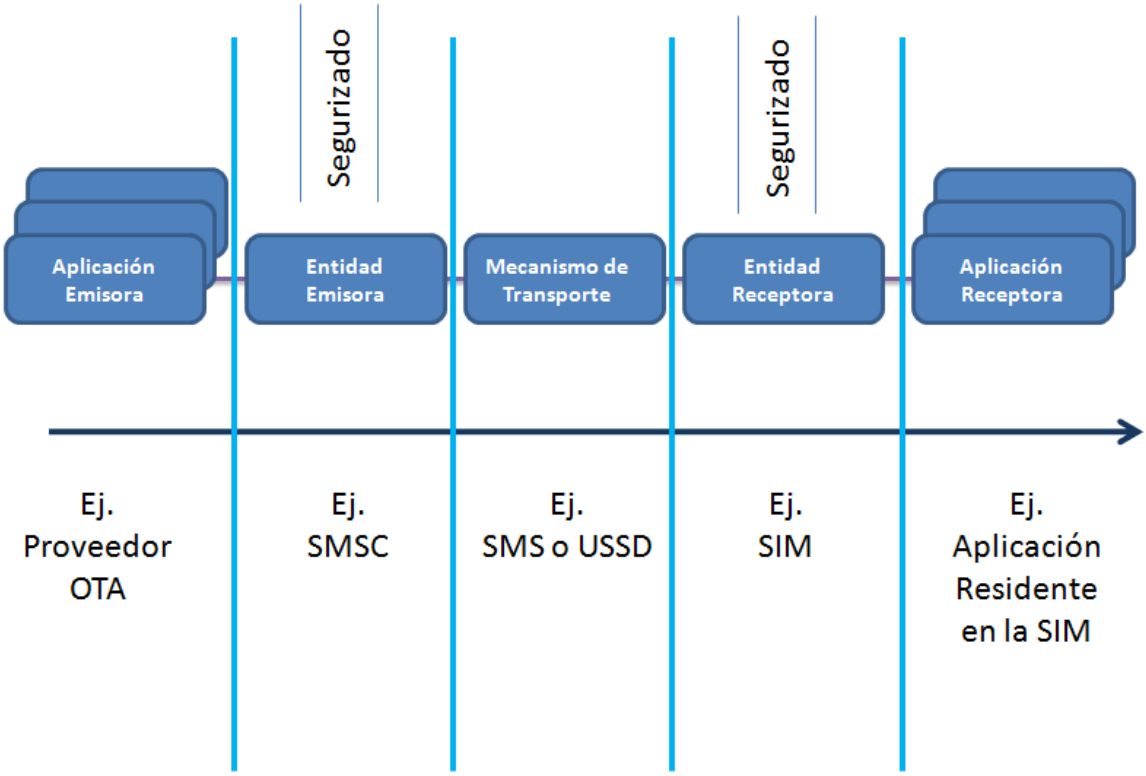


Figura 24. Arquitectura general para la actualización OTA(Over The Air) de una tarjeta.

3.4.1. Estructura generalizada de la estructura de paquetes.

Los paquetes de comandos y respuestas tienen la misma estructura, la cual consta de un encabezado de seguridad variable dentro de una base de longitud variable. Este modelo, está hecho de una doble etiqueta TLV (Tag, Length, Value), etiqueta, longitud y valor de la estructura. El encabezado del comando precede al dato segurizado en el comando empaquetado y es de longitud variable. El comando empaquetado debe ser estructurado de acuerdo a la tabla 20.

Elemento	Longitud	Observaciones
Identificador del comando empaquetado (CPI Command Packet Identifier)	1 octeto	Identifica que el bloque de datos es el paquete de comando segurizado.
Longitud del comando empaquetado(CPL Command Packet Lenght)	variable	Este indicará el número de octetos desde el identificador del encabezado del comando hasta el final del dato segurizado, incluyendo cualquiera de los complementos de los octetos requeridos para cifrar.
Identificador del comando del encabezado(CHI Command Header Identifier)	1 octeto	Identifica el comando del encabezado

Longitud del comando del encabezado(CHLCommand Header Lenght)	variable	Indicará el número de octetos desde el SPI hasta el final del RC (checksum de redundancia)/CC (checksum criptográfico)/DS (firma digital).
Indicador de parámetro de seguridad(SPI Security Parameter Indicator)	2 octetos	
Identificador de la llave de cifrado(KIc Ciphering Key Identifier)	1 octeto	Llave y algoritmo definido para cifrado
Identificador de la llave de firma o checksum criptográfico (KID Key Identifier)	1 octeto	Llave y algoritmo definido para RC (checksum de redundancia)/CC (checksum criptográfico)/DS (firma digital).
Referencia de la aplicación toolkit (TAR Toolkit Application Reference)	3 octetos	Código que depende de la aplicación
Contador (CNTR Counter)	5 octetos	Detección de respuesta y contador de secuencia de integridad
Contador de complementos(PCNTR Padding Counter)	1 octeto	Indica el número de octetos completados usados para cifrar al final del dato segurizado
Verificador de redudancia (RC Redudancy Check) Checksum criptográfico (CC Crytographic Checksum) o firma digital(DS Digital Signature)	variable	La longitud depende del algoritmo. Un valor típico es 8 octetos si se usa y para firma digital podría ser 48 ó más octetos; el mínimo debería ser 4 octetos.
Dato segurizado	variable	Contiene los mensajes de aplicación segurizados y el posible complemento de los octetos usado para el cifrado.

Tabla 20. Estructura de un comando empaquetado.

CPI	**CPL**	**CHI**	**CHL**	**SPI**	**KIC**	**KID**	**TAR**	**CNTR**	**PCNTR**	**RC/CC/DS**	**Dato segurizado con complemento**
								Nota 1	Nota 1	Nota 1	Nota 1
	Nota 3		Nota 3	Nota 2	Nota 2	Nota 2	Nota 2	Nota 2	Nota 2		Nota 2

Tabla 21. Representación lineal de un paquete de comandos.

De acuerdo a la tabla 21 las siguientes notas deben ser tomadas en cuenta:

Nota 1: Estos campos están incluidos en los datos para ser cifrados si dicha característica está indicada en el encabezado de seguridad

Nota 2: Estos campos están incluidos en el cálculo de RC/CC/DS

Nota 3: Parte o todos estos campos podrían también ser incluidos en el cálculo de RC/CC/DS, dependiendo de la implementación.

Si el cifrado está indicado, en principio el RC/CC/DS será calculado como se indica en la nota 2 y después el cifrado será aplicado, como se indica en la nota 1.

Si el SPI indica que el campo específico no debe ser usado, la entidad emisora colocará el contenido en cero y la entidad receptora ignorará el contenido.

Si el SPI indica que el RC/CC o DS está presente en el encabezado del comando, el RC/CC/DS tendrá longitud cero.

Si el complemento del contador está en cero, éste indicará que no hay complemento en los octetos y el complemento no será necesario.

3.4.1.1. Codificación del SPI.

Los SPI1 y SPI2 (indicadores de parámetros de seguridad) se codifican de acuerdo a las tablas 22 y 23.

Primer Octeto

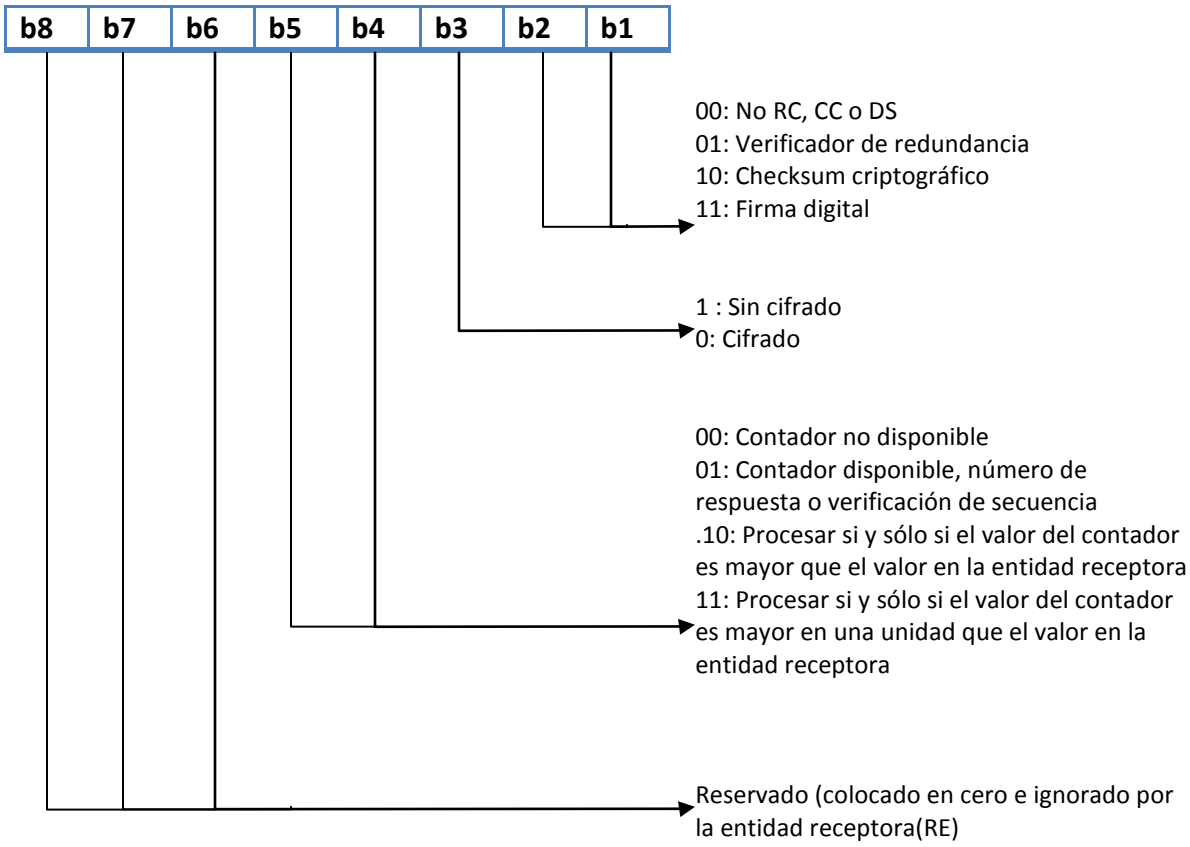


Tabla 22. Codificación del SPI1 (indicación de parámetros de seguridad).

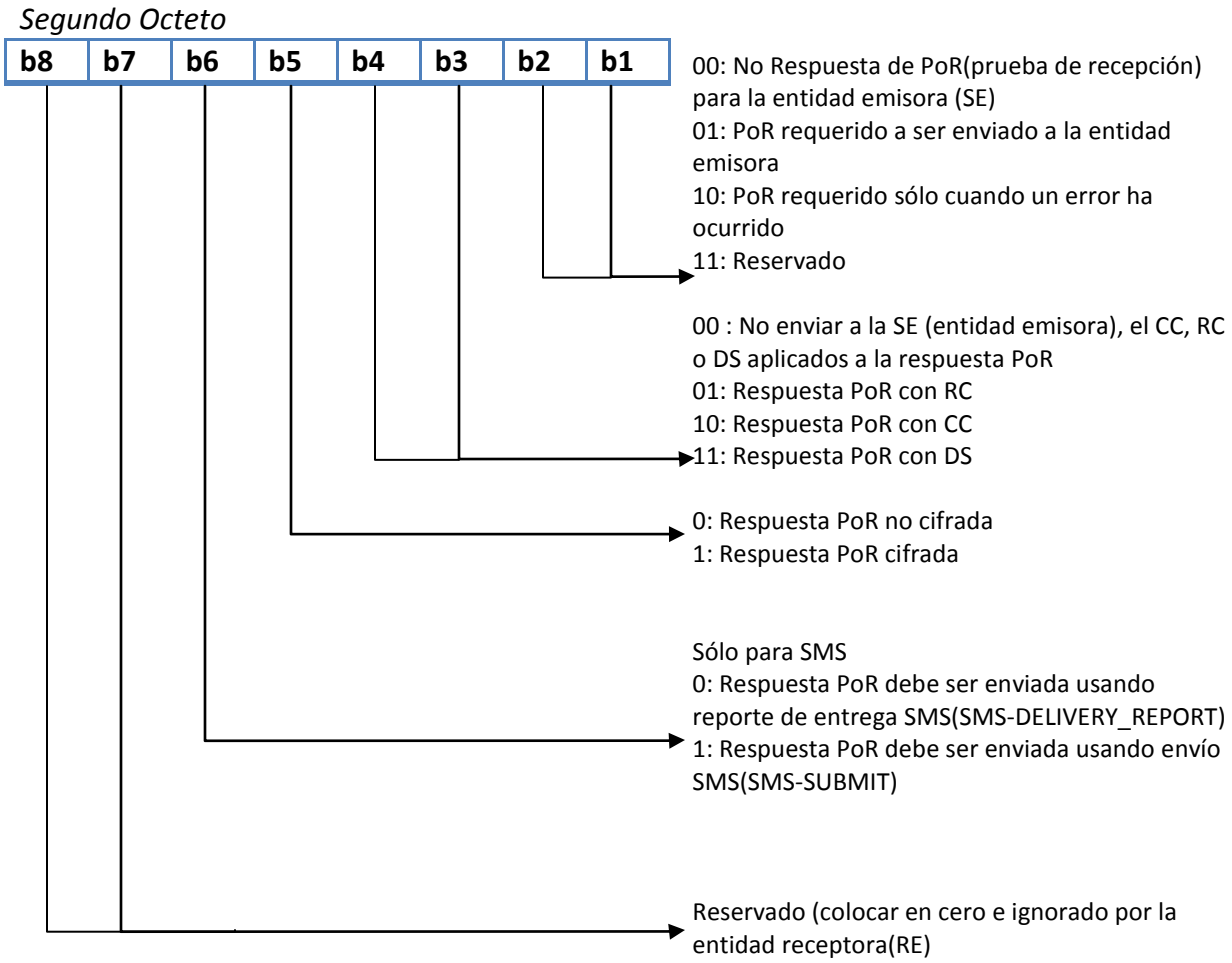


Tabla 23. Codificación del SPI2 (indicación de parámetros de seguridad).

3.4.1.2. Codificación de KIC.

La KIC (llave de cifrado) se codifica de acuerdo a la tabla 24.

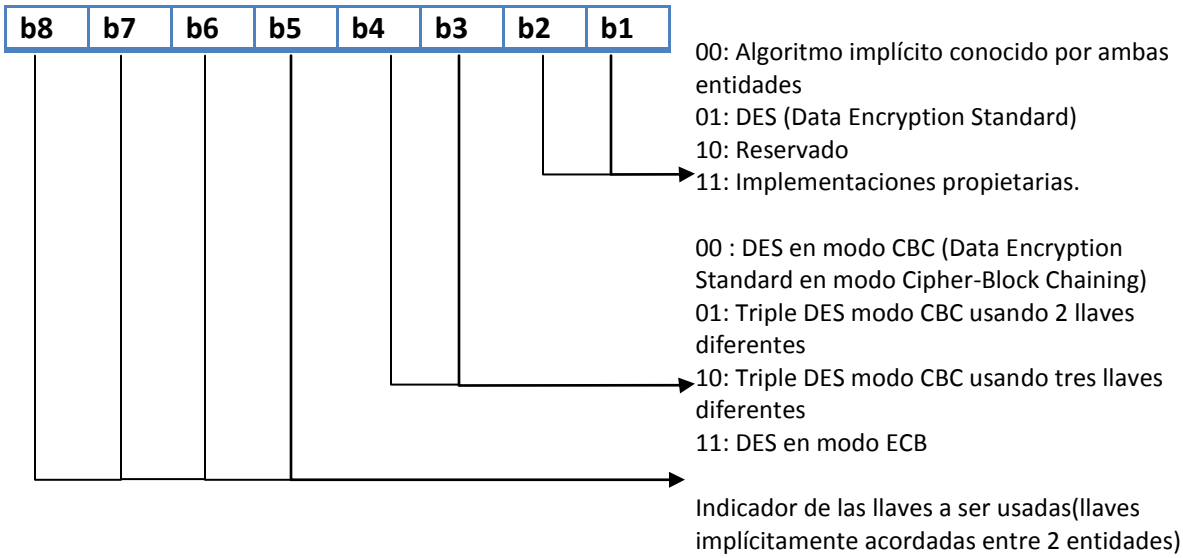


Tabla 24. Codificación de la llave de cifrado (KIC).

DES (Data Encryption Standard) es un algoritmo especificado en ISO 8731-1. DES en modo CBC (Cipher-Block Chaining) y ECB (Electronic Codebook) está descrito en el estándar ISO/IEC 10116.

Si el indicador de la llave a usar refiera a una versión de un juego de llaves de una plataforma abierta, el algoritmo a ser usado con la llave será el algoritmo asociado a esta llave (descrito en la especificación de la plataforma abierta)

3.4.1.3. Codificación de KID.

La KID (llave de firma o checksum criptográfico) se codifica de acuerdo a la tabla 25.

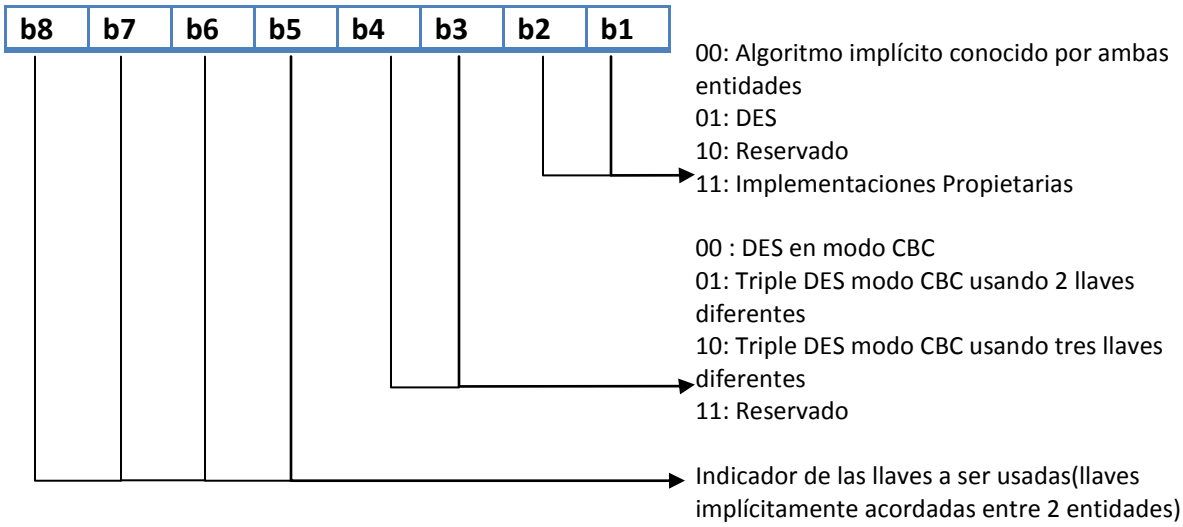


Tabla 25. Codificación de la llave de firma o checksum criptográfico (KID).

Manejo del contador

Si en el primer byte del SPI(Security Parameters Indicaton) los bits 4 y 5 están colocados en ’00´, esto significa que el contador no está disponible y debe ser ignorado por la RE (Entidad Receptora) y la RE no debe actualizar el contador.

Si el bit 5 del primer byte del SPI es igual a 1, entonces las siguientes reglas deberán ser aplicadas al manejo del contador, con el objetivo de prevenir ataques de réplica y sincronización:

- La entidad emisora (SE) coloca el nuevo valor del contador para realizar un próximo envío y éste será incrementado.

- La entidad receptora (RE) actualizará el contador uno arriba de su próximo valor recibido por el paquete de comando después de la revisión de la seguridad correspondiente (ejemplo RC/CC/DS y verificación de CNTR) hayan sido verificados exitosamente.

El próximo valor del contador es el recibido en el mensaje entrante.

- Cuando el valor del contador alcanza su máximo valor el contador se bloquea.

4. Implementación y pruebas de usuario.

4.1. Implementación.

Para la realización de esta tarjeta (U)SIM con control de acceso y monedero, se siguieron los siguientes pasos:

- Creación del sistema de archivos

- Actualización vía OTA de la (U)SIM

- Autenticación a la red

- Aplicación de control de acceso y monedero

4.2. Creación del sistema de archivos.

La creación del sistema de archivos deberá realizarse con base al estándar ETSI TS 131 102. Dichos archivos se crean de la siguiente manera:

1. Creación del directorio raíz (3F00 Dir).
2. Creación del directorio que contiene el archivo (7F10 Telecom, 7F20 GSM, etc).
3. Creación del archivo (6F07 IMSI).

Una vez creados los directorios, el archivo se debe crear con las condiciones de acceso y codificación dictadas por el estándar ETSI TS 131 102. En la figura 25 se muestran las condiciones de acceso, estructura, tamaño, identificador, etc., correspondientes al archivo IMSI.

Identificador: '6F07'	Estructura: transparent	Mandatorio
Tamaño del archivo: 9 bytes	**Frecuencia de actualización: baja**	
Ruta: 7F10		

Condiciones de acceso:

LECTURA ADM1, ADM2

ACTUALIZACIÓN ADM1, ADM2

INVALIDAR ADM1, ADM2

REHABILITAR ADM1, ADM2

Tamaño bytes	Descripción	M/O	Longitud
1	Longitud del IMSI	M	1 byte
2 al 9	IMSI	M	8 bytes

Figura 25. Características estándar del archivo IMSI.

En la tabla 26 se muestran los comandos del estándar ETSI TS 102 222, para el manejo de archivos.

Comando	Clase	Instrucción
CREAR ARCHIVO	"00" / "A0"	"E0"
BORRAR ARCHIVO	"00" / "A0"	"E4"
DESACTIVAR ARCHIVO	"00" / "A0"	"04"
ACTIVAR ARCHIVO	"00" / "A0"	"44"
TERMINAR DF	"00" / "A0"	"E6"
TERMINAR EF	"00" / "A0"	"E8"
TERMINAR EL USO DE LA TARJETA	"00" / "A0"	"FE"
ACTUALIZAR EL TAMAÑO DEL ARCHIVO	"80" / "A0"	"D4"

Tabla 26. Comandos estándar para el manejo de archivos.

Para proceder a la creación de un archivo, es indispensable crear primero su directorio correspondiente, tal como se muestra en la tabla 27. Esta creación se hace en base al estándar ETSI TS 102 222.

Codificación	Valor	Significado
Instrucción	E0	Instrucción reservada para la creación de archivos o directorios
Parámetro 1	00	Identificador y parámetros del archivo colocados como dato
Parámetro 2	00	Identificador y parámetros del archivo colocados como dato
Longitud del comando	38	Longitud del comando subsecuente codificado en hexadecimal 38=56 bytes
Etiqueta de la plantilla FCP	62	Parámetros de archivos(FCP File Control Parameters)
Longitud	36	Longitud del comando subsecuente codificado en hexadecimal 36=54 bytes
Etiqueta del descriptor del archivo	82	Etiqueta reservada
Longitud del identificador del archivo	02	Está longitud no es del parámetro siguiente, como en casi todos los comandos, es solamente del identificador del archivo
Descriptor del archivo	78	De acuerdo a la tabla 4 del estándar ETSI TS 102 222 es un archivo compartido, y es un DF (Directory File)
Byte de codificación de dato	21	Valor fijo “21”
Etiqueta del identificador del archivo	83	Etiqueta reservada
Longitud del identificador del archivo	02	
Identificador del archivo	7F20	Directorio GSM 7F20
Información del estado de ciclo de vida	8A	Etiqueta reservada
Longitud de la información del estado del ciclo de vida	01	
Información del estado del ciclo de vida	05	De acuerdo a la tabla 5 del estándar ETSI TS 102 222, se encuentra en estado operacional y activado
Atributos de seguridad	AB	Atributo de seguridad expandido, es decir todas las condiciones deben ser colocadas de manera explícita
Longitud de los atributos de seguridad	22	
Atributos de seguridad (condiciones de acceso)	50108A40804068 3010A08A0107A0 18A40683010D95 01088401A89683 010B95019000	Condiciones de acceso a ser codificadas de manera independiente entre cada implementación (proveedor de tarjetas (U)SIM)
Etiqueta del tamaño total del archivo	81	Etiqueta reservada
Longitud	03	
Longitud en bytes	007635	Tamaño en bytes 30261
Etiqueta del status del PIN	C6	Etiqueta reservada
Estado del PIN	00	Codificado en base al estándar ETSI TS 102 221.

Tabla 27. Creación del directorio 7F20 (GSM).

Una vez creado el directorio se procede a la elaboración de los archivos que estarán contenidos en el directorio, como por ejemplo el IMSI, para lo cual se debe de seleccionar primero el directorio recientemente creado, y después proceder a la creación del archivo. En la tabla 28 se muestra la creación del archivo 6F07 (IMSI).

Codificación	Valor	Significado
Instrucción	E0	Instrucción reservada para la creación de archivos o directorios
Parámetro 1	00	Identificador y parámetros del archivo colocados como dato
Parámetro 2	00	Identificador y parámetros del archivo colocados como dato
Longitud del comando	45	Longitud del comando subsecuente codificado en hexadecimal 38=56 bytes
Etiqueta de la plantilla FCP	62	Parámetros de archivos(FCP File Control Parameters)
Longitud	43	Longitud del comando subsecuente codificado en hexadecimal 36=54 bytes
Byte de codificación de dato	21	Valor fijo “21”
Etiqueta del identificador del archivo	83	Etiqueta reservada
Longitud del identificador del archivo	02	
Identificador del archivo	6F07	Creación del archivo IMSI
Información del estado de ciclo de vida	8ª	Etiqueta reservada
Longitud de la información del estado del ciclo de vida	01	
Información del estado del ciclo de vida	03	De acuerdo a la tabla 5 del estándar ETSI TS 102 222, se encuentra en estado de inicialización
Atributos de seguridad	AB	Atributo de seguridad expandido, es decir todas las condiciones deben ser colocadas de manera explícita
Longitud de los atributos de seguridad	2ª	
Atributos de seguridad (condiciones de acceso)	8A40683010A4068301019501 00A40683010A950108A40683 010B9501080A95010880010A A01800111A01	Condiciones de acceso a ser codificadas de manera independiente entre cada implementación (proveedor de tarjetas (U)SIM)
Etiqueta del tamaño total del archivo	80	Etiqueta reservada
Longitud	02	
Longitud en bytes	0009	Tamaño en bytes 9
Etiqueta del identificador corto del archivo	88	Etiqueta reservada
Longitud del identificador corto del archivo	01	

Identificador corto del archivo	38	Identificador 38
Etiqueta propietaria A5 u 85	A5	Etiqueta que establece cada fabricante de (U)SIM
Longitud	03	
Dato	C101FF	De acuerdo con la sección 6.3.2.2.2 del estándar ETSI TS 102 222

Tabla 28. Creación del archivo IMSI 6F07.

Por último, una vez creados tanto el directorio como el archivo, éste último se debe inicializar con su valor definitivo, por lo que se deben seleccionar tanto directorio como archivo, antes de actualizar su valor. A continuación se ilustra el script que actualiza el valor del archivo IMSI.

'Script: Seleccionar directorio GSM 7F20
A0 A4 0000 02 7F20

'Selección del archivo IMSI-6F07
A0 A4 0000 02 6F07

'Actualización del archivo IMSI-6F07
A0 D6 0000 09 $IMSI

En resumen, la creación del archivo IMSI se realiza de la siguiente manera:

'Script: Creación del directorio 7F20
00 E0 0000 38
62368202782183027F108A0105AB2250108A408040683010A08A0107A018A40683010D9
501088401A89683010B95019000 8103007635C600

'Script: Seleccionar directorio GSM 7F20
A0 A4 0000 02 7F20

'Script: Creación del archivo IMSI 7F20
00 E0 0000 45
624382024121830 26F078A0103AB2A8A40683010A406830101950100A40683010A95010
8A40683010B9501080A95010880010AA01800111A0180020009880138A503C101FF

'Selección del archivo IMSI-6F07
A0 A4 0000 02 6F07

'Actualización del archivo IMSI-6F07
A0 D6 0000 09 $IMS

En la tabla 29, se ilustran los archivos a ser creados en la tarjeta acorde a las necesidades del operador.

Ruta / Id	Nombre	No de registros	Tamaño del registro	Tamaño total
3F00	**3F00**			
3F00/2F00	DIR			
3F00/2F05	Lenguajes preferidos			8
3F00/2F06	Archivo de condiciones de acceso			
3F00/2FE2	ICCID (número serial)			10
3F00/7F10	**TELECOM**			
3F00/7F10/6F06	Archivo de condiciones de acceso			
3F00/7F10/6F3A	Agenda de números de la (U)SIM	250	30	7500
3F00/7F10/6F3B	Agenda de números fijos	50	30	1500
3F00/7F10/6F3C	SMS a guardar en la (U)SIM	30	176	5280
3F00/7F10/6F40	MSISDN, número	2	30	60
3F00/7F10/6F42	Parámetros del SMS	3	40	120
3F00/7F10/6F43	Estado del SMS			2
3F00/7F10/6F44	Último número marcado	10	30	300
3F00/7F10/6F49	Agenda de números de servicio	20	34	680
3F00/7F10/6F4A	EXT1	5	13	65
3F00/7F10/6F4B	EXT2	2	13	26
3F00/7F10/6F4C	EXT3	1	13	13
3F00/7F10/6F4D	BDN	5	31	155
3F00/7F10/6F4E	EXT 4	2	13	26
3F00/7F10/6F54	SUME, título del menú, en caso de existir			20
3F00/7F10/5F3A	**Agenda de números**			
3F00/7F10/5F3A/4FXX	Control de agenda de teléfono	250	2	500
3F00/7F10/5F3A/4F30	Referencia de la agenda de teléfono	1	20	20
3F00/7F10/5F3A/4F3A	Agenda de números de la (U)SIM	250	30	7500

Ruta / Id	Nombre	No de registros	Tamaño del registro	Tamaño total
3F00/7F10/5F3A/4F4A	EXT1	5	13	65
3F00/7FF0	**ADF (U)SIM**			
3F00/7FF0/6F06	Archivo de condiciones de acceso			
3F00/7FF0/6F05	Lenguajes preferidos			8
3F00/7FF0/6F07	IMSI, suscriptor GSM/UMTS			9
3F00/7FF0/6F38	Tabla de Servicios (U)SIM			12
3F00/7FF0/6F3B	Agenda de números fijos	50	30	1500
3F00/7FF0/6F3C	SMS	30	176	5280
3F00/7FF0/6F40	MSISDN (Mobile Station international ISDN number)	2	30	60
3F00/7FF0/6F42	Parámetros SMS	3	40	120
3F00/7FF0/6F43	Estado de los SMS			2
3F00/7FF0/6F46	Nombre del proveedor de servicios			17
3F00/7FF0/6F49	Agenda de números de servicio	20	34	680
3F00/7FF0/6F4B	EXT 2	2	13	26
3F00/7FF0/6F4C	EXT 3	1	13	13
3F00/7FF0/6F60	PLMNwAcT – Redes preferidas de acuerdo a la tecnología y el usuario			100
3F00/7FF0/6F61	OPLMNwACT- Redes preferidas de acuerdo a la tecnología y el operador			100
3F00/7FF0/6F62	HPLMNwACT- Redes preferidas de acuerdo a la tecnología en el país de donde es el operador			20
3F00/7FF0/6F78	Clase de control de acceso			2
3F00/7FF0/6F7B	FPLMN – Redes prohibidas			12
3F00/7FF0/6F7E	Información Local			11
3F00/7FF0/6FAD	Dato administrativo			4
3F00/7FF0/6FB7	Códigos de llamada de emergencia	2	20	40
3F00/7FF0/6FC7	Números de buzón de voz	2	30	60

Ruta / Id	Nombre	No de registros	Tamaño del registro	Tamaño total
3F00/7FF0/5F3B	**Gsm-Access**			
3F00/7FF0/5F3B/4F20	Kc			9
3F00/7FF0/5F3B/4F52	KcGPRS			9

Tabla 29. Lista de archivos requeridos por el operador.

4.3. Actualización vía OTA de la (U)SIM.

Para esta sección el cliente ha definido lo siguiente:

SPI1: 16, número de llavero a utilizar: 01

Con esto podemos realizar la implementación del juego de llaves no 1 para realizar la actualización vía OTA.

Este juego de llaves debe de crearse de acuerdo con la seguridad especificada por el cliente. Ver tabla 30.

SPI	Significado
SPI1 con valor 16	- Checksum Criptográfico - Procesar el mensaje si el contador de la entidad emisora es mayor que el de la entidad receptora - Cifrado

Tabla 30. SPI1 (indicador de los parámetros de seguridad) definidos por el operador.

Por lo tanto, se deben realizar las siguientes acciones:

- Creación del juego de llaves con la seguridad especificada
- Creación de las llaves necesarias

Cuando se crea la seguridad del juego de llaves, se debe colocar entre las características del mismo, la propiedad de actuar como ADM (código administrativo sólo conocido por el operador), esto es lo que permite la actualización de las tarjetas vía OTA.

A continuación se detalla la creación del juego de llaves en conjunto con la creación de llaves:

CLA INS XXYY LONG CA $ADM1

Donde:

CLA: clase
INS: instrucción
XX: número de llavero
YY: índice que ocupa en el llavero
LONG: longitud del comando subsecuente
CA: condiciones de acceso, SPI1 y propiedades

Así el primer llavero que contiene las llaves de OTA queda de esta manera:

'Script de creación del juego de llaves 01
CLA INS 0100 LONG CA $ADM1
'Script: Crear Llave de Cifrado-KIC
CLA INS 0101 LONG CA $KIC
'Script: Crear Llave de Firma-KID
CLA INS 0102 LONG CA $KID
'Script: Crear Llave de Cifrado-KIK
CLA INS 0103 LONG CA $KIK

Las variables ADM, KIC, KID y KIK se generan de manera aleatoria. Éstas sólo admiten caracteres entre la A-F y 0-9.

Una vez creadas las llaves y los archivos necesarios, se puede proceder a hacer una prueba de actualización remota (OTA).

Se tiene el trazado de un SMS segurizado, que puede ser desglosado de la siguiente manera:

SMS recibido por la tarjeta SIM:

D16B020283810606910552032000B5D4406910575457FF62110310104214A4D0270000
0481516011515B000103EC9B318680A1619595EE6E69694AF2DBC8DAE0D75ED8C345D1B
7820C3A76FAF5712C345F11BF01DB07302A21FC7CC4639DBF60037B24A4EDB8F3F5A185
3B50A

A continuación se ve el encabezado SMS 03.48:

D16B020283810606910552032000B5D4406910575457FF62110310104214A4D0270000
04815

Posteriormente tenemos la seguridad, dada por:

16 01 15 15

En la tabla 31 se realiza el desglose de los parámetros de seguridad.

	Significado
SPI 01, valor 16	- Checksum Criptográfico - Procesar el mensaje si el contador de la entidad emisora es mayor que el de la entidad receptora - Cifrado
SPI 02, valor 01	- PoR (Prueba de recepción) debe ser enviada a la entidad emisora.
KIC = 15	- Algoritmo triple DES en modo CBC, juego de llaves 1
KID = 15	- Algoritmo triple DES en modo CBC, juego de llaves 1
TAR = B00010	- Identificador de la aplicación receptora

Tabla 31. Desglose de los parámetros de seguridad de un mensaje seguro.

Dado el mensaje cifrado:

3EC9B318680A1619595EE6E69694AF2DBC8DAE0D75ED8C345D1B7820C3A76FAF5712C3
45F11BF01DB07302A21FC7CC4639DBF60037B24A4EDB8F3F5A1853B50A

Se obtiene el mensaje descifrado:

00000000020742A2D04643BDC771A0A40000023F00A0A40000027F20A0A40000026F46A
0D60000110174657374205 06F52FFFFFFFFFFFFFFFF0000000000000005759E43AA64F440

En donde:

A0 A4 0000 02 3F00 Selección del MF
A0 A4 0000 02 7F20 Selección del DF(GSM)
A0 A4 0000 02 6F46 Selección del archivo 6F46 (SPN)
A0 D6 0000 11 004F5441204F70FFFFFFFFFFFFFFFFFF Actualización del archivo SPN, texto OTA

Para revisar la actualización de OTA, es necesario revisar el título del SPN antes y después de la actualización.

Se realiza el envío del siguiente script:

'Selección del directorio raíz
A0 A4 0000 02 3F00
'Selección del directorio de la aplicación (U)SIM
A0 A4 0000 02 7FF0
'Selección del archivo SPN
A0 A4 0000 02 6F46
'Lectura del archivo SPN
A0 B0 0000 08

De este modo se revisa el contenido:

SPN antes:

004F70657261646F72FFFFFFFFFFFFFFFF (Operador)

SPN después:

004F5441204F70FFFFFFFFFFFFFFFFFF (OTA Op)

4.4. Autenticación a la red.

Para proceder a la validación de la autenticación 3G se procede a obtener la traza correspondiente, de los comandos entre el terminal y la tarjeta (U)SIM. La verificación se realizará con el estándar ETSI TS 131 102.

Como primer paso, procedemos a tomar una traza, modificando el número SQN, para revisar que la (U)SIM es capaz de re-sincronizar en caso de que el SQN sea diferente al enviado por la plataforma de autenticación, además de revisar que la autenticación se realiza de manera mutua ((U)SIM-red, red-(U)SIM):

```
Interpreted Data :
[+] INTERNAL AUTHENTICATE
 \---[:] Raw Data:
0x00880081221063BDC1C54C3978DB7CE082750917386310BCBE6C25891D80004696033
99AD65C51
-------------------------------------------------------------------------------
Interpreted Data :
[+] SW: 6110
 \---[:] Raw Data: 0x6110
-------------------------------------------------------------------------------
Interpreted Data :
[+] GET RESPONSE
 \---[:] Raw Data: 0x00C0000010
-------------------------------------------------------------------------------
Interpreted Data :
[+] SW: 9000 - Normal processing. Command correctly executed, and no response data
 |---[:] Data: DC0EE385D84A0FBA840FA0A82CD692EB
 \---[:] Raw Data: 0xDC0EE385D84A0FBA840FA0A82CD692EB9000
-------------------------------------------------------------------------------
Interpreted Data :
[+] INTERNAL AUTHENTICATE
 \---[:] Raw Data:
0x0088008122108B2E0126CEECCB9F56800D1A41BD401B100A62CBE4FA148000DDC4D8E
4D22E7EFB
-------------------------------------------------------------------------------
Interpreted Data :
[+] SW: 6135
 \---[:] Raw Data: 0x6135
-------------------------------------------------------------------------------
Interpreted Data :
[+] GET RESPONSE
 \---[:] Raw Data: 0x00C0000035
-------------------------------------------------------------------------------
```

Interpreted Data :
[+] SW: 9000 - Normal processing. Command correctly executed, and no response data
|---[:] Data:
DB0879EAEB7E206E533910EF768D4F03B946F736AEB54350EEDE2C10D3E0D52E49D93A8349A59890F19962FB08439D75B2EB17C0A3
\---[:] Raw Data:
0xDB0879EAEB7E206E533910EF768D4F03B946F736AEB54350EEDE2C10D3E0D52E49D93A8349A59890F19962FB08439D75B2EB17C0A39000

Después de revisar la traza, se puede observar que existen dos Internal Authenticate, y que el resultado es diferente en cada uno.

Se desglosa y analiza el primer Internal Authenticate (ver tabla 32), acorde al estándar ETSI TS 131 102.

[+] INTERNAL AUTHENTICATE
\---[:] Raw Data:
0x00880081221063BDC1C54C3978DB7CE082750917386310BCBE6C25891D8000469603399AD65C51

Código	Valor
CLA	00
INS	88
P1	00
P2	81 (contexto 3G)
Longitud del comando	22
Longitud del RAND	10
RAND	63BDC1C54C3978DB7CE0827509173863
Longitud del AUTN	10
AUTN	BCBE6C25891D8000469603399AD65C51

Tabla 32. Desglose del comando de autenticación interna.

A continuación, tenemos la respuesta al primer Internal Authenticate por parte de la (U)SIM (ver tabla 33).

Interpreted Data :
[+] SW: 9000 - Normal processing. Command correctly executed, and no response data
|---[:] Data: DC0EE385D84A0FBA840FA0A82CD692EB
\---[:] Raw Data: 0xDC0EE385D84A0FBA840FA0A82CD692EB9000

Código	Descripción
DC	Etiqueta de sincronización fallida “DC”
0E	Longitud del AUTS
AUTS	E385D84A0FBA840FA0A82CD692EB

Tabla 33. Respuesta al comando Internal Authenticate.

Es decir, tenemos un problema con la sincronización “DC”, que se debe a que el SQN de la red con el que se hizo el intento de autenticación no entra en el rango establecido, o bien es inferior al último SQN almacenado en la tarjeta.
Por este motivo, la tarjeta envía el token de autenticación para la re-sincronización AUTS (el cual contiene el último SQN con el que la tarjeta se enganchó a la red), para que la red pueda re-sincronizar su base de datos del SQN.

Una vez realizado esto, se hace un reintento de conexión a la red (segundo Internal Authenticate). Dicho reintento se desglosa en la tabla 34.

Interpreted Data :
[+] INTERNAL AUTHENTICATE
\---[:] Raw Data:
0x0088008122108B2E0126CEECCB9F56800D1A41BD401B100A62CBE4FA148000DDC4D8E4D22E7EFB

Código	Valor
CLA	00
INS	88
P1	00
P2	81 (contexto 3G)
Longitud del comando	22
Longitud del RAND	10
RAND	8B2E0126CEECCB9F56800D1A41BD401B
Longitud del AUTN	10
AUTN	0A62CBE4FA148000DDC4D8E4D22E7EFB

Tabla 34. Desglose del comando de autenticación interna.

En este caso el SQN (número de secuencia) contenido en el AUTN (token de autenticación) es un valor superior al de la tarjeta (U)SIM y que se encuentra en el rango establecido por la misma, debido a que la plataforma ha tomado como base el AUTS que envío la tarjeta en el intento anterior. Es por esto que en este momento la autenticación se realiza de manera correcta, como se puede ver claramente en la tabla 35.

Interpreted Data :
[+] SW: 9000 - Normal processing. Command correctly executed, and no response data
|---[:] Data:
DB0879EAEB7E206E533910EF768D4F03B946F736AEB54350EEDE2C10D3E0D52E49D93A8349A59890F19962FB08439D75B2EB17C0A3
\---[:] Raw Data:
0xDB0879EAEB7E206E533910EF768D4F03B946F736AEB54350EEDE2C10D3E0D52E49D93A8349A59890F19962FB08439D75B2EB17C0A39000

Código	Descripción
DB	Autenticación 3G exitosa
08	Longitud de RES
79EAEB7E206E5339	RES
10	Longitud de CK
EF768D4F03B946F736AEB54350EEDE2C	CK
10	Longitud de IK
D3E0D52E49D93A8349A59890F19962FB	IK
08	Longitud de Kc
439D75B2EB17C0A3	Kc

Tabla 35. Respuesta al comando Internal Authenticate.

Con esto se comprueba que la tarjeta realizó una autenticación exitosa y está enganchada a la red. A partir de este momento se pueden realizar llamadas y mandar mensajes SMS.

4.5. Aplicación de control de acceso.

La aplicación tiene 16 sectores, cada sector contiene 4 bloques de datos.
A su vez cada sector está divido en 4 bloques de datos, los 3 primeros son bloques de datos, mientras que el último es un bloque de seguridad. Dicho bloque de seguridad contiene las llaves y las condiciones de acceso de cada bloque.

4.5.1. Seguridad.

Cada sector se protege de manera independiente, basado en autenticación
Cada bloque de datos tiene sus propias condiciones de acceso.
El bloque de seguridad contiene dos llaves, llave A y llave B las cuales servirán para autenticar la tarjeta con el lector. Las condiciones de acceso definirán cuál o cuáles llave o llaves deberán utilizarse.
Así, la autenticación involucra las llaves almacenadas en cada sector y en el lector de tarjetas.
Comunicación cifrada, la comunicación entre el lector y la tarjeta es codificada en base a una llave de sesión generada en el proceso de autenticación.

4.5.2. Implementación.

Para poder realizar la interface de control de acceso es necesario realizar el reconocimiento del lector como un dispositivo de entrada/salida. Así pues, la manera de hacerlo es utilizando la librería javax.smartcardio, con la cual obtenemos los lectores disponibles y se almacenan en un arreglo de Strings, como se puede ver en la figura 26.

```
public String[] getReaders() throws CardException {
    TerminalFactory factory = TerminalFactory.getDefault();
    terminals = factory.terminals().list();
    Object[] readers = new Object[terminals.size()];
    readers = terminals.toArray();
    String str_readers[] = new String[readers.length + 1];
    str_readers[0] = "";
    for (int i = 1; i < str_readers.length; i++) {
        str_readers[i] = readers[i - 1].toString();
    }
    return str_readers;
```

Figura 26. Código para identificación de lector

4.5.2.1. Autenticación.

Antes de poder realizar la lectura/escritura de un bloque es necesario realizar la autenticación, que dependerá de la llave seleccionada y almacenada en la tarjeta, y el valor del índice de la llave almacenada en el lector. En la figura 27, se muestra el método utilizado para realizar estas acciones.

```
private void authenticateButtonActionPerformed(java.awt.event.ActionEvent evt) {
    if (aRadioButton.isSelected()) // Al seleccionar el tipo de llave (key A o key B) se le asigna un byte especifico.
        keyType = 0x60;
    else
        keyType = 0x61;

    byte[]apdu = new byte[10]; // Arreglo de bytes donde se formara el comando APDU de autenticacion.
    Integer keyIndex = 80; // Valor de llave en el lector de tarjetas
    byte b = keyIndex.byteValue();
    Integer addressBlock = blockBox.getSelectedIndex();
    byte add = addressBlock.byteValue(); // Dependiendo el bloque seleccionado, se le asigna un byte especifico.
    byte[]TYPEKEY = {add,keyType,b}; /* Se forma el cuerpo del APDU de autenticación, utilizando el numero de bloque
                                        el tipo de llave y el valor de llave en el lector de tarjetas*/
    System.arraycopy(AUTHENTICATE, 0, apdu, 0, 7);
    System.arraycopy(TYPEKEY, 0, apdu, 7, 3); /* Se forma el comando APDU de autenticación utilizando la constante
                                                 "AUTHENTICATE" y el cuerpo del comando (TYPEKEY)*/
    sendAPDU(apdu); // Se envia el comando APDU a la tarjeta
```

Figura 27. Código para la autenticación del bloque de seguridad.

4.5.2.2. Lectura/Escritura.

Una vez autenticada la tarjeta, se puede proceder a la lectura/escritura del bloque de datos.

Antes de poder actualizar un bloque de datos, es indispensable realizar el proceso de autenticación, una vez realizado este procedimiento, es posible actualizarlo. En el método descrito a continuación, se realiza la selección del bloque de datos, para después proceder a la lectura del mismo. A continuación se muestra el código para la selección del bloque de datos, figura 28.

```
// Metodo de lectura del bloque seleccionado
private void readButtonActionPerformed(java.awt.event.ActionEvent evt) {
    byte[]apdu = new byte[5]; // Arreglo de bytes donde se formara el comando APDU de lectura
    Integer addressBlock = blockBox.getSelectedIndex();
    byte add = addressBlock.byteValue(); // Dependiendo el bloque seleccionado, se le asigna un byte especifico.
    byte[]ADDLEN = {add,(byte)0x10}; // Se forma el cuerpo del comando APDU de lectura.
    System.arraycopy(READ_BLOCK, 0, apdu, 0, 3);
    System.arraycopy(ADDLEN, 0, apdu, 3, 2); /* Se forma el comando APDU de lectura utilizando la constante
                                                "READ_BLOCK" y el cuerpo del comando (ADDLEN)*/
    sendAPDU(apdu); // Se envia el comando APDU a la tarjeta
    displayTextField.setText(getHexString(r.getData())); // Se despliega el SW
```

Figura 28. Código para la selección de bloque de datos.

La lectura/escritura de los bloques de datos se realiza a través de APDU (Application Protocol Data Unit) el cual es la manera en que la tarjeta entiende los comandos, a continuación en la figura 29 se ilustra el método para hacer la escritura.

```
byte[]apdu = new byte[21]; // Arreglo de bytes donde se formara el comando APDU de escritura
Integer addressBlock = blockBox.getSelectedIndex();
byte add = addressBlock.byteValue(); // Dependiendo el bloque seleccionado, se le asigna un byte especifico.
byte[]ADDLEN = {add,(byte)0x10}; // Se forma el cuerpo del comando APDU de escritura.
byte[]apduData = hexStringToByteArray(updateData); // Se convierte la infromación a actualizar a un arreglo de bytes
System.arraycopy(UPDATE_BLOCK, 0, apdu, 0, 3);
System.arraycopy(ADDLEN, 0, apdu, 3, 2);
System.arraycopy(apduData, 0, apdu, 5, 16); /* Se forma el comando APDU de escritura utilizando la constante
                                               "UPDATE_BLOCK", el cuerpo del comando (ADDLEN) y la información
                                               a actualizar*/
sendAPDU(apdu); // Se envia el comando APDU a la tarjeta.
displayTextField.setText("");
```

Figura 29. Código para escritura del bloque de datos.

Cada ejecución de comando APDU, genera una respuesta de la tarjeta, en este caso el "9000" significa que el comando se ejecutó correctamente, y una respuesta distinta significa que fue ejecutada incorrectamente. Así por ejemplo si la respuesta no es 9000, cachamos la excepción ya que estamos usando dispositivos de I/O.

4.6. Pruebas de usuario.

Autenticación a la red 3G,

La autenticación a red 3G se ha probado mediante la verificación de que el equipo móvil tiene señal y puede realizar y recibir llamadas.

PIN1 (habilitar, deshabilitar y cambio de PIN1)

Para probar el PIN1 se realizó la prueba desde el teléfono (Samsung Galaxy Ace), en la opción de Configuración→ Ubicación y seguridad→ Definir bloqueo de tarjeta SIM→Bloquear tarjeta SIM. En este punto se coloca el PIN1 y con esto se habilita el PIN1.

Una vez habilitado el PIN1, es posible actualizarlo, presentando primeramente el PIN1 actual, y después el nuevo PIN1 en la misma ruta antes mencionada.

De igual manera, para deshabilitarlo, el PIN1 debe estar activo y se debe ir a la misma opción en donde se activa.

Código de desbloqueo del PIN1 (PUK1)

Para probar el PIN1 se realizó la prueba desde el teléfono (Samsung Galaxy Ace), en la opción de Configuración→ Ubicación y seguridad→ Definir bloqueo de tarjeta SIM→Bloquear tarjeta SIM. En este punto se coloca el PIN1 3 veces consecutivas de manera errónea. Después el terminal dice que para rehabilitar el PIN1 se debe presentar el código PUK1. Si se presenta correctamente el PUK1, entonces el contador del PIN1 se vuelve a colocar en 3 y permite actualizar el PIN1.

PIN2 (habilitar, deshabilitar y cambio de PIN2)

Para probar el PIN2 se realizó la prueba desde el teléfono (Samsung Galaxy Ace), en la opción de Configuración→ Configuración de llamadas→ Números M Fijo→Activar M fijo. En este punto se coloca el PIN2 y con esto queda habilitado.

Una vez habilitado el PIN2, es posible actualizarlo, presentando primeramente el PIN2 actual, y después el nuevo PIN2 en la misma ruta antes mencionada.

De igual manera, para deshabilitarlo, el PIN2 debe estar activo y se debe ir a la misma opción en donde se activa.

Acceso al FDN (añadir un contacto, verificar que sólo se puede llamar a contactos de FDN, borrar contacto, llenar la agenda FDN)

Para poder realizar este procedimiento es indispensable tener activo el PIN2. Una vez que esté activo, se pueden agregar contactos a la agenda de números fijos, y solamente se podrán hacer llamadas a los números que estén en dicha agenda.

Esta prueba se realizó, activando el PIN2 y después se añadió un contacto en la ruta Configuración→ Configuración de llamadas→ Definir Números M Fijo→Contactos M Fijo. Se procedió a realizar una llamada a uno de los números que estaban dados de alta, y se comprobó que se podía realizar. Después se realizó una llamada a un número que no estaba dado de alta en esta agenda y la llamada fue rechazada.

Probar la agenda (revisar que acepta 250 registros, modificar registro, añadir y borrar)

Se procedió a la creación de 250 contactos. Una vez creados se dieron de alta en la agenda de la (U)SIM, desde la opción Importar/Exportar→Exportar a tarjeta (U)SIM. Una vez hecho este procedimiento cada contacto apareció con el símbolo de la tarjeta (U)SIM al costado derecho.

Se procedió a realizar una llamada con un contacto de la tarjeta (U)SIM de manera exitosa. Después el contacto fue actualizado y se realizó una nueva llamada de manera exitosa.
La última prueba realizada fue el borrado de un contacto de la tarjeta (U)SIM.

Revisar el idioma que presenta el terminal

Esta prueba se realizó, desde la opción Configuraciones → Idioma y texto y ahí apareció el idioma Español que es el que se configuró en la tarjeta SIM.

Números de servicio

Se revisaron los contactos almacenados en la agenda de contactos. En esta se encontraban Bomberos, Atn Ciudadana, Policía. Se procedió a realizar las llamadas y éstas fueron realizadas de manera exitosa.

Buzón de voz

Se verificó desde la opción Configuraciones → Configuración de Llamada→Buzón de voz. Una vez que se verificó el número, se realiza la llamada al mismo y éste es redireccionado al buzón de voz.

Envío y recepción de SMS, verificar los SMS almacenados en la SIM.

Se realizaron envío y recepción de SMS de manera exitosa. En la opción Configuración→Centro de Servicio se revisó el centro de mensaje apropiado del operador. Se configuró una (U)SIM para almacenar 20 mensajes. Cuando el mensaje 21 llega a la (U)SIM el primer mensaje deja de estar en la (U)SIM ya que este es un archivo cíclico tipo FIFO.

Verificar el SPN requerido

Una vez que el terminal fue encendido y se engancho a la red, el nombre del operador fue desplegado.

Protocolo de comunicación tipo A

Se generó un pequeño programa que realiza la autenticación en el bloque de datos seleccionado. También se puede realizar la lectura/escritura en el bloque seleccionado.

Se realizó una prueba con un lector de comunicación a distancia que permitió el acceso a una oficina presentando el mismo identificador que el de una credencial de un trabajador.

Las siguientes 3 validaciones fueron simuladas. Se colocó un slot de memoria que contenía el monto del monedero y de acuerdo a montos establecidos, cada que se presentaba la tarjeta se realizó el incremento / decremento correspondiente.

5. Resultados y conclusiones.

5.1. Resultados.

Los resultados obtenidos en el desarrollo e implementación de la tarjeta (U)SIM para el control de acceso con comunicación inalámbrica fueron los siguientes:

Para el operador de red:

- Introducción de una nueva tecnología y ofrecer otro tipo de servicios. Con este tipo de prácticas el cliente se posiciona como líder en el campo de la telefonía celular, además de obtener la lealtad de sus suscriptores y a su vez la adición de nuevos suscriptores.
- Cuota de recuperación por servicios. El cliente estipula en sus contratos obtener ganancias por cada transacción relacionada a su nueva tecnología.

Para el usuario:

- Facilidad de uso de los servicios. Los usuarios siempre buscarán la forma más sencilla de hacer las cosas, y este tipo de tecnología está pensada precisamente para ello.
- El usuario suele tener dificultades para traer muchas tarjetas en su cartera, y suele olvidar siempre la que más necesitaba. Con esta solución, se pueden traer todas las credenciales en un solo dispositivo (la tarjeta (U)SIM).
- Reducción de costos, el usuario no necesita que se emita su tarjeta de acceso al trasporte público, lo cual indica un costo extra para su bolsillo.

Esta solución apoya indirectamente el medio ambiente, pues se estarían emitiendo muchísimo menos millones de tarjetas por año.

5.2. Conclusiones.

El desarrollo de una tarjeta (U)SIM con una aplicación para el control de acceso, representó un reto en mi carrera profesional, ya que para poder realizar esta tarjeta primero que nada tuve que documentarme, entender la tecnología específica Java Card y la tecnología de comunicación a distancia NFC (Near Field Communication) y posteriormente implementarlo.
A continuación describo las conclusiones en los puntos que considero más importantes:

Desarrollo profesional

- Afrontar el reto de creación de una nueva tarjeta con tecnología sin contacto. Este tipo de reto, fue bastante interesante, pues en principio no conocía la tecnología de radio frecuencia, por lo que tuve que investigar de que se trataba, cómo se relacionaba con ese pequeño microprocesador denominado tarjeta (U)SIM y las limitantes que se tenían. Al principio me pareció que no iba a ser posible realizar esta tarjeta y que eran muchos los elementos involucrados que no conocía, sin embargo, poco a poco descubrí que era posible realizar el reto. Me permitió relacionarme con personas de los operadores de telefonía móvil, entender su perspectiva y asesorarlos en cuanto a lo que era y no era posible desarrollar.
- En cuanto al análisis y planeación, el hecho de elaborar un plan de trabajo donde se plasmaban las actividades y tiempos, proponer soluciones, cumplir con las especificaciones del cliente y tener juntas de seguimiento me permitió aumentar mi experiencia y habilidad en la administración y desarrollo de proyectos.
- Los objetivos se cumplieron de manera cabal, se pudo elaborar la tarjeta (U)SIM con la característica de control de acceso. El comportamiento de la tarjeta (U)SIM como suscriptor en una red UMTS no se ha visto afectado por la incorporación de la aplicación de control de acceso. La aplicación de control de acceso se ha podido validar a nivel conceptual (con simulador) y a nivel real permitiendo a algunos empleados ingresar a sus oficinas el lugar de usar su gafete.

Diseño de la solución y utilidad

- A nivel proyecto se ha podido presentar de cara al operador de telefonía móvil con una muy buena aceptación en cuanto al comportamiento de la tarjeta y la experiencia de usuario. No obstante, el proyecto necesita de un tercero, pudiendo ser el sistema de transporte público, las oficinas gubernamentales, las universidades públicas, etc. Este tipo de entidades, no han decidido realizar el proyecto con los operadores de telefonía móvil argumentando que no pueden obligar a sus usuarios a permanecer con un solo operador de telefonía móvil, y en otros casos argumentando que no tienen la infraestructura necesaria para colocar los torniquetes o puertas con el control de acceso y no cuentan con el presupuesto suficiente para incorporar dicha infraestructura.

- Algunos de los problemas enfrentados fue la interpretación de los estándares, ya que en muchos casos para encontrar la información precisa, es necesario saltar entre secciones y entre estándares, y en muchos de los casos la información no es muy clara. Además la tecnología Java Card es un framework limitado, pues por las características físicas del chip ((U)SIM) no se tienen todas las librerías que podrían tenerse en el API de Java Card convencional. Dado lo anterior, es complicado adecuarse al ambiente de trabajo y entender qué se puede hacer y qué no, y entender la limitante de la tarjeta (U)SIM.
- En cuanto a la metodología de desarrollo podemos notar que es semejante al modelo incremental pero con la diferencia de que el análisis se hizo una sola vez. De acuerdo a la metodología que seguí, se entregó una tarjeta con un software de prueba completamente operacional y funcional. Debido a la falta de acuerdos con entidades gubernamentales y los operadores de telefonía móvil aún no se ha podido implementar este tipo de tarjetas de manera masiva.

I. Fuentes de información.

3GPP TS 11.11 V8.13.0 (2005-06)
3rd Generation Partnership Project; Technical Specification Group Terminals
Specification of the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface
(Release 1999)

3GPP TS 11.14 V8.9.0 (2001-12)
3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the
Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
(Release 1999)

3GPP TS 23.040 V6.6.0 (2005-12)
3rd Generation Partnership Project; Technical Specification Group Terminals;
Technical realization of the Short Message Service (SMS); (Release 6)

3GPP TS 23.048 V5.2.6 (2005-06)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Security Mechanisms for the (U)SIM application toolkit stage 2(Release 5)

3GPP TS 11.11 V8.13.0 (2005-06)
3rd Generation Partnership Project; Technical Specification Group Terminals
Specification of the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface
(Release 1999)

3GPP TS 11.14 V8.9.0 (2001-12)
3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the
Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
(Release 1999)

3GPP TS 23.040 V6.6.0 (2005-12)
3rd Generation Partnership Project; Technical Specification Group Terminals;
Technical realization of the Short Message Service (SMS); (Release 6)

3GPP TS 23.048 V5.2.6 (2005-06)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Security Mechanisms for the (U)SIM application toolkit stage 2(Release 5)

3GPP TS 24.008 V11.4.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
(Release 11)

3GPP TS 22.030 V12.0.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Man-Machine Interface (MMI) of the User Equipment (UE) (Release 12)

3GPP TS 22.038 V11.0.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
(U)SIM Application Toolkit (USAT); Service description; Stage 1
(Release 11)

3GPP TS 31.101 V10.0.1 (2011-06)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals;
UICC-terminal interface; Physical and logical characteristics
(Release 10)

3GPP TS 55.205 V11.0.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
Specification of the GSM-MILENAGE Algorithms: An example algorithm set for the GSM Authentication and Key Generation functions A3 and A8
(Release 11)

3GPP TS 51.011 V5.0.0 (2001-12)
3rd Generation Partnership Project; Technical Specification Group Terminals;
Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
(Release 5)

3GPP TS 31.102 V11.3.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals;
Characteristics of the Universal Subscriber Identity Module ((U)SIM) application
(Release 11)

3GPP TS 22.011 V9.4.0 (2010-06)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
Service accessibility
(Release 9)

3GPP TS 23.041 V11.4.0 (2012-09)
3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals;
Technical realization of Cell Broadcast Service (CBS)
(Release 11)

3GPP TS 22.002 V11.0.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)
(Release 11)

3GPP TS 22.022 V11.0.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
Personalisation of Mobile Equipment (ME); Mobile functionality specification
(Release 11)

3GPP TS 23.003 V11.3.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
(Release 11)

3GPP TS 33.102 V11.4.0 (2012-09)
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
3G Security; Security architecture
(Release 11)

II. Glosario.

- **IMSI** – Código de Identificación Único para el Operador (*International Mobile Subscriber Identity*).
- **ICCID** – Número Serial de la tarjeta (*Integrated Circuit Card ID).*
- **MSISDN** – Número telefónico asociado a una tarjeta (U)SIM (*Mobile Station international ISDN number*).
- **OTA** – Protocolo usado para la comunicación remota con la tarjeta (U)SIM (Over The Air) .
- **Ki** – LLave de autenticación del suscriptor.
- **Llave de Transporte** – Llave usada para el cifrado de la llave de autenticación del suscriptor.
- **KIC**- Identificador de la llave y algoritmo utilizado para el cifrado (*Key and algorithm Identifier for ciphering).*
- **KID** - Identificador de la llave y algoritmo utilizado para RC/CC/DS (*Key and algorithm Identifier for RC/CC/DS).*
- **KIK** - Identificador de la llave y algoritmo utilizado para la protección de KIC y KID (*Key Identifier for protecting KIC and KID).*
- **RC** – Verificador de Redundancia (*Redundancy Check).*
- **CC** – Checksum Criptográfico (*Cryptographic Checksum*).
- **DS** – Firma Digital (*Digital Signature).*
- **ADM** – Código de acceso a los archivos de la tarjeta (U)SIM, controlado por el operador.
- **CHV** – PIN de la tarjeta (U)SIM (*Card Holder Verification*).
- **PUK** – Código de desbloqueo de código PIN (*PIN Unblocking Key / PIN2 Unblocking Key*).
- **Input File** – Archivo de entrada para generación de tarjetas.
- **Tarjeta de Ingeniería** – Tarjeta generada para propósitos de pruebas.
- **UICC** - Tarjetas con chip usadas en teléfonos móviles en redes GSM y UMTS (*Universal Integrated Circuit Card*).
- **HCI** Host Controller Interface.
- **SWP** - Protocolo de comunicación de contacto (*Single Wire Protocol*).
- **PICC** Tarjeta con chip de proximidad (*Proximity Integrated Circuit Card*).
- **Applet** – Programa desarrollado para una tarjeta para proveer un servicio.
- **Sat or S@t** – Lenguaje de programación de servicios interactivos.
- **STK** (Sim ToolKit) – Lista de comandos de la tarjeta a ser enviados al equipo móvil.
- **ME** – Equipo móvil (*Mobile Equipment*).
- **Plataforma** – Servidor conectado a algún servidor del operador, el cual permite que provee algún servicio a la tarjeta SIM/(U)SIM.
- **MNO** – Operador de red *(Mobile Network Operator*).
- **HLR** – Base de datos donde se almacena el perfil de cada suscriptor, servicios, restricciones a nivel de la red local (*Home Location Register*).

- **VLR** – Base de datos donde se almacena el perfil de cada suscriptor, servicios, restricciones a nivel de la red foránea (*Visitor Location Register*). Ésta almacena la información de los suscriptores registrados en el MSC.
- **MSC** – Centro de switcheo móvil (*Mobile Switching Center*).
- **AuC** – Centro de autenticación a cargo de la autenticación de los suscriptores de la red (*Authentication Center*) .
- **APDU** – Lista de comandos a ser enviados entre el terminal y la tarjeta SIM/(U)SIM (*Application Protocol Data Unit*).
- **ATR** – Answer to Reset: card's "signature".
- **EEPROM** – Memoria programable de la tarjeta SIM/(U)SIM .
- **SIM** – Chip para una red 3G *(Subscriber Identity Module: 2G GSM Chip*).
- **(U)SIM** – Chip para una red 3G (*Universal Subscriber Identity Module: 3G UMTS Chip*).
- **GSM** – Sistema global de telecomunicaciones móviles de segunda generación (*Global System for Mobile Communication*)
- **UMTS** – Sistema universal de telecomunicaciones móviles (*Universal Mobile Telecommunications System*) .
- **2G** – Red celular de segunda generación
- **3G** – Red celular de tercera generación.
- **BAP** – Tarjeta muestra de producción (bueno a producir).
- **PoR** – Prueba de recepción (Proof o Receipt).
- **JCRE** – Ambiente de ejecución de tarjetas Java (Java Card Runtime Environment).