

Anexo III

Descripción de Interfaces de Comunicación

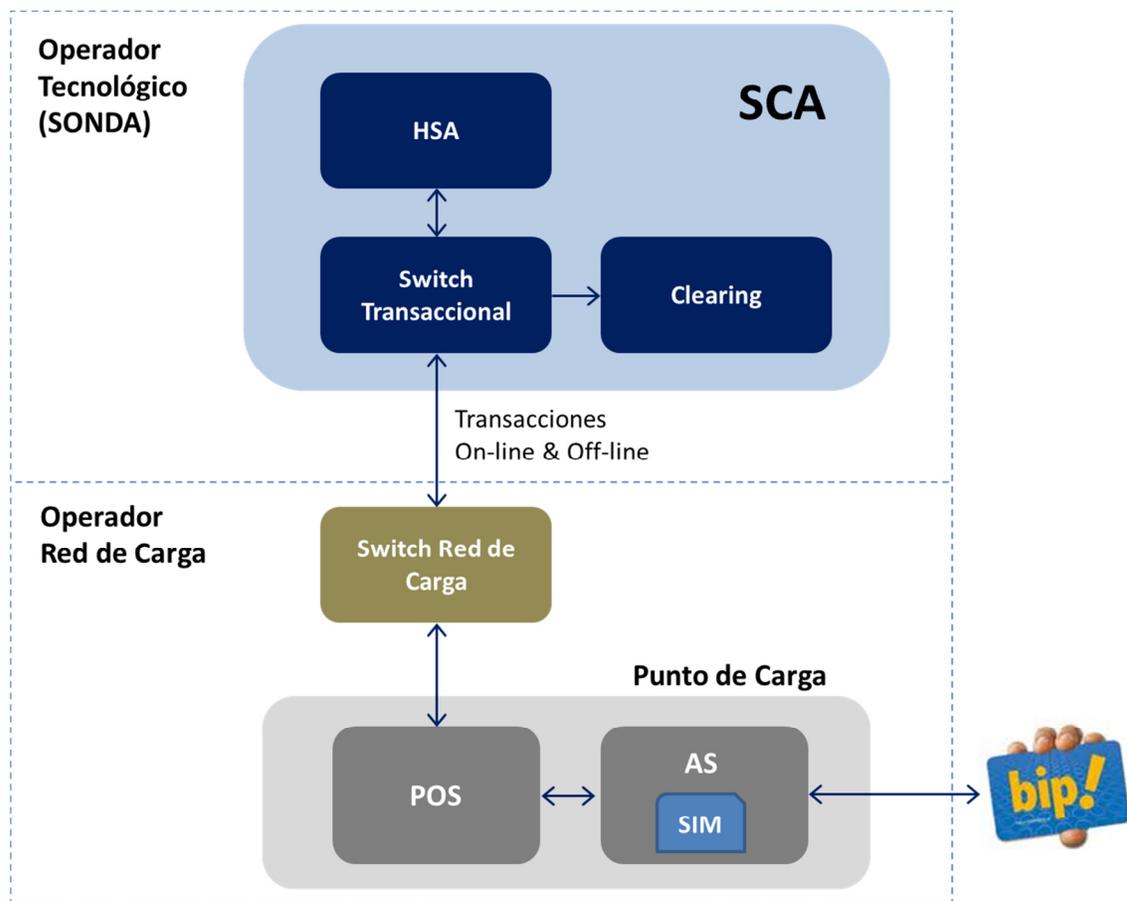
1 Objetivos

El presente Anexo tiene por objetivo entregar una descripción general, acerca de las interfaces que deberán ser desarrolladas por el Operador, para la integración tecnológica de su solución, con el Switch Transaccional de SONDA y con la Antena Segura (AS).

METRO hará entrega a la empresa adjudicada, durante la etapa de Ingeniería, de las especificaciones detalladas de dichas interfaces.

2 Diagrama general de integración

A continuación se adjunta diagrama esquemático que representa a los diferentes componentes tecnológicos que participan en el proceso de carga de Cuotas de Transporte.



3 Mecanismos o protocolos de intercambio

Se explican las definiciones necesarias para comprender el funcionamiento de la aplicación de recarga de la Tarjeta bip y carga de cupos de transporte y todas las interrelaciones con su entorno. Dicho entorno está conformado por quienes interactúan directamente con el sistema, Tarjeta bip, Antena Segura, POS y Switch Transaccional.

Las funcionalidades:

- Reconocimiento de AS
- Inicialización de AS
- Apertura AS y POS Solicitud de cupos de transporte al Switch Sonda
- Cierre de AS y POS.
- Anulación de Cupos de Transporte
- Carga con Registro Asegurado (#RA)
- Carga de Contrato por Convenio o Mandato
- Generación de #RA de Emergencia
- Reversa de Mandatos
- Consulta de Saldos
- Actualización de firmware AS

La AS se comunica con el POS a través de un puerto serial, utilizando un protocolo de comunicación propietario de Multivia por comandos, es decir, el POS (Master) solicita a la Antena Segura (Slave) la ejecución de algún comando, la Antena Segura lo ejecuta y devuelve el resultado al POS. Este protocolo posee elementos para el flujo de datos y control de errores.

4 Descripción de las Interfaces de Comunicación

4.1 Integración de POS con Antena Segura

Se deberá considerar la integración del POS con dos modelos de Antena Segura, y que corresponden a las siguientes:

- a) Antena Segura, del tipo INTEGRISYS (Obligatorio)
- b) Antena Segura, del tipo SOLEM (Opcional de funcionamiento paralelo al anterior)

Las especificaciones que a continuación se describen son comunes para ambos tipos de antena, pero en donde se necesitará una programación de mensajería personalizada, para cada una de ellas.

El formato de la mensajería que los POS deben utilizar para comunicarse con la Antena Segura está basado en el estándar internacional ISO 8583:1993 sobre TCP/IP, con modificaciones anidadas a éste sobre dos campos que contienen las reglas de negocio de METRO.

4.2 Comandos POS – AS

A continuación se entrega una lista del subconjunto de los comandos que el POS puede ejecutar sobre la AS, y que son necesarios para ejecutar acciones básicas de la AS y de limpieza de sus áreas de trabajo.

Comando	Función
CEAP	Energización en AS
CEAP2	Desencriptación de la WkPS
CIAP1	Inicialización en AS
CIAP2	Inicialización en AS
CAT1	Actualiza Tablas AS
CAT2	Actualiza Tablas AS
CLSE	Lectura Saldo Efectivo AS
CGSE	Graba Saldo Efectivo AS
CCME	Carga Monedero con Efectivo
CLX	Lectura de TM General en AS
CGX	Grabación de TM General en AS

Comando	Función
CTT	Traspaso de Tx
CTT2	Traspaso de Tx – 2 limpia areas
CCMT	Carga Monedero con Tarjeta, #RA o Mandato
CSTA	Consulta de Saldo TM en AS
CCAM	Cierre y Limpieza de AS en AS

4.2.1 Estructura de Comando POS al AS

STX	CMD	MAC	LEN	DATA	LRC	ETX
1 byte	1 byte	1 byte	1 byte	Max. 256 bytes	1 bytes	1 byte

STX : Start of Text 0x02

CMD : Código del comando, p.e 0xC5, 0xD5

MAC : Número de autenticación, o Numero del Paquete, p.e 0x01

LEN : Largo de la data

DATA : Data contigua de largo LEN

LRC : Calculado con los campos CMD, MAC, LEN y DATA

ETX : End of Text 0x03

Es un requerimiento de seguridad que los primeros 8 bytes (CMD (1), MAC (1), LEN (1) y DATA (1:5)) de todas las transacciones serán siempre encriptados con la WkAP (working key AS-POS), por lo que el POS encriptará dicho conjunto de campos y la AS deberá desencriptarlo para saber cuál es el comando que se está solicitando.

Si el campo DATA es menos de 5 bytes, y con el propósito de completar un largo de 8 bytes a ser encriptados, ésta se rellena con el Valor x'CA'.

4.3 Transacciones POS al Switch

La red debe conectarse al Switch de Sonda para poder cargar Cupos de Transporte en la AS, para las cargas de recaudación presencial siempre debe existir una Antena Segura que tiene Cupos de Transporte en el SAM en consignación para ser cargadas en las tarjetas, la comunicación entre las redes y el Switch es transaccional y encriptada. Para

que un punto de carga sea válido debe estar inscrito y reconocido en nuestros sistemas. El switch empaqueta las transacciones recibidas y las envía al clearing para ser procesadas.

La comunicación entre un POS y el Switch es socket sobre TCP/IP se realiza mediante flujo de información denominado para este caso: Transacción, el que se presenta bajo un protocolo formato ISO8583. Ver anexo 3

A continuación se presenta una lista de las mismas, las que representan el subconjunto de todas las transacciones implementadas en el Switch que será usado en los casos de uso aquí especificados.

Código	Descripción
TIP	<p>Inicialización AS.</p> <p>Esta transacción tiene la finalidad de solicitar un registro de inicialización para la antena segura del equipo de autoservicio. Este registro contiene llaves de encriptación entre otras.</p>
TIP03	<p>Reconocimiento AS.</p> <p>Esta transacción tiene la finalidad de solicitar la entrega de una llave de encriptación DES, para la encriptación de datos entre el equipo de autoservicio y el Switch METRO.</p>
TAT	<p>Actualiza Tablas de Difusión en AS.</p> <p>Esta transacción tiene la finalidad de solicitar la entrega de tablas de difusión que se deben actualizar en la antena segura.</p>
TCCT	<p>Carga de Cuotas de Transporte.</p> <p>Esta transacción tiene la finalidad de entregar al equipo de autoservicio un monto de cuota de transporte para ser cargado en la antena segura de éste.</p>
TACCT	<p>Anula carga de cuotas de transporte.</p> <p>Esta transacción tiene la finalidad de solicitar al servidor transaccional la reversa de la carga de los cupos de transporte previamente solicitados.</p>
TTAM	<p>Traspaso de Transacciones del AS (Devuelve Cupo)</p> <p>Esta transacción tiene la finalidad de informar al servidor central las ventas de cupos de transporte realizadas por el equipo de autoservicio (cierre de sesión)</p>
TTAM2	<p>Traspaso de Transacciones del AS-2.</p>
TCMR	<p>Carga Monedero con #RA, Directo.</p>
TGRA	<p>Genera #RA de emergencia.</p>

Código	Descripción
TCMM	Carga Monedero o Contrato con Mandato.
TCMMR	Reversa de carga de Contrato por Mandato.
TCAM	Cierre y limpieza RAM del AS. La finalidad de esta transacción es la de enviar al Switch, desde la antena segura, el último piggyback, de tal forma de que se pueda cerrar y cuadrar la última transacción.

Opcionalmente se pueden disponer de dos transacciones adicionales, si el Administrador de la Red (Metro) así lo decide y así lo autoriza al equipo de la red:

Código	Descripción
TCCTF	Carga de Cuotas de Transporte Forzadas
TTAMF	Devolución de Cuotas de Transporte Forzadas

4.4 Encriptación y Seguridad de Comandos POS – AS

En el diálogo de comunicaciones entre el POS y la AS se ha establecido, por razones de seguridad, que los 8 primeros Bytes (a partir del byte de CMD) estén encriptados con una llave denominada WkAP que es generada por el HSA y actualizada (enviada a la AS y POS) en cada proceso de Inicialización. Por otra parte se ha definido que el segundo byte del mensaje después del comando, sea representado por un MAC (Message Authentication Code), el cual se genera a partir de la última respuesta recibida por el POS desde la AS, a partir de las variables (CA/R || TSAM). La AS, al entregar la respuesta ha generado este valor y lo ha almacenado.

4.4.1 Encriptación con WKAP

La encriptación de los 8 primeros bytes a partir del byte CMD la realiza el POS en base a encriptación DES y con la llave WkAP. La llave WkAP la genera el HSA y es actualizada en ambos equipos (POS y AS) con la transacción de inicialización diaria, ésta debe ser almacenada en memoria permanente (en el POS en particular) de tal forma que ante falta de energía se pueda recuperar. Para las transacciones realizadas antes de las de inicialización (Reconocimiento), se utilizará como WkAPo el valor del AMID (Identificación de la Antena Segura en el Sistema AFT) que existe en la AS y que se incorpora en el POS de manera manual al integrarlo con una Antena Segura en particular.

4.4.2 Utilización del MAC

El cálculo del valor del MAC, se realiza con información (C A/R || TSAM) de la AS tanto en ésta para almacenarlo y futura validación, como en el POS, donde se calcula con la información recibida en la respuesta, se almacena y se envía con la próxima transacción a la AS.

Es la AS, al recibir el MAC del POS la que realiza la comparación (entre el MAC recibido y el almacenado de la respuesta anterior) y acepta la transacción. Considerando que en la primera transacción del POS a la AS no existe un MAC, se ha definido como MACo el valor del bytes menos significativo del AMID que existe en ambos equipos desde el principio.

El algoritmo para calcular el MAC es suministrado a los desarrolladores por el Administrador del Sistema AFT, y puede verse en el documento “Comunicaciones del Circuito de Carga”

4.4.3 Almacenamiento de variables en memoria no volátil

Tanto la AS como el POS deberán guardar las variables WKAP y MAC en memoria no volátil, de tal forma que en caso de corte de energía estos valores no se pierdan y puedan ser recuperados.

4.4.4 Variables de partida (condición cero)

Para poder atender la partida del sistema o el reemplazo de uno de los equipos de estos pares, se fija como valor para la condición cero las siguientes:

- WKAPcero = AMID (identificación de la AS) de 8 bytes.
- MACcero = primer byte del AMID (el menos significativo o el de más a la derecha)

Estos valores los dispone la AS en su memoria fija y no varían nunca. Para el caso del POS, se ha definido la función que el valor del AMID debe ser incorporado a dichos equipos en el momento en que una AS se conecta a ellos, ya sea en condición cero o bien en el caso de un reemplazo de una AS o POS, es decir en el momento de conexión de una AS a un POS, se le debe incorporar a este último el AMID respectivo y ser almacenado en memoria no volátil junto al POSID.

De esta forma en caso de requerirse la condición cero, tanto la AS como el POS podrán disponer de estas variables.

4.4.5 Análisis de Condiciones de Borde

4.4.5.1 Partida del sistema (condición cero)

Al instalarse una AS a un POS, se deberá incorporarse los datos de configuración iniciales que se utilizarán para el reconocimiento, inicialización y las restantes operaciones de ahí en adelante, algunos de estos datos iniciales son el valor del identificador de la AS "AMID", el valor del identificador único del POS "POSID", con ello el POS contará con el WKAPcero y el MACcero para comenzar su operación. Otros valores que deben ser configurados son el RUN Distribuidor, Run Cajero, Pin del Cajero.

4.4.5.2 Corte de energía en uno de los equipos

Si alguno de los equipos pierde energía, al disponerse las WKAP y los MAC en memoria no volátil, podrán recuperar dichos valores para ejecutar los comandos.

4.4.5.3 Corte de energía en ambos equipos

Si ambos equipos pierden energía, al disponerse las WKAP y los MAC en memoria no volátil, podrán recuperar dichos valores para ejecutar los comandos.

4.4.5.4 Reemplazo de la AS

Si se reemplaza la AS, significa que se dispone de un nuevo "conjunto" de equipos en dicho lugar, situación que debe reflejarse para las validaciones en el SIM (nuevo) y en el HSA. Dado esto, al POS se le debe ingresar el nuevo AMID y generar la condición cero. La AS por ser nueva, viene con condición cero prefijada en su SIM.

Corresponderá en esta situación que el primer conjunto de comandos a realizar sea el de Reconocimiento y luego el de Inicialización para poder trabajar.

4.4.5.5 Reemplazo del POS

Si se reemplaza el POS, significa que también se dispone de un nuevo conjunto de equipos en dicho lugar, situación que debe reflejarse para las validaciones del SIM (antiguo) y el HSA. Ello obliga a ingresar al POS el AMID respectivo y generar los comandos del Reconocimiento y de la Inicialización.

El POS estará en condición cero con el AMID respectivo, sin embargo la AS estará con WKAP y MAC antiguos. Al recibir el comando descifrará con la WKAP almacenada y obtendrá un comando no reconocido y/o un MAC no válido. Ante esta situación, la AS intentará por su sola descifrar con su WKAPo (el AMID) y obtener el valor del comando CEAP y el MAC cero respectivo. Si no es así deberá rechazar la operación.

El Clearing dejará en un servidor FTP los archivos de Intercambio de Información, El clearing pone a disposición de los usuarios del sistema la información procesada por los Módulos que lo conforman en cuentas y casillas Ftp que se estructuran de la siguiente manera:

\Intercambios\Redes

Para cada uno de estos directorios se debe crear la siguiente estructura Interna de directorios:

IN

OUT

INBKP

OUTBKP

Log

5 Catálogo de mensajes, especificando su origen y destino

5.1 Catálogo de mensajes del POS al Switch

Errores en la TIP03/TIP		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
ERROR_TERMINAL_INVALIDA	96	
ERROR_EN_SESION_HSA	97	
ERROR_EN_HSA	98	

Errores en la TCCT		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
OPERADOR_NO_EXISTE	400	TTAM
CAJERO_NO_EXISTE	402	TTAM, TGRT
PIN_INVALIDO	403	TTAM, TGRT
RUT_OPERADOR_NO_EXISTE	401	
CONVENIO_INVALIDO	404	TGRT
ESTADO_DE_CONVENIO_INVALIDO	405	TGRT
SALDO_TRANSACCION_INVALIDO	406	
MONTO_INVALIDO	407	
APERTURA_YA_EFECTUADA	408	
APERTURA_YA_EFECTUADA_POR_CAJERO_DISTINTO	455	

Errores en la TACCT/TIP/TCAM/TCMR		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
ID_CONTEXTO_SWITCH_ANTERIOR_NO_EXISTE	511	

Errores en la TTAM		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
NO_EXISTE_APERTURA_PREVIA_DE_CAJA	406	
CIERRE_EFECTUADO	407	
CUPO_DEVUELTO_ERRONEO	410	
ERROR_AL_OBTENER_EL_CANAL	409	

Errores en la TTAM2		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
WKSIM_INCORRECTA	501	
ERROR_AL_OBTENER_SESION_DESCARGA	502	

Errores TCMR		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
TARJETA_NO_EXISTE	411	TCMM,TGRT,FVRA01
TARJETA_EN_LISTA_NEGRA	412	TCMM,TGRT,FVRA01
ERROR_NO_EXISTE_RA	420	

Errores TCMM		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
SECUENCIA_INVALIDA	410	
MANDATO_NO_EXISTE	415	
FECHA_MANDATO_INVALIDA	421	
TARJETA_CON_SALDO_RA_DISPONIBLE	423	
MONTO_SOLICITADO_INVALIDO	422	
ESTADO_DE_MANDATO_INVALIDO	416	FVRA01

Errores FVRA01		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
CONTRATO_EN_LISTA_NEGRA	413	
CONVENIO_NO_EXISTE	415	
MONTO_BAJO_EL_MINIMO	417	
MONTO_BAJO_EL_MAXIMO	418	
MONTO_NULO	419	
RUN_PORTADOR_INVALIDO	421	

Errores Comunes		
<i>Descripción</i>	<i>Código</i>	<i>Uso Adicional</i>
ERROR_BASE_DATOS	99	
ERROR_AL_INSERTAR_TRANSACCION	601	
LLAVES_DES_NO_EXISTE_PARA_SWITCH	100	
LLAVES_RSA_NO_EXISTEN	100	
FECHA_CONVENIO_INVALIDA	102	
LLAVE_POS_INVALIDA	103	
LLAVE_SIM_INVALIDA	104	
DEMASIADAS_SESIONES_ABIERTAS	419	
ERROR_MODIFICAR_LLAVE_POS	600	
ERROR_INSERTAR_TRANSACCION	601	
ERROR_AL_ACTUALIZAR_LLAVES_RSA	607	
ERROR_AL_VALIDAR_POS	607	
ERROR_GENERICO	707	
ERROR_COMUNICACION_HSA	1000	
ERROR_LOTE_SIN_INICIAR	2000	
ERROR_COMUNICACION_POS	3000	
MEDIO_DE_ACCESO_CON_IDENTIFICACION_DUDOSA	666	
ERROR_RA_EMERGENCIA_EXISTENTE	500	

5.2 Catálogo de mensajes de AS al POS

Código	Descripción
9000	Comando finalizado exitosamente
9010	Se ha producido un error con el RTC interno
9601	CKS incorrecto. El Checksum CKS presentado en Data no coincide con el checksum CKS esperado por el SIM
9602	AMID incorrecto. El identificador AMID presentado en Data no coincide con el identificador AMID esperado por el SIM
9603	POSID incorrecto. El identificador POSID presentado en Data no coincide con el identificador POSID esperado por el SIM
9604	No se ha cargado el POSID. El identificador POSID debe ser cargado antes de invocar el comando
9606	No se ha cargado la WK1SIM. La clave WK1SIM debe ser cargada antes de invocar el comando
9607	No se ha cargado la WKAP. La clave WKAP debe ser cargada antes de invocar el comando
9608	Valor incorrecto de parámetro P1. El valor del parámetro P1 no corresponde al esperado por el comando
9609	SIM anulada. No es posible ejecutar el comando por que el SIM está anulado
9610	Lc incorrecto. El largo del dato que se intentó ingresar no corresponde al definido para este comando
9611	INS no soportado. El comando no está definido en esta aplicación
900A	Ha caducado el saldo del contrato #3 y se informa el monto
900B	Se ha renovado el saldo del contrato #3 previo a la carga
900C	Tarjeta Inhabilitada
900D	Se ha bloqueado un Contrato en la TM por LN
900F	Se requiere una pronta inicialización
960A	La SIM no ha sido personalizada. La tarjeta SIM no contiene datos válidos para operar en el sistema, debe ser personalizada
960B	Valor incorrecto de parámetro P2. El valor del parámetro P2 no corresponde al esperado por el comando
960C	Valor incorrecto de datos HSM. Uno o más identificadores enviados en el bloque 1 no coinciden con los que espera el SIM
960D	SIM bloqueada. El número de intentos permitidos para la presentación en falso de un identificador fue excedido
960E	El comando no es el esperado. La tarjeta está ejecutando un comando que ingresa datos en más de un bloque y no se ha comprobado el ingreso de datos
960F	El comando esta fuera de secuencia. La tarjeta está ejecutando un comando que ingresa datos en más de un bloque y el identificador del bloque no corresponde al esperado

Código	Descripción
9FF0	Slot de SmartCard incorrecto
9FF1	Timeout en la recepción de la SmartCard
9FF2	APDU invalido
9FF3	Largo invalido
9FF4	Status Byte invalido
9FF5	Procedre Byte invalido
9FF6	Timeout en la recepción del ATR en el PowerUp
9FF7	ATR invalido
9FF8	SmartCard no energizada
9FF9	Protocolo no soportado
9FFF	El modulo SIM no responde
9XXX	Error no documentado
FB00	El saldo efectivo del SIM es insuficiente para realizar la operación CCMT
FB01	El SIMID enviado a la AM no coincide con el obtenido por el SIM
FB02	El SIM no puede encriptar con la MKSIM
FB03	El saldo efectivo del SIM es distinto a cero
FC00	El módulo Mifare no responde
FC01	No existe una tarjeta en el rango de la antena
FC02	La autenticación del sector no ha sido exitosa
FC03	La lectura del bloque no ha sido exitosa
FC04	La escritura del bloque no ha sido exitosa
FC0D	El Bloque Valor se encuentra corrupto
FC0E	El CRC del bloque de datos es incorrecto
FC0F	La tarjeta a grabar no coincide con la utilizada en la lectura
FC10	El bloque de respaldo no coincide con el original
FC11	Existe más de una tarjeta en el rango de la antena
FC12	Enviar usuario a otro AS-VAL para reparar la tarjeta
FC13	Enviar usuario al CAE para reparar la tarjeta
FC14	Se reparó exitosamente la tarjeta
FD00	La TM se encuentra inhabilitada para su uso
FD01	El Monto a cargar en la TM no se encuentra en el rango permitido
FD02	La versión de la TM se encuentra fuera de vigencia
FD03	La TM o el Contrato de la TM se encuentra inhabilitada por la Lista Negra
FD04	Los Contratos de la TM son incompatibles para el Tipo de Contrato
FD05	El SN enviado por el POS no coincide con el obtenido por la TM
FD06	El SN procesado previamente por la AM no coincide con el obtenido por la TM
FD07	El SN obtenido de la TX de la AM no coincide con el obtenido por la TM
FD08	Ha expirado el plazo de devolución de la TM
FD09	La Versión del Aplicativo de la TM se encuentra fuera de vigencia

Código	Descripción
FD0A	La Versión Alternativa del Aplicativo de la TM no se encuentra operativa
FD0B	El Perfil de la TM se encuentra inhabilitado para su uso
FD0C	La Fecha de Inicio del Perfil de la TM se encuentra fuera de vigencia
FD0D	La Fecha de Fin del Perfil de la TM se encuentra fuera de vigencia
FD0E	La TM se encuentra bloqueada por Lista Negra
FD0F	La TM se encuentra bloqueada temporalmente
FD10	El Contrato Monedero de la TM se encuentra fuera de vigencia
FD11	La TM no se encuentra activada
FD12	El Nro. de TM externo enviado por el POS no coincide con el obtenido por la TM
FD13	Ha expirado el tiempo de anulación de la TX
FD14	El Monto de anulación de la TX no coincide con el procesado previamente en la TM
FD15	El Monto a cargar en la TM es insuficiente para la compra del plástico + la carga mínima
FD16	El Tipo de Contrato a cargar no coincide con el Contrato existente en la TM
FD17	No es posible anular una TX de venta y carga de la TM
FD18	El NTT de la TM se encuentra fuera del rango permitido para la anulación de la TX
FD19	No existen TX para anular en la AM que correspondan a la TM
FD1A	El Monto de devolución no coincide con el obtenido por la TM
FD1B	No existe precio del plástico para el tipo de tarjeta obtenido por la TM
FD1C	La Versión de Claves de la TM se encuentra fuera de vigencia
FD1D	El IRG no coincide por el enviado por la AM
FD1E	Ha expirado el tiempo de uso del IRG
FD1F	No es posible desbloquear la TM por no estar personalizada
FD20	No es posible desbloquear la TM por no coincidir el RUT
FD21	No es posible desbloquear/emitir la TM por estar habilitada
FD22	No es posible desbloquear la TM por no estar bloqueada temporalmente
FD23	No es posible desbloquear la TM por no estar en LN
FD24	No es posible desbloquear la TM por estar los perfiles fuera de vigencia
FD25	No es posible desbloquear la TM por estar la FAT fuera de vigencia
FD26	No es posible emitir la TM por estar ya emitida
FD27	No es posible cambiar el TTA por estar la Tarjeta Emitida
FD28	Contrato disponible no recargable
FD29	Contrato #1 con menor daño
FD2A	Contrato #2 con menor daño
FD2B	Ha expirado el tiempo de venta del contrato
FD2C	No existe lugar en la TM para la carga del contrato
FD2D	No se han cumplido ninguna regla de asignación de espacios en los contratos
FE00	La Versión de la tabla AM difiere al obtenido del HSM

Código	Descripción
FE01	El CheckSum de la tabla AM difiere al obtenido del HSM
FE02	Se ha producido un error en la grabación de la tabla AM solicitada
FE03	Se ha producido un error en la lectura del registro de la tabla de TX
FE04	Se ha producido un error en el borrado del registro de la tabla de TX
FE05	Se ha producido un error al inicializar la tabla de TX
FE06	Se ha producido un error en la grabación del registro de la tabla de TX
FE07	Se ha producido un error en la grabación del registro de la tabla de PiggyBack
FE08	La tabla AM no se encuentra en el rango permitido
FE09	El registro o bloque de la tabla AM no se encuentra en el rango permitido
FE0A	Se ha producido un error en la lectura del registro de las tablas AM para el calculo del CheckSum
FE0B	El registro de la Tx a descargar no se encuentra en el rango permitido
FE0C	No es posible completar el comando solicitado por existir TX sin descargar
FE0D	El Tipo de Contrato no se encuentra en la tabla de Contratos/Precios de la AM
FE0E	La tabla de TX no posee espacio suficiente para las nuevas TX.
FE0F	La Inicializacion del FS no pudo ser completada.
FE10	No se ha habilitado una descarga de firmware desde el HSA.
FF00	El Monto a cargar en la TM supera el máximo permitido
FF01	El POSID/VALID enviado por el POS/VAL no coincide con el almacenado en la AM
FF02	El CKS calculado del firmware no coincide con el asignado en la AM
FF03	El Registro AM solicitado no se encuentra en el rango permitido
FF04	El Registro AM solicitado se encuentra protegido ante escritura
FF05	No se ha podido grabar el nuevo valor en el Registro AM solicitado
FF06	No se ha podido leer el Registro AM de protección de escritura
FF07	El Registro AM solicitado no permite protección ante escritura
FF08	No es posible vender una TM a través del Medio de Pago RA o Mandato
FF09	El Medio de Pago no está habilitado para el Tipo de Contrato utilizado
FF0A	El #SEC enviado por el POS no coincide con el almacenado en la AM
FF0B	La secuencia de inicialización de la AM es incorrecta o está incompleta
FF0C	El Medio de Pago no está permitido para el comando solicitado
FF0D	El Tipo de Contrato no está permitido para el comando solicitado
FF0E	El comando solicitado no se encuentra habilitado
FF0F	El comando solicitado no es reconocido
FF10	El Nro. intentos sin inicialización ha llegado el máximo permitido
FF11	No puede operar por falta de inicialización
FF12	El Tipo de Ajuste no se encuentra en el rango permitido
FF13	El RUT del Cajero enviado por el POS/VAL no coincide con el almacenado en el SIM

Código	Descripción
FF14	El CKSIM enviado por el POS es incorrecto
FF15	La fecha enviada por el POS/VAL supera a la fecha de inicio del Perfil
FF16	El CKS calculado del paquete de la tabla no coincide con el calculado por la AM
FF17	El valor de CONTP recibido por el Switch no coincide con el CONTP calculado en la AM
FF18	El Valor del Saldo del Cajero es incorrecto

5.3 Mensajería ISO 8583

La modalidad de comunicación soportada en esta mensajería es abrir socket sobre TCP/IP utilizando Mensajería ISO8583 Introduce el concepto de número de versión de mensaje para distinguir entre mensajes que cumplen con ésta o subsecuentes ediciones del estándar y las que cumplen con la edición de 1987. Para el caso de Red se utilizará la versión de 1993.

El estándar ISO8583:1993 define que cada mensaje debe componerse de al menos 3 de 5 elementos, indicados a continuación.

5.3.1 Identificador del Tipo de Mensaje (Obligatorio)

Este elemento es aquel que identifica al mensaje e indica el su función. Se compone de 4 dígitos numéricos, en que cada uno de estos, de izquierda a derecha, tendrá el siguiente significado:

- Primera posición: El número de versión del estándar.
- Segunda posición: La clase del mensaje.
- Tercera posición: La función del mensaje.
- Cuarta posición: El originador de la transacción.

Cada mensaje deberá comenzar, en forma obligatoria, con un Identificador del Tipo de Mensaje. El largo de este identificador será de 4 bytes. Los números de versión no deberán ser asignados como resultado de políticas internas.

5.3.1.1 Primera Posición – Número de Versión^[1]

0	ISO 8583:1987
1	ISO 8583:1993
2 – 7	Reservado para el uso de ISO.
8	Reservado para uso nacional.
9	Reservado para uso privado.

^[1] Esta posición siempre deberá contener el valor "1", ya que la mensajería definida en este documento se basa en la versión de 1993 del ISO 8583.

5.3.1.2 Segunda Posición – Clase del Mensaje^[2]

0	Reservado para el uso de ISO.
1	Autorización.
2	Financiera.
3	Transmisión de archivo.
4	Reversa.
5	Reconciliación.
6	Administrativa.
7	Cuotas.
8	Administración de Red.
9	Reservado para el uso de ISO.

5.3.1.3 Tercera Posición – Función del Mensaje^[3]

0	Requerimiento.
1	Respuesta al Requerimiento.
2	Aviso.
3	Respuesta al Aviso.
4	Notificación.
5 – 9	Reservado para el uso de ISO.

^[2] Esta posición siempre deberá contener el valor "2", ya que todas las transacciones del Sistema AFT serán consideradas como financieras desde el punto de vista del ISO 8583 de 1993.

^[3] Esta posición siempre deberá contener el valor "0" para los mensajes de requerimiento (que se generan en los puntos de acceso) ó "1" para los mensajes de respuesta (que se generan en el Switch).

5.3.1.4 Cuarta Posición – Originador de la Transacción^[4]

0	Adquiriente.
1	Repetición del Adquiriente.
2	Proveedor de la Tarjeta.
3	Repetición del Proveedor de la Tarjeta.
4	Otro.
5	Repetición de Otro.
6 – 9	Reservado para el uso de ISO.

5.3.2 Bitmap Primario (Obligatorio)

El estándar internacional ISO8583:1993 usa un concepto llamado “bitmap”, gracias al cual a cada elemento de dato le es asignado un indicador de posición en un campo de control, o “bitmap”. La presencia de un elemento de dato en un mensaje específico es indicado por un uno (1) en la posición (bit) asignada; la ausencia de un elemento de dato es indicado por un cero (0) en la posición (bit) asignada.

El Bitmap Primario es parte de la cabecera del mensaje, así como el Identificador del Tipo de Mensaje. Este bitmap tiene un largo de 8 bytes, representando en cada uno de sus 64 bits, de izquierda a derecha, la presencia o ausencia de un elemento de dato.

El Bitmap Primario siempre deberá estar presente en el mensaje.

5.3.3 Bitmap Secundario (Opcional)

Dado que el estándar ISO8583:1993 especifica que el mensaje puede contener hasta 128 elementos de datos, se hace necesaria la presencia de un segundo bitmap, o Bitmap Secundario, que permite indicar la presencia o ausencia de los restantes 64 elementos de datos.

Este Bitmap Secundario se encuentra exactamente después del Bitmap Primario y es considerado como el primer elemento de dato de los 128 posibles. Por lo anterior, si el Bitmap Secundario está presente en el mensaje, éste deberá indicarse, con un valor “1”, en el primer bit del Bitmap Primario. Este bitmap tiene un largo de 8 bytes, representando en cada uno de sus 64 bits, de izquierda a derecha, la presencia o ausencia de un elemento de dato.

El Bitmap Secundario no es utilizado en la mensajería de Operador.

^[4] Esta posición siempre deberá contener el valor “0”.

5.3.4 Datos asociados al Bitmap Primario (Obligatorios)[5]

A continuación se detallarán solamente los campos utilizados en la mensajería para contener las transacciones de Operador.

47	Datos adicionales de uso nacional	ANS(..999)	Opcional. Largo variable. Debe llevar, al inicio, 3 bytes adicionales a los 999 máximos, indicando el largo de la data.
48	Datos adicionales de uso privado	ANS(..999)	Mandatorio. Largo variable. Debe llevar, al inicio, 3 bytes adicionales a los 999 máximos, indicando el largo de la data.

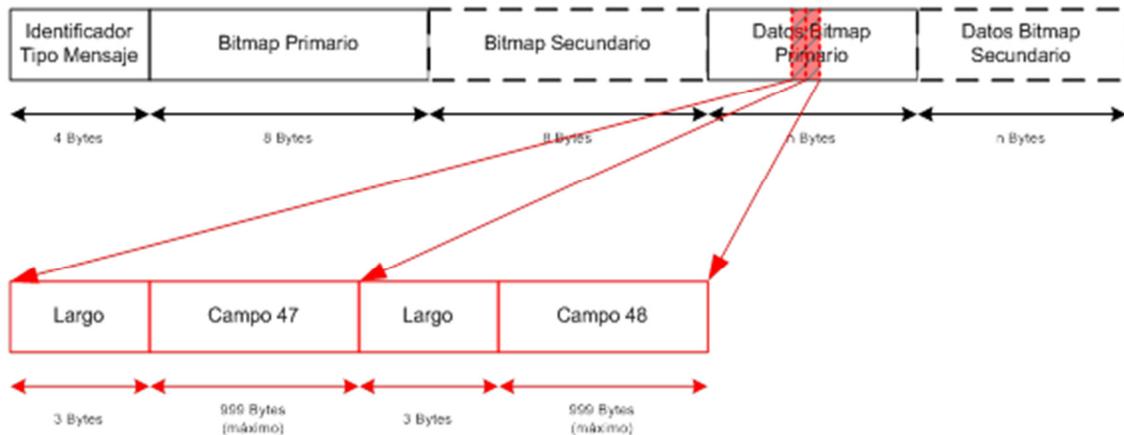
Las transacciones se enviarán como una cadena de caracteres en el campo AdditionalDataNational (campo N° 48) del estándar ISO8583:1993, a partir de la cual se rescatará con el fin de ser procesada por el Switch.

Los datos que no puedan ir en la estructura de la transacción, como aquellos que van y vienen hacia y desde el HSA, serán enviados como una cadena de caracteres en el campo AdditionalDataPrivate (campo N° 47) de la estructura ISO8583:1993, a partir de la cual se rescatará con el fin de ser procesada por el Switch.

El campo 47, dado su uso y su variabilidad, será explicado en forma particular en cada transacción que lo utilice.

5.3.5 Formato de la Mensajería

Cada mensaje deberá tener el siguiente formato:



[5] Refiérase al ISO 8583 de 1993 para un mayor detalle de los campos asociados al Bitmap Primario.

5.3.5.1 Campo 48

Este elemento de dato del ISO8583:1993 contendrá el requerimiento, y la respuesta, alternativamente, de las transacciones de Operador, cuyos formatos se especificarán más adelante. El largo de este elemento de dato es variable y puede llegar a tener un máximo de 999 bytes.

Además, antecediendo al elemento de dato, deberán ser incluidos 3 bytes que se utilizarán para indicar el largo real del campo 48. Este largo deberá ser especificado como un valor numérico entero ASCII, indentado a la derecha y rellenado con ceros a la izquierda.

Campos de Datos

Los campos de datos son los elementos de datos que componen la transacción de Operador y que irán en el campo 48. Corresponden a los campos asociados a cada transacción; y la presencia o ausencia de ellos depende de la transacción que se está ejecutando.

Los campos de datos que irán en el campo 47 dependerán de la transacción que se esté ejecutando, y serán especificados en la descripción de cada una de estas transacciones.

Todos los campos de datos que se utilizarán en el campo 48, que definen a la transacción, son de largo fijo.

Se utilizará la siguiente nomenclatura para especificar cada campo de dato del campo 48:

ID Campo

Corresponde a un número que identifica en forma única al campo de dato en la especificación de la transacción.

Nombre Switch

Nombre asignado al campo de dato internamente al Switch.

Nombre Operador

Nombre asignado al campo de dato por Operador.

Tipo del Campo

Atributo asociado a cada uno de los campos de datos. Los posibles atributos son los siguientes:

Atributo	Significado
N	Dato Numérico.
B	Dato Binario.
ANS	Dato Alfanumérico y caracteres especiales.

- **Dato Numérico (N):** Este tipo de dato corresponde a valores numéricos enteros. Su representación deberá estar en hexadecimal y en nibbles. Lo primero significa que el valor numérico en notación decimal deberá ser transformado a notación hexadecimal; y lo segundo significa que cada dígito hexadecimal deberá ser puesto en un nibble, es decir, cada dígito deberá ir en un medio byte.

Además de lo anterior, los datos numéricos deberán estar indentados a la derecha y rellenos con ceros a la izquierda, hasta completar el largo especificado para ese dato. Si el contenido ocupa un valor impar de nibbles, se le deberá agregar uno más a la izquierda para completar una cantidad par de los mismos, y, por ende, tener cantidades enteras de bytes.

Por ejemplo, si deseamos poner en un campo de dato de tipo numérico el valor "1038" (decimal), lo primero es transformarlo a notación hexadecimal, lo cual nos daría el valor "40E" que tiene tres dígitos. Este valor no nibbleado ocuparía tres bytes, ya que cuenta con tres dígitos; pero si deseamos pasarlo a nibbles, el dato utilizará un byte y medio, es decir, la mitad de los bytes originales. Como la cantidad de nibbles es impar, se le deberá agregar un nibble más a la izquierda completando así cuatro nibbles (dos bytes); y este cuarto nibble deberá contener un cero. Finalmente el dato numérico quedará como "040E" (asumiendo que el largo del campo es de dos bytes), siendo éste el que se deberá enviar en la transacción.

La notación para este tipo de dato será N(<n>), donde <n> indica la cantidad máxima de dígitos que deberá tener el valor numérico. A partir de este valor se puede deducir el largo físico que tendrá el dato numérico en la transacción; es decir, $\frac{n}{2}$ cuando n es par y $\frac{n+1}{2}$ cuando n es impar, corresponde a la cantidad de bytes que físicamente ocupará en la transacción.

- **Dato Binario (B):** Este tipo de dato corresponde a valores que tienen una interpretación de su contenido bit a bit, o que éste no tiene una interpretación numérica u alfanumérica tradicional. Para el primer caso se puede poner como

ejemplo el campo "Bitmap" de la transacción, cuya interpretación es bit a bit, ya que cada uno de éstos indica la presencia o ausencia de los distintos datos. Para el segundo caso se puede poner como ejemplo el campo "PiggyBack", cuya interpretación interna no es ni numérica ni alfanumérica.

La notación para este tipo de dato será B(<n>), donde <n> indica la cantidad máxima de bits que deberá tener el valor binario. A partir de este valor se puede deducir el largo físico que tendrá el dato binario en la transacción; es decir, corresponde a la cantidad de bytes que físicamente ocupará en la transacción.

- **Dato Alfanumérico (ANS):** Este tipo de dato corresponde a valores con caracteres alfabéticos y numéricos. Su representación será literal; es decir, cada carácter de este dato ocupará un byte en la transacción.

Además de lo anterior, los datos alfanuméricos deberán estar indentados a la izquierda y rellenados con blancos (espacios) a la izquierda, hasta completar el largo especificado para ese dato.

La notación para este tipo de dato será ANS(<n>), donde <n> indica la cantidad máxima de caracteres que deberá tener el valor alfanumérico. A partir de este valor se puede deducir el largo físico que tendrá el dato alfanumérico en la transacción; es decir, *n* corresponde a la cantidad de bytes que físicamente ocupará en la transacción.

La única excepción a esta regla corresponde a los campos "FhoTransaccion" y "FhoRegistro", que, siendo de tipo alfanumérico, deberán ir además nibbleados (ver la explicación dada en el punto del dato numérico).

Largo del Campo

Largo real, en bytes, del campo de dato.

- Todos los campos, independiente del tipo de atributo, son de largo fijo.
- Los datos que contendrán RUNes irán sin puntos, sin guión y sin dígito verificador.
- Los campos 36 al 64 no deberán ir en ninguna transacción, ya que su uso no está determinado aún.
- Sólo irán aquellos campos que estén indicados en el Bitmap con un valor "1". Lo anterior implica que la posición de cada uno de los campos se determinarán en base al largo fijo de los mismos.

Vista la explicación anterior podemos indicar que los datos que se usarán en las distintas transacciones de Operador son los siguientes:

ID Campo	Nombre Switch	Nombre Operador	Tipo y Largo del Campo
48.01	Bitmap	Bitmap	B(64), 8 bytes
48.02	CodTransaccion	CodTx	ANS(5), 5 bytes
48.03	IdContextoSwitch	#SEC Switch	N(16), 8 bytes
48.04	NumTarjetaInterno	#Tmser	N(16), 8 bytes
48.05	NumTarjetaExterno	#Tmex	N(16), 8 bytes
48.06	RUNTarjetaHabiente	RUT	N(16), 8 bytes
48.07	RUNPortador	RUNP	N(16), 8 bytes
48.08	FhoTransaccion	FhoTx	ANS(7), 7 bytes
48.09	CodPACC	AMID	N(16), 8 bytes
48.10	NumSecuencia	#SECAM	N(16), 8 bytes
48.11	FhoRegistro	TimeStamp	ANS(7), 7 bytes
48.12	RUNDistribuidor	RUND	N(16), 8 bytes
48.13	RUNCajero	Run Cajero	N(16), 8 bytes
48.14	PINCajero	PIN	ANS(8), 8 bytes
48.15	Sesion	Sesion	N(2), 1 byte
48.16	CodCAU	CodCAU	N(2), 1 byte
48.17	IdCuenta	#TC/#TD	ANS(24), 24 bytes
48.18	CodAutorizacion	Cod. Aut.	ANS(8), 8 bytes
48.19	NumRA	#RA	N(16), 8 bytes
48.20	MtoSolTransaccion	\$x	N(16), 8 bytes
48.21	MtoTransaccion	\$x	N(16), 8 bytes
48.22	IdContextoSwitchAnterior	#SEC Ant.	N(16), 8 bytes
48.23	PiggyBack	Pb	B(192), 24 bytes
48.24	CodResultado	C A/R	N(16), 8 bytes
48.25	SaldoTotalRA	SaldoTotRA	N(16), 8 bytes
48.26	PINTarCreDebito	PIN	B(64), 8 bytes

ID Campo	Nombre Switch	Nombre Operador	Tipo y Largo del Campo
48.27	RUNTarCreDebito	RUN	N(16), 8 bytes
48.28	OtroDatoTarCreDebito	OtroDato	ANS(16), 16 bytes
48.29	SIM_ID	SIMID	B(64), 8 bytes
48.30	WorkingKey	WK	B(64), 8 bytes
48.31	CKSIM	CKSIM	B(8), 1 byte
48.32	NumTxConsecutivas	#TxCon	N(4), 2 bytes
48.33	POS_ID	POSID	N(16), 8 bytes
48.34 (1)	TXOffLine (FVRA03 – Req.)	TXOffLine	B(256), 40 bytes
48.34 (2)	TXOffLine (FVRA03 – Resp.)	TXOffLine	B(512), 72 bytes
48.34 (3)	TXOffLine (FROL00 – Req.)	TXOffLine	B(400), 62 bytes
48.35	CodContrato	CodContrato	N(4), 2 bytes
48.36 – 48.64	[Para Uso Futuro]		