ANEXO 4I

Especificación Técnica Indicadores

Descripción de tokens

- TOKEN Q1

Este token lleva el modo de autorización con valores que indican si fue autorizado fuera de línea (stand in), o si es una transacción autorizada con listas positivas u otros casos.
Puede ser calificado de origen por el Adquirente (autorización off-line del negocio) y debe ser retornado forzosamente por el Emisor.
Este token debe informarse a nivel batch.

- TOKEN Q2

Este token indica el dispositivo de entrada de la transacción. (ejemplo: terminal pos, autorización voz, cargos automáticos, e-commerce, etc.).
Este token debe informarse a nivel batch.

- TOKEN Q6

Contiene indicadores para Pagos Diferidos.
Este token debe informarse a nivel batch.

- TOKEN 04

Este token contiene el resultado de la Validación del CVV2/CVC2.
Este token debe informarse a nivel batch.

- TOKEN C0

Contiene el valor del CVV2 o CVC2 además del nivel de Seguridad en una transacción de Comercio Electrónico.
Este token debe informarse a nivel batch.

- TOKEN C4

Este token sirve para indicar las capacidades de la Terminal (Lector de Banda Magnética o de Chip, etc.), así como si el tarjetahabiente está presente durante la transacción.
Este token debe informarse a nivel batch.

- TOKEN C6

Este token aloja los datos de autenticación del tarjetahabiente. Aplica a transacciones E-Commerce realizadas con tarjetas de marca VISA, bajo el esquema VERIFIED BY VISA.
Este token no se intercambia a nivel batch.

- TOKEN CE

Este token aloja los datos de autenticación del tarjetahabiente. Aplica a transacciones E-Commerce, realizadas con tarjetas marca MASTERCARD bajo el esquema SECURE CODE.
Este token no se intercambia a nivel batch.

- TOKEN R4

Token para indicar el número de contrato en transacciones de cargos Periódicos.
Este token no se intercambia a nivel batch.

- TOKEN CZ

Indica el tipo de dispositivo de pago utilizado por el tarjetahabiente en transacciones contactless (ejemplo: tarjeta, dispositivo móvil, sticker, etc.).
Este token puede informarse a nivel batch.

- TOKEN B1

Contiene el nombre de la institución emisora que cobra una comisión por uso de línea de crédito a su tarjetahabiente. Este token es utilizado para presentar el nombre de la institución en pantalla.
Se utiliza en los mensajes de respuesta.
Este token no se intercambia a nivel batch.

- TOKEN B2

Contiene los datos principales para hacer una solicitud de autorización EMV, este token es enviado por el Adquirente al Emisor.
Integra los valores con los que es calculado el ARQC.
Se utiliza en los mensajes de solicitud de autorización.
A nivel batch se intercambia únicamente el valor del ARQC.

- TOKEN B3

Contiene datos secundarios para hacer una solicitud de autorización EMV, este token es enviado por el Adquirente al Emisor.
Indica el resultado de la validación entre la tarjeta y el dispositivo cuyos valores son discrecionales utilizados en los mensajes de solicitud.
Brinda apoyo al Emisor en la toma de decisión para la aprobación de la transacción EMV.
A nivel batch no se intercambia este token.

- TOKEN B4

Contiene información acerca del tipo de transacción de autorización, como la capacidad de la terminal o la manera en que la tarjeta fue leída, este token es enviado por el Adquirente al Emisor.
Muestra la calificación y estatus de los elementos que son considerados en una transacción EMV.
Se utiliza en los mensajes de solicitud.
A nivel batch no se intercambia este token.

- TOKEN B5

Contiene la información de respuesta EMV, como el criptograma de respuesta ARPC y banderas para el manejo de Scripts, este token es enviado por el Emisor hacia el Adquirente.
Integra el resultado de la validación por parte del Emisor de una transacción EMV incluyendo el ARPC y los indicadores para asociar los scripts incluidos en otro token. Se utiliza en los mensajes de respuesta.
A nivel batch no se intercambia este token.

- TOKEN B6

Contiene Scripts de configuración para el chip enviados por el Emisor al Adquirente.
Considera los scripts generados por el Emisor para otorgar instrucciones hacia el chip de a la tarjeta. Se utiliza en los mensajes de respuesta.
A nivel batch no se intercambia este token.

- TOKEN BJ

Contiene el comando que indica la ejecución correcta del script por el Emisor al Adquirente.
Muestra la confirmación de la correcta ejecución de los Scripts de la transacción original.
A nivel batch no se intercambia este token.

- TOKEN 25

Contiene el monto de Surcharge (comisión del adquirente) que será cobrado al tarjetahabiente.
Se utiliza en los mensajes de solicitud de autorización.
A nivel batch no se intercambia este token.

- TOKEN 30

Contiene el monto de Loyalte Fee (comisión por uso de línea de crédito) que será cobrado al tarjetahabiente.
Se utiliza en los mensajes de respuesta.
A nivel batch no se intercambia este token.

Consideraciones al uso de tokens

Criterios para E-Commerce

Para considerar como válidos los Indicadores de E-Commerce deben estar calificados, con 9 en el token Q2.

Para una transacción de 3Dsecure con autenticación del tarjetahabiente deberán estar presentes los tokens que se mencionan a continuación:

- Token Q2 subcampo 1 (valor 9)
- Token 04 subcampo 3 (valor “ ”)

- Token C4 subcampo 3 (valor 2), subcampo 4 (valor 5), subcampo 5 (valor 1), subcampo 10 (valor 6)
- Token C0 subcampo 1 (validar que este poblado con cuatro caracteres CVV2, CVC2 o “”), subcampo 8 (valor 0,1,2 o 9), subcampo 10(0,1,2), subcampo 12 (Valores validos 0,1,2,3,4,5,6,7), subcampo 5 (valor 5,6,7) en caso de que este campo tenga un valor de 5 se debe validar que este poblado el Token C6 para Visa y el Token CE para MasterCard

Para una transacción con promoción deben estar poblados, los subcampos 1, 2 y 3 en el token Q6 según corresponda la promoción de acuerdo al numeral 3.2.4 de este documento

El valor 7 (COMERCIO ELECTRONICO POR CANAL SEGURO NO AUTENTICADO) es un ECI válido para transacciones de e-commerce, sin embargo será prerrogativa del Emisor autorizar o rechazar transacciones marcadas con este valor en el subcampo 5 token C0. Las transacciones con este ECI no incluirán los tokens C6 y CE.

Consideraciones para transacciones de E-Commerce bajo el esquema 3D Secure

Naturaleza excluyente de los tokens C6 y CE. Sólo viajará en el token que corresponda a la marca de la tarjeta, es decir, C6 para tarjetas marca Visa y CE para tarjetas marca MasterCard, siempre que el valor del ECI sea 5 o 6 (Atempts)

TOKEN C0 SUBCAMPO 5		
Valor	**Descripción Subcampo**	**Observaciones**
Valores de una transacción bajo el esquema 3D Secure		
5	Comercio seguro, titular autenticado (3D Secure)	Debe contener los indicadores de AVV/UCAF o CAVV, calculados por ACS.
6	Comercio seguro, titular no autenticado (3D Secure)	Contiene los indicadores de AVV/UCAF o CAVV, calculados por EL EMISOR (ACS), **NO** podrán ser poblados por el Adquirente (MPI) con valores default. En el caso del ECI 6 únicamente deberá venir poblado cuando la marca genere un Atempt.
Valores de una transacción de Comercio electrónico sin autenticación		
7	Autenticación 3D Secure no realizada	La autenticación 3D Secure no se llevó a cabo

Se incluye una “Bandera de Resultado de Validación de CAVV / UCAF-AAV”, en el subcampo 12 del token C0 para que el Emisor informe el resultado de la validación de ese dato. Esta bandera deberá ser calificada en todos los mensajes ISO de respuesta a solicitud de autorización (210)

Transacciones MO/TO

Una transacción MOTO debe llevar el valor 08 en token Q2 que identifica el medio de acceso para las transacciones MO/TO de acuerdo al MCC que le corresponda y que sea una transacción manual, indicado en el POS Entry Mode con valor 01.

Para considerar como válidos los Indicadores de Transacciones MO/TO se debe validar el token C4 en el subcampo 3 (valor 3), subcampo 4 (valor 1,2,3), subcampo 5 (valor 1), subcampo 12 (valor 4).

Token C0, subcampo 5 (valor 1), subcampo 8 (valor 0, 1, 2, 9); si el subcampo 8 tiene el valor 9, el subcampo 1 no se debe de validar.

Cuando la transacción MOTO sea autenticada debe contener los valores de autenticación.

Consideraciones para transacciones con Pagos Diferidos

Las promociones podrán ser habilitadas en comercios de acuerdo a las especificaciones del Campo 63 Token Q6 en el proceso online y en el archivo de intercambio Batch de 350 posiciones.

Token Q6		
Sub campo	**Nombre**	Valores válidos
1	Diferimiento	Numero de Meses en el que el pago no será exigible (compre hoy y pague después), justificado con ceros y no espacios a la izquierda
2	Número de pagos	Número de meses en que se va a dividir los pagos (con o sin intereses) justificado con ceros y no espacios a la izquierda
3	Tipo de plan	Tipo de plan a utilizarse 00.- Sin promoción 03.- Sin intereses al tarjetahabiente 05.- Con Intereses para el tarjetahabiente 07.- Compre hoy y Pague después (Skip Payment Puro).

- **EJEMPLOS:**

Los plazos de meses sin intereses se arman COMO SE DESCRIBE A CONTINUACIÓN:

6 meses sin intereses:
    - 00 06 03

12 meses sin intereses:
    - 00 12 03

Los plazos de meses con intereses se arman COMO SE DESCRIBE A CONTINUACIÓN:

3 meses con intereses:
    - 00 03 05

9 meses con intereses:
    - 00 09 05

Los plazos de skip payment PURO se arman COMO SE DESCRIBE A CONTINUACIÓN: (EN ESTE CASO NO HAY DIFERIDO Y SE VA A REVOLVENTE A PARTIR DEL MES INDICADO)

Compre hoy y pague en 3 meses:
    - 03 00 07

Compre hoy y pague en 4 meses:
    - 04 00 07

Los plazos de skip payment + meses sin intereses se arman de la siguiente forma:

3 meses de gracia + 6 meses sin intereses:
    - 03 06 **03**
    - El primer subcampo nos indica los 3 meses del salto.
    - El segundo subcampo nos indica los 6 meses en que la compra se va a parcializar.
    - El tercer subcampo nos indica que la compra es a meses sin intereses.

3 meses de gracia + 18 meses sin intereses:
    - 03 18 **03**
    - El primer subcampo nos indica los 3 meses del salto.
    - El segundo subcampo nos indica los 18 meses en que la compra se va a parcializar.
    - El tercer subcampo nos indica que la compra es a meses sin intereses.

Los plazos de skip payment + meses con intereses se arman de la siguiente forma:

3 meses de gracia + 6 meses con intereses:
    - 03 06 **05**
    - El primer subcampo nos indica los 3 meses del salto.
    - El segundo subcampo nos indica los 6 meses en que la compra se va a parcializar.
    - El tercer subcampo nos indica que la compra es a meses con intereses.

3 meses de gracia + 18 meses con intereses:

- 03 18 **05**
- El primer subcampo nos indica los 3 meses del salto.
- El segundo subcampo nos indica los 18 meses en que la compra se va a parcializar.
- El tercer subcampo nos indica que la compra es a meses con intereses.

Consideraciones para transacciones en el modo de acceso de EMV.

Las transacciones deben contener un valor 05 en los primeros dos valores del campo 22. "POS Entry mode" cuando la transacción se realicen a través de la lectura del Chip.

El código de servicio extendido dentro del campo 35 (Track 2 Data) contendrá un 2xx (para las tarjetas internacionales) o un 6xx (para las tarjetas de uso nacional).

Los valores del terminal Capability, en el Token C4 subcampo 11, que pueden ser considerados como una transacción EMV son:

3 = Lector ContactLess Chip
5 = Lector de Banda y Lector de Chip EMV - compatible
8 = Lector de Banda, Entrada manual y Lector de Chip EMV -compatible
9 = Lector de Chip EMV - Lector exclusivamente de Chip – compatible

En estas transacciones, se puede hacer uso de los tokens B2, B3, B4, B5, B6, BJ, dependiendo de la implementación realizada por las instituciones involucradas.

Los emisores deben de realizar las validaciones pertinentes a los datos contenidos en el campo ARQC del Token B2, así como también el poder generar el Token de respuesta B5 debidamente llenado para todas las transacciones bajo el esquema EMV; y de la misma manera, debe validar en línea el PIN del tarjetahabiente.

Los emisores deben de realizar las validaciones pertinentes a los datos contenidos en el campo ARQC del Token B2, así como también el poder generar el Token de respuesta B5 debidamente llenado para todas las transacciones bajo el esquema EMV; y de la misma manera, debe validar en línea el PIN del tarjetahabiente.

Los emisores que reciban una solicitud de Autorización que incluya el ARQC del Token B2 y autoricen la Operación con Tarjeta sin validar dicho ARQC o no envíen en la respuesta de Autorización de Operación el ARPC del Token B5, asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Tarjetahabientes en el uso de dichas tarjetas. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Tarjetahabientes a más tardar cuarenta y ocho horas posteriores a la reclamación.

Los adquirentes que tramiten Solicitudes de Autorización de Operaciones con Tarjetas a nombre de sus Comercios afiliados cuyo Dispositivo para Operaciones con Tarjeta tenga la capacidad de lectura de CHIP EMV y no envíen el ARQC del Token B2 o no validen en la autorización de Operación el ARPC del Token B5, asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Tarjetahabientes en el uso de dichas tarjetas por lo que el emisor tendrá el derecho de contracargar la operación y el Adquirente no tendrá derecho de representarla. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Tarjetahabientes a más tardar cuarenta y ocho horas posteriores a la reclamación.

Validación del CVV2 o CVC2

Este Token contiene el resultado de la validación del CVV2 o CVC2 en transacciones Moto. (También aplica para transacciones manuales) El Emisor lo puede responder en mensajes 0210.

Consideraciones para transacciones de Cargos Periódicos

Una transacción MOTO debe llevar un valor 02 en token Q2. La fecha de vencimiento puede ser distinta a la fecha de vencimiento real de la tarjeta.

Para las transacciones de cargos periódicos, no tendrán el valor del CVV2/CVC2 en el Token C0.

El Token R4 se utiliza cuando se envía el número de contrato.

Campos involucrados en el mensaje ISO para Cargos periódicos. Adicionales al campo 63.

CAMPO	FORMATO	DESCRIPCIÓN	COMENTARIOS/POSIBLES VALORES	TIPO TRANSACCIÓN
18 Campo Merchant type		Determina el giro del comercio	Campo numérico de 4 posiciones, del giro real del comercio	Compras
Campo 22 Point of Service Entry Mode	N F 3	Determina la forma en la cual el número de tarjeta fue introducido y la capacidad de la terminal para aceptar/solicitar el NIP.	Posiciones: 1-2 → Forma de lectura del número de tarjeta: 01 = Manual 3 → Capacidad de aceptación del NIP: 00 = Desconocido.	Compras y reversos (time out)
Campo 35. Track 2 Data	ANS V 2:37	Contiene la información del track 2 almacenada en la banda magnética. (para cargos periódicos su estructura es armada)	No incluye los caracteres (sentinels) de inicio y fin del track2. Para el caso de tarjetas digitadas, el track2 se compone del número de cuenta y separador ("=") y la fecha de expiración en formato AAMM	Compras y reversos (time out)
63. POS Additional Data	ANS V 3:102	Información adicional	Ver especificación del Campo 63.en el numeral 2.9.28	Compras

Para considerar como válidos los Indicadores de Cargos Periódicos se debe validar el token C4 subcampo 4 valor 4 y subcampo 5 valor 1, token R4 subcampo 1 el cual no debe de viajar vacío, espacios ni ceros, solo se debe de validar que este poblado.

Comercio Interred

Una transacción de comercio Interred debe llevar el token Q2, valor 04, que identifica el medio de acceso para las transacciones de comercio interred.

Para considerar como válidos los Indicadores de Transacciones de comercio Interred deben estar calificados, en el token C4 en el subcampo 4 (valor 0), subcampo 5 (valor 0), subcampo 9 (valor 0,1 o 3), subcampo 11 (valor 2,3,4,5,6,7,8 o 9), subcampo 12 (valor 1,2 o 5)

Criterios para CAT - Transacciones Activadas por el Tarjetahabiente

Una transacción de CAT debe llevar el token Q2, valor 19, que identifica el medio de acceso para las transacciones de CAT.

Para considerar como válidos los Indicadores de Transacciones CAT deben estar calificados, en el token C4 en el subcampo 1 (valor 1), subcampo 4 (valor 0), subcampo 5 (valor 0), subcampo 10 (valor 1,2 o 3), subcampo 12 (valor 2 o 3)

Criterios para transacciones de Comercios Multicaja

Una transacción de Comercios Multicaja debe llevar el token Q2, valor 17 que identifica el medio de acceso para las transacciones de Comercios Multicaja.

Para considerar como válidos los Indicadores de Transacciones Comercios Multicaja deben estar calificados, en el token C4 en el subcampo 4 (valor 0), subcampo 5 (valor 0), subcampo 9 (valor 0,1 o 3), subcampo 11 (valor 2, 3, 4, 5, 6, 7, 8 o 9), subcampo 12 (valor 1,2 o 5).

Criterios para transacciones de Terminal Punto de Venta

Una transacción de Terminal Punto de Venta debe llevar el token Q2, valor 03, que identifica el medio de acceso para las transacciones de Terminal Punto de Venta.

Para el token C4 subcampo 4 debe indicar de acuerdo al modo de entrada; si es una transacción con PEM 90, 05 o 80 debe traer valor 0; si la transacción es con PEM 01 debe traer los valores (1 ,2,3,4 o 5)

Para considerar como válidos los Indicadores de Transacciones Terminal Punto de Venta deben estar calificados, en el token C4 en el subcampo 4 (valor 0), 5 (valor 0), 9 (valor 0,1 o 3), 11 (valor 2, 3,4,5,6,7,8 o 9), 12 (valor 1,2 o 5)

Criterios para transacciones TAG

Una transacción de TAG debe llevar el token Q2, valor 24, que identifica el medio de acceso para las transacciones de TAG.

Para considerar como válidos los Indicadores de TAG deben estar calificados, en el token C4 en el subcampo 5 (valor 1)

Tokens utilizados

TOKEN Q1: IDENTIFICADOR DEL MODO DE AUTORIZACIÓN

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador. “ “ = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. Q1 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. 00002 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo separador. “ “ = valor fijo (Espacio en blanco)
1	Identificador del modo de autorización	11	11	1	X(01)	0 = Respuesta por el Emisor en línea (autorizado o declinado) 1 = Respuesta por el Switch fuera de línea, stand in 2 = Capturado off line por el negocio o en el punto de Servicio, referido 4 = Autorizado Off line del negocio, archivo negativo 5 = Transacción forzada o de ajuste, 220 6 = Respuesta por Stand In con listas positivas (autorizado o declinado) 9 = Default
2	Identificador del modo de validación del criptograma Campo 100% informativo, el Adquirente no debe usarse para tomar alguna decisión on-line	12	12	1	X(01)	Emisor graba, Adquirente lee “ “, 0, 4 = Criptograma y Datos EMV NO validados. F = Error de Formato en Datos EMV. G = Criptograma NO es un ARQC. I = ARQC inválido T = Criptograma es válido, pero el TVR/CVR no es aceptable para el Emisor. U = Criptograma NO pudo ser validado por fallas en el sistema. 2 = Criptograma y Datos EMV aceptados.

TOKEN Q2: INDICADOR DEL MEDIO DE ACCESO

#	NOMBRE	INICIO	FIN	LONG	FORMA-TO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador. " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. Q2 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. 00002 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador. " " = valor fijo (Espacio en blanco)
1	Identificador del medio de acceso que realiza la solicitud de autorización	11	12	2	9(02)	Adquirente graba, Emisor lee 00 = Digitada manualmente presencia de tarjeta. (Fuentes Papel) 01 = Autorización Voz Normal (Manual) 02 = Sistema de Cargos Periódicos 03 = TPV (Terminal Punto de Venta) 04 = Comercio Interred 08 = Comercios MO/TO 09 = Internet (comercio electrónico) 10 = Intercambio Nacional 14 = Audiorespuesta IVR (derogado) 17 = Comercios Multicaja 18 = Autorizaciones Voz Referidas 19 = Cardholder Activated Terminals 20 = QPS (Valor Transitorio) 22 = Pago Móvil (derogado) 24 = TAG (Dispositivo de Comunicación) 26 = Contactless only

TOKEN Q6: INFORMACIÓN DE PAGOS DIFERIDOS.

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Separador 1. " " valor fijo
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del token que se está enviando. Q6 valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del token. 00006 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Separador 2. " " valor fijo
1	Diferimiento	11	12	2	9(02)	Numero de Meses en el que el pago no será exigible, justificado con ceros a la izquierda
2	Numero de pagos	13	14	2	9(02)	Número de meses en que se van a dividir los pagos, justificado con ceros a la izquierda.
3	Tipo de plan	15	16	2	9(02)	Tipo de plan a utilizarse: 00.- Sin promoción 03.- Sin intereses al tarjetahabiente 05.- Con Intereses para el tarjetahabiente 07.- Compre hoy y Pague después

TOKEN 04: RESULTADO DE LA VALIDACIÓN DEL TOKEN C0.

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. 04 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. 00020 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	Bandera de error en la Información adicional de la Solicitud de la Transacción	11	11	1	X(01)	Código utilizado para proporcionar información adicional de la transacción. Los valores permitidos son: Adquirente graba al solicitar la autorización. " " = valor fijo (Espacio en blanco) Adquirente lee Emisor graba A = Límite de Ajuste Excedido (Cierre de Preventa) de acuerdo al parámetro fijo configurado en el PTDF (Pos Terminal Definition File) para el comercio (Restaurante, Hotel, Agencia, etc.). C = Falla en la validación de los datos de la tarjeta al momento de leerla. E = Límite de Devolución Excedido de acuerdo al parámetro configurado en BDU (Base de Datos Única de Comercios). S = Error en la consistencia del Mensaje de solicitud. T = Error en la información del Token enviado en la solicitud K = Error de sincronización en el código de la Autenticación del Mensaje. I = Código del Mensaje de Autenticación Inválido (MAC). M = Falla en el Código del Mensaje de Autenticación (MAC).
2	Grupo de ruteo	12	22	11	X(11)	Adquirente lee Emisor lee
3	Bandera de Verificación de la Tarjeta	23	23	1	X(01)	Indica el resultado al verificar los valores de seguridad de la Tarjeta que realizó la solicitud de compra. Adquirente graba al solicitar la autorización. " " = valor fijo (Espacio en blanco) Al recibir respuesta Emisor graba/Adquirente lee 0 = La verificación de la tarjeta no se realizó porque la transacción fue denegada antes de que el proceso de verificación de la tarjeta comenzara. C = Se realizó la verificación de la tarjeta y el Código de validación fue inválido. D = Se realizó la verificación de la tarjeta y el Código de validación fue inválido. La transacción es denegada, cuando el campo de CV_BAD_DISP contiene el valor de "1, 2 o 3" en el CPF – Archivos de Prefijos de Tarjetas J = No se realizó la Verificación del código de validación porque la longitud del Track presentó un error. La transacción es denegada. K = No se realizó la verificación del código de validación porque la longitud del Track presentó un error. La transacción es referida. L = No se realizó la verificación del código de validación porque la longitud del Track presentó un error. La bandera del BAD TRACK ACTION que se encuentra en el "CPF indica que la transacción continúe procesándose. N ó " " = La entidad autorizadora no ha intentado realizar la verificación de la tarjeta ó no pudo verificar el Código de Validación debido a un error en el dispositivo de seguridad. O = No se realizó la verificación del código de validación porque no estaba en la tarjeta. P = No se realizó la verificación de la tarjeta, ya que el código de validación no estaba en la tarjeta. R = Se realizó la verificación de la tarjeta y el Código de validación fue incorrecto. La transacción es referida. Y = Se realizó la verificación de la tarjeta y el Código de validación fue correcto.
4	Extensión de Ciudad	24	28	5	X(05)	Cuando el nombre de la ciudad en la cual se localiza el comercio es mayor a 13 caracteres, este campo contiene los últimos cinco caracteres del nombre de la ciudad.
5	Datos completos del	29	29	1	X(01)	Es una bandera que indica cuando el Comercio o el

	Track 2					Adquirente de la transacción pueden capturar y transmitir completos los datos del Track 1 o Track 2. Adquirente graba al solicitar la autorización. " " = valor fijo (Espacio en blanco) Al recibir respuesta Emisor graba Adquirente lee Los valores permitidos son: Y ó " " = Si, el comercio o el Adquirente de la transacción captura y transmite los datos completos del Track. N = No, el comercio o el Adquirente de la transacción no captura y transmite los datos completos del Track.
6	Bandera de Archivo de acumulación de Usos	30	30	1	X(01)	Este campo solo se utiliza para Autorizaciones Negativas con el método de acumulación de usos de la tarjeta. Los valores permitidos son: " " = No existe registro en Archivo de acumulación de Usos 1 = Existen registros en Archivo de acumulación de Usos

TOKEN C0: CÓDIGO DE VALIDACIÓN

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. C0 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección datos de Token. 00026 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	CVV2/CVC2 (Código de validación)	11	14	4	X(04)	Código de validación de seguridad de la Tarjeta Adquirente graba Emisor lee "" = 4 Espacios en Blanco CVV2 = VISA (Card Verification Value) CVC2 = MasterCard (Card Validation Code) Nota: 3 Dígitos con espacio a la derecha
2	Código de Status de la retransmisión de la transacción	15	15	1	X(1)	Adquirente graba Emisor lee " " = Transacción normal(Espacio en blanco) A = Retransmisión aprobada D = Retransmisión declinada R = Retransmisión S = Retransmisión SAF (Store and Forward) Transacción de "Preventa"
3	Contador de retransmisiones de la transacción	16	18	3	X(03)	Número de veces que la transacción se retransmitió para ser procesada Adquirente graba Emisor lee 001 = valor fijo.
4	Código Postal del Comercio	19	28	10	X(10)	Código postal donde se encuentra el Comercio Adquirente graba Emisor lee " " = 10 Espacios en Blanco
5	Indicador de Comercio Electrónico	29	29	1	X(01)	Adquirente graba Emisor lee 0, " " = No es uma transacción de comercio electrónico 1 = Transacción MOTO 5 = Comercio seguro, titular autenticado (3D Secure) 6 = Comercio seguro, titular no autenticado (3D Secure) 7 = Autenticación 3D Secure no realizada
6	Tipo de tarjeta	30	30	1	X(01)	Adquirente graba Emisor lee B = Tarjeta "Business card" R = Tarjeta "Corporate card" S = Tarjeta "Purchasing card" " " = Desconocido (Espacio en blanco).
7	Transacción forzada o SAF (Preventa)	31	31	1	X(01)	Adquirente graba Emisor lee F = Transacción forzada S = Transaction Store-And-Forward (Preventa) " ", 0 = No es transacción forzada ni SAF (Preventa)
8	Indicador de CV2 (Código de validación) presente	32	32	1	X(01)	Adquirente graba Emisor lee 0 = El CV2 no fue incluido deliberadamente o no fue proporcionado por el negocio

	"CV2" corresponde al CVV2 en caso de Visa y CVC 2 en caso de MasterCard.					1 = El CV2 está presente 2 = El CV2 está impreso en la tarjeta pero es ilegible 9 = El CV2 no está impreso en la tarjeta " " = No hay información disponible
9	Indicador de información adicional	33	33	1	X(01)	Adquirente graba Emisor lee 0 = No fue capturada información adicional con la transacción original 1 = Fue capturada información adicional con la transacción original " " = Este campo no es utilizado
10	Authentication collector indicator	34	34	1	X(01)	Adquirente graba Emisor lee 0 = UCAF no soportado 1 = UCAF es soportado por comercio pero los datos no fueron capturados. 2 = UCAF es soportado por el comercio y si contiene datos Este campo solo aplica para Tx MasterCard en caso de ser una Tx VISA tendrá el valor 0 " " = Este campo no es utilizado
11	Bandera de propensión de fraude del comercio	35	35	1	X(01)	Adquirente graba Emisor lee Indicador de propensión al fraude para ese comercio. 1 = no propenso al fraude 2 = propenso al fraude 3 = altamente propenso al fraude " " = (Espacio en blanco) No Soportado por el momento.
12	Resultado de la validación CAVV/AAV	36	36	1	X(01)	Resultado de la validación CAVV (VISA) / AVV (MasterCard) 0 = No se realizó la validación por error en la recepción de datos 1 = Validación fallida 2 = Validación aprobada 3 = No se realizó la validación pues no existe información en el EAF 4 = La validación no se realizó por error del sistema (EAF corrupto) 5 = El Adquirente participa en los métodos de autenticación pero el Emisor no participa 6 = El Bin participa y no se realizó la validación 7 = CAVV/AAV duplicado " " = No hay información disponible

TOKEN C4: DATOS DE LA TERMINAL

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Separador 1. " " valor fijo
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del token que se está enviando. C4 valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del token. 00012 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Separador 2. " " valor fijo
1	Indicador si la terminal es atendida por el adquiriente	11	11	1	9(01)	Código indicando cuando la terminal es atendida por el ratailer, valores validos son: 0 = La terminal es atendida. 1 = La terminal no es atendida, por ejemplo una terminal activada por el tarjeta habiente o una PC 2 = No se usó terminal, por ejemplo autorizaciones por voz.
2	TERM-OPER-IND	12	12	1	9(01)	Reservado para uso futuro, se envía en cero.
3	Localización de la terminal	13	13	1	9(01)	Indicador de la localización de la terminal: 0 = La terminal está en el local 1 = La terminal es remota 2 = La terminal está en la ubicación del tarjetahabiente (Ej. Ecommerce) 3 = No se usó terminal (por voz, por ejemplo)
4	Indicador de presencia del tarjetahabiente	14	14	1	9(01)	Indicador de la presencia del tarjeta habiente en la TPV: 0 = El tarjetahabiente está presente 1 = El tarjetahabiente no está presente (no se especifica

						razón) 2 = El tarjetahabiente no está presente (transacción iniciada por correo o fax) 3 = El tarjetahabiente no está presente (autorización por voz) 4 = El tarjetahabiente no está presente (transacción recurrente) 5 = El tarjetahabiente no está presente (orden electrónica desde una PC o internet)
5	Indicador de presencia de tarjeta	15	15	1	9(01)	Indicador de presencia de la tarjeta en la TPV: 0 = La tarjeta está presente 1 = La tarjeta no está presente.
6	Indicador de capacidad de captura de tarjetas	16	16	1	9(01)	0 = La terminal no tiene capacidad de captura de tarjetas 1 = La terminal tiene capacidad de captura de tarjetas
7	Indicador de status	17	17	1	9(01)	Código indicando el status del requerimiento: 0 = Requerimiento normal 4 = Requerimiento preautorizado.
8	Nivel de seguridad del adquiriente	18	18	1	9(01)	Código indicando el novel de seguridad del adquiriente: 0 = Sin seguridad 1 = Sospechoso de fraude 2 = Identificación verificada
9	Routing indicator	19	19	1	9(01)	0 = EMV Early 1 = EMV FULL 3 = NO EMV
10	Activación de la terminal por el tarjetahabiente	20	20	1	9(01)	Código indicando cuando la terminal fue activada por el tarjetahabiente con una tarjeta y si así fue, el nivel de seguridad: 0 = La terminal no puede ser activada por tarjeta 1 = Terminal automática con PIN, nivel 1 2 = Terminal de autoservicio nivel 2 (montos mayores a $250) 3 = Terminal de monto limitado, nivel 3 (montos hasta $250) 4 = Comercio In-flight, nivel 4 6 = Comercio Electrónico 7 = Radio Frecuencia (Contact Less) 8 = Uso futuro 9 = mPOS
11	Indicador de capacidad para transferir datos de la tarjeta a la terminal *Este campo debe viajar en línea y no debe validarse en línea.*	21	21	1	9(01)	Código indicando las capacidades que tiene la terminal para transferir datos de la tarjeta a la terminal: 0 = Desconocida 1 = No hay terminal (autorizaciones voz) 2 = Lector de banda magnética 3 = Contactless Chip, Chip contacto y banda magnética. 4 = Contactless Magstripe, Chip contacto y banda magnética 5 = Lector de banda y lector de chip EMV-compatible 6 = Entrada manual 7 = Lector de banda y entrada manual 8 = Lector de banda, entrada manual y lector de chip EMV-Compatible 9 = Lector exclusivamente de Chip EMV – compatible
12	Método de Identificación del Tarjetahabiente	22	22	1	X(01)	Un código que indica cómo fue identificado el Tarjetahabiente en el punto de servicio: 0, “ ” = Desconocido (default) 1 = Firma 2 = PIN 3 = Terminal no atendida 4 = Orden correo teléfono 5 = Transacción QPS (Quick Payment Service), pagaré sin firma. 6 = Analisis de firma electrónica. 7 = Biometricos 8 = Biograficos 9 = Contactless sin autenticación del tarjetahabiente

TOKEN C6: CÓDIGOS PARA 3D SECURE (VISA)

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. **! = valor fijo (Admiración Cerrada)**
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador. **" " = valor fijo (Espacio en blanco)**
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. **C6 =** valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. **00080 =** valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador. **" " = valor fijo (Espacio en blanco)**
1	XID	11	50	40	X(40)	**Adquirente graba** **Emisor lee** Reservado para implementación futura de VISA La información deberá estar en claro.
2	CAVV–Cardholder Authentication Verification Value	51	90	40	X(40)	**Adquirente graba** **Emisor lee** CAVV – Valor Calculado por VISA como Autentificador del Tarjetahabiente. La información deberá estar en claro.

TOKEN CE: AUTENTICACIÓN DE DATOS DEL TARJETAHABIENTE PARA TRANSACCIONES 3D SECURE (MASTER CARD)

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador. " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. CE = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. 00202 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador. " " = valor fijo (Espacio en blanco)
1	Indicador	11	12	2	X(02)	Adquirente graba Emisor lee 00 = No lo maneja 01 = UCAF 02 = Chip Authentication Program (CAP) token
2	Datos de autenticación del tarjeta habiente	13	212	200	X(200)	Formato Ans-28. Los datos de autenticación del token CE deben estar justificados a la izquierda. El token no debe contener espacios en blanco antes de los datos de autenticación. En la posición 1 deberá tener el siguientes valor: j – La primera y siguientes transacciones autenticadas. h – Cuando la transacción es un attemp.

TOKEN R4: NÚMERO DE CONTRATO EN TRANSACCIONES DE CARGOS PERIÓDICOS.

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador. “ “ = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. R4 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token. 00020 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador. “ “ = valor fijo (Espacio en blanco)
1	Número de contrato	11	30	20	X(20)	Número de contrato sobre el que se realiza el cargo recurrente. El campo debe estar justificado a la izquierda, rellenando con espacios las posiciones que no sean ocupadas. De estar presente el token, no pueden contener sólo espacios.

TOKEN CZ: INDICADOR DE TIPO DE DISPOSITIVO CONTACTLESS

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Separador 1. “ “ valor fijo
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del token que se está enviando. CZ valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del token. 00040 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Separador 2. “ “ valor fijo
1	ATC	11	14	4	X(04)	The Application Transaction Counter (ATC) value from the base segment of the Cardholder Authorization File (CAF). The value in the token is the current value after ATC verification and Dynamic Card Verification have been performed. The largest ATC value is 65,535. The field is defined as non-integer, but will contain binary data. It should be initialized with binary zeroes.
2	FORM-FACTR-IND	15	22	8	X(08)	This field contains Visa-defined data to be used for the identification of the cardholder device, its security features, and the communication technology used to acquire a contactless transaction. The field is defined as non-integer, but will contain binary data. It should be initialized with binary zeroes. Valid values are as follows: Byte 1 = Cardholder device type Values: 00 = Card (default) 01 = Mobile Phone or Smartphone 02 = Key Fob (Llavero) 03 = Watch (Reloj) 04 = Mobile Tag (Calcomanias) 05 = Wristband (Brazalete) 06 = Mobile Phone Case or Sleeve 07–99 = Reserved for future use Byte 2 = Cardholder device security features Byte 3 = Reserved Byte 4 = Communication technology
3	USER-FLD-ACI	23	50	28	X(28)	This field is reserved for future use

TOKEN B2: DATOS DE SOLICITUD

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token.
						! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador.
						" " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando.
						B2 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token.
						00158 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo separador.
						" " = valor fijo (Espacio en blanco)
1	BIT-MAP	11	14	4	X(4)	Indica si los datos en cada uno de los campos restantes en el token están presentes o ausentes. El token en sí mismo es una estructura de formato fijo, por lo que la ausencia de un elemento de datos significa que el campo correspondiente está presente, pero que su contenido no debe ser considerado.
					LVL 2	Tenga en cuenta que las posiciones de los bits dentro del bitmap siguen la convención de la norma ISO 8583 (es decir, el bit de orden más alto representa el primer campo en el token).
						Bit Map Posición
						Campo Nombre EMV Token
						1 USER-FLD1 n/a
						2 CRYPTO-INFO-DATA B2 - 3 (9F27)
						3 TVR B2 – 4 (95)
						4 ARQC B2 – 5 (9F26)
						5 AMT-AUTH B2 – 6 (9F02)
						6 AMT-OTHER B2 – 7 (9F03)
						7 AIP B2- 8 (82)
						8 ATC B2 – 9 (9F36)
						9 TERM-CNTRY-CDE B2 – 10 (9F1A)
						10 TRAN-CRNCY-CDE B2 - 11 (5F2A)
						11 TRAN-DAT B2 – 12 (9A)
						12 TRAN-TYPE B2 – 13 (9C)
						13 UNPREDICT-NUM B2 – 14 (9F37)
						16 ISS-APPL-DATA B2 – 16 (9F10)
2	USER-FLD1	15	18	4	X(4)	Debe contener ceros binarios.
					LVL 2	
3	CRIPTO-INFO-DATA	19	20	2	X(2)	Tipo de criptograma y las acciones a llevar a cabo por la terminal. Los valores válidos se muestran en la tabla a continuación.
					LVL 2	En las especificaciones EMV, las definiciones que incluyen posiciones de bit indican que los bits están ordenados de forma descendente, del 8 a la izquierda, hasta el 1 a la derecha.
						Posición descripción
						8–7 Tipo de criptograma.
						Los valores válidos son los siguientes:
						00 =AAC
						01 =TC
						10 = ARQC
						11 = AAR
						6 Reservado para uso futuro
						5 Reservado para uso futuro
						4 Aviso de la bandera requerida.
						Los valores válidos son los siguientes:
						0 = Aviso no requerido.
						1 = Aviso requerido.
						3–1 La razón, el aviso, del código de referencia.
						Los valores válidos son los siguientes:
						01000 = Ninguna Información
						001 = Servicio no permitido
						010 = Intentos de PIN excedido
						011 = Falla de autenticación del Emisor
4	TVR	21	30	10	X(10)	Los resultados de la verificación de la terminal. Este campo indica el estado de las diferentes funciones como se ve desde la terminal. Los valores válidos se muestran en las tablas siguientes. El valor por defecto para todos los ajustes de bits es un valor de 0.
					LVL 2	En las especificaciones EMV, las definiciones que incluyen posiciones de bit indican que los bits están ordenados de forma descendente, del 8 a la izquierda, hasta el 1 a la derecha.
						Las posiciones de bit que NO se señalan están reservadas para uso futuro.
						Byte 1
						Posición Descripción

						8 Bandera de autenticación de datos fuera de línea.
						Los valores válidos son los siguientes:
						0 = Se realizó la autenticación de datos fuera de línea.
						1 = No se realizó la autenticación de datos fuera de línea.
						7 Bandera de autenticación de datos estáticos fuera de línea. Los valores válidos son los siguientes:
						0 = Autenticación de datos estáticos fuera de línea lograda.
						1 = Autenticación de datos estáticos fuera de línea fallida
						6 Bandera de datos de tarjeta de circuito integrado (ICC). Los valores válidos son los siguientes:
						0 =Datos de tarjeta de circuito integrado (ICC) presentes.
						1 = Datos de tarjeta de circuito integrado (ICC) ausentes.
						5 Bandera de tarjeta en archivo de excepciones. Los valores válidos son los siguientes:
						0 = La tarjeta no aparece en el archivo de excepción de la terminal.
						1 = La tarjeta aparece en el archivo excepción de la terminal.
						4 Bandera de autenticación de datos dinámicos fuera de línea. Los valores válidos son los siguientes:
						0 = Autenticación de datos dinámicos fuera de línea lograda.
						1 = Autenticación de datos dinámicos fuera de línea fallida
						Byte 2
						Posición Descripción
						8 Bandera de versión del ICC y la terminal. Los valores válidos son los siguientes:
						0 = El ICC y la terminal tienen la misma versión de aplicación.
						1 = El ICC y la terminal tienen diferente versión de aplicación.
						7 Bandera de aplicación expirada. Los valores válidos son los siguientes:
						0 = La aplicación no ha expirado.
						1 = La aplicación ha expirado.
						6 Bandera de aplicación efectiva. Los valores válidos son los siguientes:
						0 = La aplicación es efectiva.
						1 = La aplicación no es efectiva.
						5 Bandera de servicio solicitado. Los valores válidos son los siguientes:
						0 = El servicio solicitado está permitido para el producto de la tarjeta.
						1 = El servicio solicitado no está permitido para el producto de la tarjeta.
						4 Bandera de nueva tarjeta. Los valores válidos son los siguientes:
						0 = La transacción no se inició con una nueva tarjeta.
						1= La transacción se inició con una nueva tarjeta.
						Byte 3
						Posición Descripción
						8 Bandera de verificación del tarjetahabiente. Los valores válidos son los siguientes:
						0 = verificación satisfactoria del tarjetahabiente.
						1 = verificación no satisfactoria del tarjetahabiente.
						7 Bandera de método de verificación del tarjetahabiente, no reconocido (CVM). Los valores válidos son los siguientes:
						0 = El CVM fue reconocido.
						1 = El CVM no fue reconocido.
						6 Bandera de intentos de ingreso de PIN. Los valores válidos son los siguientes:
						0 = El límite de intentos de ingreso de PIN no fue excedido.
						1= El límite de intentos de ingreso de PIN fue excedido.
						5 Condición de: PIN requerido/PIN PAD no disponible. Los valores validos son los siguientes:
						0 = El ingreso del PIN no es requerido o el PIN PAD está presente y operando.
						1 = El ingreso del PIN es requerido y el PIN PAD no está presente o es inoperable.
						4 Condición de: PIN requerido/PIN no ingresado. Los valores válidos son los siguientes:
						0 = El ingreso del PIN no es requerido o el PIN PAD no está presente o el PIN fue capturado.
						1 = El ingreso del PIN es requerido, el PIN PAD está presente y el PIN no fue capturado.
						3 Bandera de PIN en línea. Los valores válidos son los siguientes:
						0 = PIN en línea no capturado.
						1 = PIN en línea capturado.
						Byte 4
						Posición Descripción

						8 Bandera de límite de piso. Los valores válidos son los siguientes:
						0= El monto de la transacción no excede el límite de piso.
						1 = El monto de la transacción excede el límite de piso.
						7 Bandera de límite inferior fuera de línea consecutivo. Los valores válidos son los siguientes:
						0 = No se ha superado el límite inferior fuera de línea consecutivo.
						1 = Se ha superado el límite inferior fuera de línea consecutivo.
						6 Bandera de límite superior fuera de línea consecutivo. Los valores válidos son los siguientes:
						0 = No se ha superado el límite superior de fuera de línea consecutivo.
						1 = Se ha superado el límite superior de fuera de línea consecutivo.
						5 Bandera de selección aleatoria. Los valores válidos son los siguientes:
						0 = La transacción no fue seleccionado aleatoriamente para procesamiento en línea.
						1 = La transacción fue seleccionado aleatoriamente para procesamiento en línea.
						4 Bandera de procesamiento en línea forzado por el comercio. Los valores válidos son los siguientes:
						0 = El comercio no forzó la transacción en línea.
						1 = El comercio forzó la transacción en línea.
						Byte 5
						Posición Descripción
						8 Estado del certificado transacción de la lista de objetos de datos (TDOL). Los valores válidos son los siguientes:
						0 = No se utilizó el TDOL por defecto.
						1 = Se utilizó el TDOL por defecto.
						7 Bandera de autenticación del emisor. Los valores válidos son los siguientes:
						0 = La Autenticación del emisor fue exitosa.
						1 = La Autenticación del emisor no fue exitosa.
						6 Bandera de procesamiento de script antes del comando GENERATE AC final. Los valores válidos son los siguientes:
						0 =Procesamiento de script no falló antes del comando GENERATE AC final.
						1 = Procesamiento de script falló antes del comando GENERATE AC final.
						5 Bandera de procesamiento de script después del comando GENERATE AC final. Los valores válidos son los siguientes:
						0 = Procesamiento de script no falló después del comando GENERATE AC final.
						1 = Procesamiento de script falló después del comando GENERATE AC final.
5	ARQC	31	46	16	X(16)	El criptograma de solicitud de autorización. El criptograma devuelto por el ICC en respuesta al comando GENERATE AC.
					LVL 2	
6	AMT-AUTH	47	58	12	X(12)	El importe autorizado de la transacción (excluyendo ajustes). Los datos en este campo son justificados a la derecha (es decir, decimal codificado en binario).
					LVL 2	
7	ATM-OTHER	59	70	12	X(12)	El importe secundario asociado con la transacción, representa el importe de cash-back. Los datos en este campo son justificados a la derecha (es decir, decimal codificado en binario).
					LVL 2	
8	AIP	71	74	4	X(4)	El perfil de intercambio de aplicación. Este campo indica las capacidades de la tarjeta para soportar funciones específicas en la aplicación. Los valores válidos se muestran en las tablas siguientes.
					LVL 2	En las especificaciones EMV, las definiciones que incluyen posiciones de bit indican que los bits están ordenados de forma descendente, del 8 a la izquierda, hasta el 1 a la derecha.
						Las posiciones de bit que NO se señalan están reservadas para uso futuro.
						Byte 1
						Posición Descripción
						8 Bandera de inicialización. Los valores válidos son los siguientes:
						0 = No inicializar.
						1 = inicializado.
						7 Bandera de autenticación de datos estáticos fuera de línea soportada. Los valores válidos son los siguientes:
						0 = Autenticación de datos estáticos fuera de línea no soportada.
						1 = Autenticación de datos estáticos fuera de línea soportada.

						6 Bandera de autenticación de datos dinámicos fuera de línea soportada. Los valores válidos son los siguientes:
						0 = Autenticación de datos dinámicos fuera de línea no soportada.
						1 = Autenticación de datos dinámicos fuera de línea soportada.
						5 Bandera verificación del tarjetahabiente soportada. Los valores válidos son los siguientes:
						0 = Verificación del tarjetahabiente no soportada.
						1 = Verificación del tarjetahabiente soportada.
						4 Bandera de administración de riesgos de la terminal soportada. Los valores válidos son los siguientes:
						0 = La administración del riesgo de la terminal no será realizada.
						1 = La administración del riesgo de la terminal será realizada.
						3. Bandera de autenticación del emisor soportada. Los valores válidos son los siguientes:
						0 = La autenticación del emisor no está soportado
						1 = La autenticación del emisor está soportado.
9	ATC	75	78	4	X(4)	El contador de transacción de la aplicación. La aplicación del chip mantiene e incrementa este contador.
					LVL 2	
10	TERM-CNTR-CDE	79	81	3	X(3)	Código que indica el país de la terminal, de acuerdo con la norma ISO 3166, *Códigos para la representación de nombres de países*. Los datos en este campo son justificados a la derecha (es decir, decimal codificado en binario).
					LVL 2	
11	TRAN-CRNCY-CDE	82	84	3	X(3)	Código que indica el código de moneda de la transacción, como se recibió desde el dispositivo o intercambio, de acuerdo con la norma ISO 4217, *Códigos para la representación de Monedas y Fondos*. Los datos en este campo son justificados a la derecha (es decir, decimal codificado en binario).
					LVL 2	
12	TRAN-DAT	85	90	6	X(6)	La fecha local (en formato AAMMDD) en la que la operación fue autorizada. Los datos de este campo se almacena como datos empaquetados (es decir, decimal codificado en binario).
					LVL 2	
13	TRAN-TYPE	91	92	2	X(2)	Código que indica el tipo de transacción financiera, representado por los dos primeros dígitos del código de procesamiento de la norma 1987 ISO 8583, *Mensajes originados por tarjetas bancarias – Especificación de mensajes de intercambio - Contenido para transacciones financieras*. Los datos de este campo se almacena como datos empaquetados (es decir, decimal codificado en binario).
					LVL 2	
14	UNPREDICT-NUM	93	100	8	X(8)	Número impredecible utilizado para proporcionar la variabilidad y unicidad a la generación del criptograma.
					LVL 2	
15	ISS-APPL-DATA-LGTH	101	104	4	X(4)	Indica la longitud de los datos de aplicación emisor en el campo siguiente. Las versiones ASCII binario del token deben contener el mismo valor en este campo. La versión ASCII del token debe contener el la representación decimal (no hexadecimal) del valor de longitud.
					LVL 2	
16	ISS-APPL-DATA	105	168	64	X(64)	Datos de la aplicación propietaria del emisor para la transmisión al emisor en una transacción en línea. Los datos en este campo son justificados a la izquierda y rellenado con ceros binarios a la derecha.
					LVL 2	Redefiniciones
16a	VISA-APPL-DATA				LVL 2	REDEFINES ISS-APPL-DATA
						La definición Visa / UKIS de los datos de aplicación Emisor
16a	LGTH	105	106	2	X(2)	
					LVL 4	
16a	DERIV-KEY-INDEX	107	108	2	X(2)	
					LVL 4	
16a	CRYPTO-VER-NUM	109	110	2	X(2)	
					LVL4	
16a	CRYPTO-VRF-RSLTS	111	118	8	X(8)	
					LVL4	
16a	INFO	119	168	50	X(50)	
					LVL4	
16b	MCPA-APPL-DATA				LVL 2	REDEFINES ISS-APPL-DATA
						La definición 2.1 MasterCard / Europay (MCPA) MChip de los datos de aplicación Emisor.
16b	DERIV-KEY-INDEX	105	106	2	X(2)	
					LVL 4	
16b	CRYPTO-VER-NUM	107	108	2	X(2)	
					LVL 4	
16b	CRD-VRFY-RSLTS	109	116	8	X(8)	
					LVL 4	
16b	DAC	117	120	4	X(4)	
					LVL 4	
16b	INFO	121	168	48	X(48)	

					LVL 4	
16c	MCHIP4-APPL-DATA					REDEFINES ISS-APPL-DATA
					LVL2	La definición 4 MasterCard / Europay MChip de los datos de aplicación Emisor.
16c	DERIV-KEY-INDEX	105	106	2	X(2)	
					LVL 4	
16c	CRYPTO-VER-NUM	107	108	2	X(2)	
					LVL 4	
16c	CRD-VRFY-RSLTS	109	120	12	X(12)	
					LVL 4	
16c	DAC	121	124	4	X(4)	
					LVL 4	
16c	CNTR	125	140	16	X(16)	
					LVL 4	
16c	INFO	141	168	28	X(28)	
					LVL 4	
16d	CCD-A-APPL-DATA				LVL 2	REDEFINES ISS-APPL-DATA
16d	LGTH	105	106	2	X(2)	
					LVL 4	
16d	COMMON-CORE-ID	107	108	2	X(2)	
					LVL 4	
16d	DERIV-KEY-INDEX	109	110	2	X(2)	
					LVL 4	
16d	CRD-VRFY-RSLTS	111	120	10	X(10)	
					LVL 4	
16d	COUNTERS	121	136	16	X(16)	
					LVL 4	
16d	ISS-DISCR-DATA-LGTH	137	138	2	X(2)	
					LVL 4	
16d	ISS-DISCR-DATA	139	168	30	X(30)	
					LVL 4	

Token B2 subcampo 16 se deriva en las siguientes posibilidades

#	LONGITUD	INICIO	FIN	NOMBRE
16a				VISA-APPL-DATA
16a	2	95	96	LGTH
16a	2	97	98	DERIV-KEY-INDEX
16a	2	99	100	CRYPTO-VER-NUM
16a	8	101	108	CRYPTO-VRF-RSLTS
16a	50	109	158	INFO
16b				MCPA-APPL-DATA
16b	2	95	96	DERIV-KEY-INDEX
16b	2	97	98	CRYPTO-VER-NUM
16b	8	99	106	CRD-VRFY-RSLTS
16b	4	107	110	DAC / ICC DN
16b	48	111	158	INFO
16c				MCHIP4-APPL-DATA
16c	2	95	96	DERIV-KEY-INDEX
16c	2	97	98	CRYPTO-VER-NUM
16c	12	99	110	CRD-VRFY-RSLTS
16c	4	111	114	DAC / ICC DN
16c	16	115	130	CNTR
16c	28	131	158	INFO
16d				CCD-A-APPL-DATA
16d	2	95	96	LGTH
16d	2	97	98	COMMON-CORE-ID
16d	2	99	100	DERIV-KEY-INDEX
16d	10	101	110	CRD-VRFY-RSLTS
16d	16	111	126	COUNTERS
16d	2	127	128	ISS-DISCR-DATA-LGTH
16d	10	129	158	ISS-DISCR-DATA

TOKEN B3: DATOS DISCRESIONALES EMV

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token.
						! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador.
						" " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando.
						B3 = valor fijo

H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token.
						00080 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador.
						" " = valor fijo (Espacio en blanco)
1	BIT-MAP	11	14	4	X(4)	Indica si los datos en cada uno de los campos restantes en el token están presentes o ausentes. El token en sí mismo es una estructura de formato fijo, por lo que la ausencia de un elemento de datos significa que el campo correspondiente está presente, pero que su contenido no debe ser considerado.
					LVL 2	Tenga en cuenta que las posiciones de los bits dentro del bitmap siguen la convención de la norma ISO 8583 (es decir, el bit de orden más alto representa el primer campo en el token).
						Bit Map
						Position FieldName EMV Token Tag
						1 TERM-SER-NUM B3 - 2 (9F1E)
						2 EMV-TERM-CAP B3 - 3 (9F33)
						3 USER-FLD1 n/a
						4 USER-FLD2 n/a
						5 EMV-TERM-TYPE B3 - 6 (9F35)
						6 APPL-VER-NUM B3 - 7 (9F09)
						7 CVM-RSLTS B3 - 8 (9F34)
						8 Este campo contendrá uno de los siguientes elementos de datos:
						DF-NAME B3 - 10.1 (84)
						o APPLICATION ID 4F
2	TERM-SERL-NUM	15	22	8	X(8)	Número del dispositivo de interface (IFD), número de serie único y permanente asignado a la terminal por el fabricante.
3	EMV-TERM-CAP	23	30	8	X(8)	Dato proporcionado de la tarjeta: método de verificación del tarjetahabiente; y capacidades de seguridad de la terminal. Los valores válidos se muestran en las tablas siguientes. El valor por defecto para todos los bits es 0.
					LVL 2	Byte 1 (Capacidad de entrada de datos de la tarjeta)
						Posición Descripción
						8 Capacidad de ingreso por tecleado manual. Los valores válidos son los siguientes:
						0 = La terminal no soporta la entrada manual para ingresar los datos de la tarjeta.
						1 = La terminal soporta la entrada manual para ingresar los datos de la tarjeta.
						7 Capacidad de banda magnética. Los valores válidos son los siguientes:
						0 = La terminal no soporta el ingreso de datos por medio de la banda magnética de la tarjeta.
						1 = La terminal soporta el ingreso de datos por medio de la banda magnética de la tarjeta.
						6 Terminal con capacidad de chip de contacto. Los valores válidos son los siguientes:
						0 = La terminal no soporta el ingreso de datos desde el chip de la tarjeta.
						1 = La terminal soporta el ingreso de datos desde el chip de la tarjeta.
						Byte 2 (Capacidades CVM)
						Posición Descripción
						8 Capacidad de verificación de PIN en texto plano para el chip de la tarjeta. Los valores válidos son los siguientes:
						0 = La terminal no utiliza el CVM verificación del PIN en texto plano.
						1 = La terminal utiliza el CVM verificación del PIN en texto plano.
						7 Capacidad de verificación de PIN cifrado en línea. Los valores válidos son los siguientes:
						0 = La terminal no utiliza el CVM PIN cifrado en línea.
						1 = La terminal utiliza el CVM PIN cifrado en línea.
						6 Capacidad de firma (en papel). Los valores válidos son los siguientes:
						0 = La terminal no utiliza el CVM firma (en papel).
						1 = La terminal utiliza el CVM firma (en papel).
						5 Capacidad de verificación de PIN cifrado fuera de línea. Los valores válidos son los siguientes:
						0 = PIN cifrado fuera de línea no fue utilizado como CVM por la terminal.
						1 = PIN cifrado fuera de línea fue utilizado como CVM por la terminal.
						Byte 3 (Capacidades de Seguridad)
						Posición Descripción
						8 Capacidad de autenticación de datos estáticos. Los valores válidos son los siguientes:

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>0 = La autenticación de datos estáticos no se utiliza en esta terminal.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1 = La autenticación de datos estáticos se utiliza en esta terminal.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>7 Capacidad de autenticación de datos dinámicos. Los valores válidos son los siguientes:</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>0 = La autenticación de datos dinámicos no se utiliza en esta terminal.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1 = La autenticación de datos dinámicos se utiliza en esta terminal.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>6 Capacidad de captura de tarjeta. Los valores válidos son los siguientes:</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>0 = La terminal no tiene capacidad de capturar la tarjeta.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1 = La terminal tiene capacidad de capturar la tarjeta.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Byte 4 USER-FLD1-EMV-TERM-CAP
Este campo se utiliza para asegurar la alineación de texto.</td></tr>
<tr><td>4</td><td>USER-FLD1</td><td>31</td><td>34</td><td>4</td><td>X(4)
LVL 2</td><td>Debe contener ceros binarios</td></tr>
<tr><td>5</td><td>USER-FLD2</td><td>35</td><td>42</td><td>8</td><td>X(8)
LVL 2</td><td>Debe contener ceros binarios.</td></tr>
<tr><td>6</td><td>EMV-TERM-TYPE</td><td>43</td><td>44</td><td>2</td><td>X(2)</td><td>Tipo de terminal EMV, indica el entorno de la terminal, su capacidad de comunicaciones, y su control operativo, como se muestra en la tabla a continuación.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>LVL 2</td><td>
<table>
<tr><td></td><td colspan="3">Control Operativo</td></tr>
<tr><td>Entorno</td><td>Institución financiera</td><td>Comercio</td><td>Tarjetahabiente</td></tr>
<tr><td colspan="4">Terminal Atendida</td></tr>
<tr><td>Sólo online</td><td>11</td><td>21</td><td>N/A</td></tr>
<tr><td>Offline con capacidad online</td><td>12</td><td>22</td><td>N/A</td></tr>
<tr><td>Sólo offline</td><td>13</td><td>23</td><td>N/A</td></tr>
<tr><td colspan="4">Terminal no Atendida</td></tr>
<tr><td>Sólo online</td><td>14</td><td>24</td><td>34</td></tr>
<tr><td>Offline con capacidad online</td><td>15</td><td>25</td><td>35</td></tr>
<tr><td>Sólo offline</td><td>16</td><td>26</td><td>36</td></tr>
</table>
</td></tr>
<tr><td>7</td><td>APPL-VER-NUM</td><td>45</td><td>48</td><td>4</td><td>X(4)
LVL 2</td><td>El número de versión asignado por el sistema de pago para la aplicación de la terminal.</td></tr>
<tr><td>8</td><td>CVM-RSLTS</td><td>49</td><td>54</td><td>6</td><td>X(6)</td><td>Resultados del último método de verificación del tarjetahabiente (CVM) ejecutado. Los valores válidos se muestran en las tablas siguientes. El valor por defecto para todos los ajustes de bits es un valor de 0.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>LVL 2</td><td>En las especificaciones EMV, las definiciones que incluyen posiciones de bit indican que los bits están ordenados de forma descendente, del 8 a la izquierda, hasta el 1 a la derecha.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Byte 1 CVM ejecutado</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Posición Descripción</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>7 0 = Falla la verificación del tarjetahabiente si este CVM no es exitoso</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1 = Aplicar la siguiente regla de verificación de la tarjeta (CVR) si este CVM no es exitoso</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>6–1 000000= Procesamiento de CVM fallido</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>000001 = Verificación de PIN en texto plano realizada por el chip de la tarjeta</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>000010 = PIN cifrado verificado en línea</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>000011 = Verificación de PIN en texto plano realizada por el chip de la tarjeta y firma (papel)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>000100 = Verificación de PIN cifrado realizada por el chip de la tarjeta</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>000101 = Verificación de PIN cifrado realizada por el chip de la tarjeta y firma (papel)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>0xxxxx = Los valores en el rango 000110 - 011101 están reservados para uso futuro por la especificación EMV</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>011110 = Firma (papel)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>011111 = No se requiere CVM</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>10xxxx = Los valores en el rango 100000 – 101111 están reservados para uso futuro por los sistemas de pago</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>11xxxx = Los valores en el rango 110000 – 111110 están reservados para uso futuro por el Emisor</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>111111 = No disponible para su uso</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Byte 2 Condición de CVM</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Valor Descripción</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>00 Siempre</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>01 Efectivo o cashback</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>02 No es efectivo o cashback</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>03 Terminal es compatible con la CVM</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>04 Reservado para uso futuro</td></tr>
</table>

						05 Reservado para uso futuro
						06 La transacción es en la moneda de la aplicación y se encuentra bajo 'x' valor
						07 La transacción es en la moneda de la aplicación y se encuentra arriba de 'x' valor
						08 La transacción es en la moneda de la aplicación y se encuentra bajo 'y' valor
						09 La transacción es en la moneda de la aplicación y se encuentra arriba de 'y' valor
						0A–7F Reservado para uso futuro
						80–FF Reservado para uso futuro en los sistemas de pago
						Byte 3 Resultado de CVM
						Valor Descripción
						0 Desconocido (por ejemplo firma)
						1 Fallido (por ejemplo PIN offline)
						2 Exitoso (por ejemplo PIN offline)
9	DF-NAME-LGTH	55	58	4	X(4) LVL 2	Longitud del nombre de archivo dedicado o identificador de la aplicación en el campo siguiente. Las versiones ASCII y binarias del token deben contener el mismo valor en este campo. La versión ASCII del token debe contener la representación del valor de longitud en decimal (no hexadecimal)
10	DF-NAME	59	90	32	X(32) LVL 2	Nombre del archivo dedicado (como se describe en la norma ISO / IEC 7816-4) o identificador de aplicación (como se describe en la norma ISO / IEC 7816-5). Los datos se justifican a la izquierda y se rellenan a la derecha con ceros binarios

TOKEN B4: ESTATUS EMV

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de token.
						! valor fijo
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Separador 1.
						" " valor fijo
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del token que se está enviando.
						B4 valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del token.
						00020 valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Separador 2.
						" " valor fijo
1	PT-SRV-ENTRY-MDE	11	13	3	X(3) LVL 2	El modo de entrada del punto de servicio. Este campo indica la forma en que se ingresaron los datos de la tarjeta en el dispositivo y la capacidad de ingreso de PIN de la terminal
2	TERM-ENTRY-CAP	14	14	1	X(1)	La capacidad de la terminal. Este campo se definido por el proceso adquirente. Los valores válidos son los siguientes:
					LVL 2	0 = Desconocido
						2 = Capacidad de lectura de banda magnética
						5 = Capacidad de lectura de chip de contacto
3	LAST-EMV-STAT	15	15	1	X(1)	Indica si la tarjeta utilizada para iniciar una transacción de banda magnética es una tarjeta chip. Los valores válidos son los siguientes:
					LVL 2	0 = No es una tarjeta con chip
						1 = Es una tarjeta con chip " " = Campo no utilizado
4	DATA-SUSPECT	16	16	1	X(1)	Indica si el método de autenticación de los datos de la tarjeta (CAM) es confiable. Este indicador se establece mediante el proceso de adquisición. Los valores válidos son los siguientes:
					LVL 2	0 = Datos de CAM son correctos
						1 = Datos de CAM no son confiables " " = Campo no utilizado
5	APPL-PAN-SEQ-NUM	17	18	2	X(2) LVL 2	El número de secuencia de aplicación del PAN (Tag 5F34). Este campo identifica y diferencia las tarjetas con el mismo PAN. Este campo contiene espacios si la tarjeta no incluye un número de secuencia de aplicación del PAN
6	DEV-INFO	19	24	6	X(6) LVL 2	Campo de información del dispositivo. Este campo contiene datos específicos del dispositivo.
6A	CAM-FLAGS	19	24		LVL 2	REDEFINE DEV-INFO
						Identifica las condiciones encontradas en la terminal. Los valores válidos se muestran en las tablas siguientes. El valor por defecto para todos los bits es un valor 0. Este campo es específico de transacciones en cajeros automáticos.
						Este campo es específico de un terminal NCR y se define por NCR en la *Especificación Funcional NCR NDC + CAM 2.*
						Byte 1
						Como se define por NCR
						Posición Descripción
						4 Indicador de recuperación de los datos de la aplicación. Los valores

						válidos son los siguientes:
						0 = La recuperación de datos de la aplicación fue exitosa.
						1 = La recuperación de datos de la aplicación no fue exitosa.
						3 Indicador de obtención de opciones de procesamiento. Los valores válidos son los siguientes:
						0 = Obtención de opciones de procesamiento exitosa.
						1 = obtención de opciones de procesamiento fallida.
						2 Indicador de selección de aplicaciones. Los valores válidos son los siguientes:
						0 = Selección de aplicación exitosa
						1 = Selección de aplicación no exitosa
						Byte 2
						Como se define por NCR
						Posición Descripción
						8 Bandera de lista de opciones de procesamiento de objetos de datos (PDOL). Los valores válidos son los siguientes:
						0 = Datos PDOL válidos.
						1 = Datos PDOL inválidos..
						7 Bandera de lista de objetos de datos de administración de riesgo de la tarjeta (CDOL1). Los valores válidos son los siguientes:
						0 = Datos CDOL1 válidos.
						1 = Datos CDOL1 inválidos.
						6 Bandera de comando GENERATE AC. Los valores válidos son los siguientes:
						0 = GENERATE AC exitoso.
						1 = GENERATE AC falló.
						4 Bandera de procesamiento del método de autenticación de la tarjeta (CAM). Los valores válidos son los siguientes:
						0 = Procesamiento de CAM no exitoso.
						1 = Procesamiento de CAM exitoso.
						3 Bandera procesamiento de entrada fácil. Los valores válidos son los siguientes:
						0 = Procesamiento de entrada fácil iniciada.
						1 = Procesamiento de entrada fácil no iniciada.
						2 Bandera de inicio de procesamiento CAM. Los valores válidos son los siguientes:
						0 = Procesamiento CAM iniciado.
						1 = Procesamiento CAM no iniciado.
6B	CVM-RSLTS	19	24		LVL 2	REDEFINES DEV-INFO
						Resultados del último método de verificación del tarjetahabiente (CVM) realizado. Los valores válidos se muestran en las tablas siguientes. El valor por defecto para todos los bits es un valor 0. Este campo es específico de las transacciones de terminal punto de venta.
						Este campo se define como 24 bits (tres bytes) por EMV, pero se convierte a seis bytes ASCII, cada uno contienen un carácter hexadecimal que representa cuatro bits cuando se incluye en el token.
						Byte 1 (CVM Realizado)
						Posición Descripción
						7 0 = Falla la verificación del tarjetahabiente si este CVM no es exitoso
						1 = Aplicar la siguiente regla de verificación de la tarjeta (CVR) si este CVM no es exitoso
						6–1 000000= Procesamiento de CVM fallido
						000001 = Verificación de PIN en texto plano realizada por el chip de la tarjeta
						000010 = PIN cifrado verificado en línea
						000011 = Verificación de PIN en texto plano realizada por el chip de la tarjeta y firma (papel)
						000100 = Verificación de PIN cifrado realizada por el chip de la tarjeta
						000101 = Verificación de PIN cifrado realizada por el chip de la tarjeta y firma (papel)
						0xxxxx = Los valores en el rango 000110 - 011101 están reservados para uso futuro por la especificación EMV
						011110 = Firma (papel)
						011111 = No se requiere CVM
						10xxxx = Los valores en el rango 100000 – 101111 están reservados para uso futuro por los sistemas de pago
						11xxxx = Los valores en el rango 110000 – 111110 están reservados para uso futuro por el Emisor
						111111 = No disponible para su uso
						Byte 2 Condición de CVM
						Valor Descripción
						00 Siempre
						01 Efectivo o cashback
						02 No es efectivo o cashback
						03 Terminal es compatible con la CVM

						04 Reservado para uso futuro
						05 Reservado para uso futuro
						06 La transacción es en la moneda de la aplicación y se encuentra bajo 'x' valor
						07 La transacción es en la moneda de la aplicación y se encuentra arriba de 'x' valor
						08 La transacción es en la moneda de la aplicación y se encuentra bajo 'y' valor
						09 La transacción es en la moneda de la aplicación y se encuentra arriba de 'y' valor
						0A–7F Reservado para uso futuro
						80–FF Reservado para uso futuro en los sistemas de pago
						Byte 3 Resultado de CVM
						Valor Descripción
						0 Desconocido (por ejemplo firma)
						1 Fallido (por ejemplo PIN offline)
						2 Exitoso (por ejemplo PIN offline)
6C	ICHG-DEF	19	24		LVL 2	REDEFINES DEV-INFO
						La definición de intercambio. Este campo es utilizado solamente por la interfaz de VisaNet
6D	APPRVD-RC	19	20	2	X(2) LVL 4	En algunas de las solicitudes de autorización recibidas a través de la interfaz de intercambio, este campo contiene el Código de Respuesta de Autorización (ARC) que se requieren para la generación del Criptograma de Respuesta de Autorización (ARPC)
6D	UNUSED	21	24	4	X(4) LVL 4	Este campo está reservado para un uso futuro.
7	RSN-ONL-CDE	25	28	4	X(4) LVL 2	El código de razón del mensaje especifica qué una transacción vaya a autorizarse en línea (en lugar de ser completada localmente), o por qué una transacción se ha completado de forma local (en lugar de ser autorizados en línea). Los valores se definen en la norma ISO 8583 (1993) Estándar
8	ARQC-VRFY	29	29	1	X(1)	Resultado de la verificación del Criptograma de Solicitud de Autorización (ARQC). Los valores válidos son los siguientes:
					LVL 2	0 = ARQC no verificado
						1 = ARQC revisado por un switch y falló la verificación
						2 = ARQC revisado por un switch y pasó la verificación
						3 = ARQC revisado por un emisor y falló la verificación
						4 = ARQC revisado por un emisor y pasó la verificación
						9 = ARQC no verificado; la transacción fue degradada a banda magnética en lugar de chip " " = Valor por default
9	ISO-RC-IND	30	30	1	X(1) LVL 2	Indicador de Código de Respuesta ISO 8583 (1987). Este campo indica si el código de respuesta enviado al intercambio debe ser utilizado en la generación del criptograma respuesta de autorización (ARPC), o si el código de respuesta ISO recibido del intercambio debe ser devuelto a la terminal como el Código de respuesta de autorización. Los valores válidos son los siguientes:
						" " = No hay información disponible (donde " "-indica un espacio en blanco)
						0 = No utilice el código de respuesta de intercambio
						1 = Utilice el código de respuesta provisto en la generación del ARPC para transacciones aprobadas
						9 = Utilice el código de respuesta de intercambio como ARC enviado al terminal

Token B4 subcampo 6 se deriva en las siguientes posibilidades

B4 STATUS TOKEN				
C	LONGITUD	INICIO	FIN	NOMBRE
6A	6	9	14	CAM-FLAGS
6B	6	9	14	CVM-RSLTS
6C	6	9	14	ICHG-DEF
6D	2	9	10	APPRVD-RC
6D	4	11	14	UNUSED

TOKEN B5: DATOS EMV DE RESPUESTA

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador de inicio de Token.
						! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador
						" " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando.
						B5 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección de datos del Token.
						00038 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador

						" " = valor fijo (Espacio en blanco)
1	ISS-AUTH-DATA-LGTH	11	14	4	X(4) LVL 2	Longitud de la representación binaria de los datos en el campo siguiente. Las versiones ASCII y binarias del token deben contener el mismo valor en este campo. La versión ASCII del token debe contener la representación del valor de longitud en decimal (no hexadecimal)
2	EMV-ISS-AUTH-DATA				X(32) LVL 2	Los datos se justifican a la izquierda y se rellena a la derecha con ceros binarios.
3	ISS-AUTH-DATA REDEFINES EMV-ISS-AUTH-DA				LVL 2	Datos de autenticación del Emisor (Tag 91) enviado al chip de la tarjeta para la autenticación del Emisor en línea.
4	ARPC	15	30	16	X(16) LVL 4	Criptograma de respuesta de autorización calculado por la aplicación de la tarjeta para la autenticación del Emisor en línea.
5	ADDL-DATA	31	46	16	X(16) LVL 4	Datos adicionales de autenticación del Emisor utilizados en el algoritmo para calcular el criptograma de respuesta de autorización.
5ª	VISA-ADDL-DATA	31	46		LVL 4	REDEFINE ADDL-DATA Definición Visa / UKIS de los datos adicionales de autenticación del Emisor.
5A	ISS-RESP-CDE	31	34	4	X(4) LVL 6	
5ª	INFO	35	46	12	X(12) LVL 6	
5B	MCPA-ADDL-DATA	31	46	16	LVL 4	REDEFINE ADDL-DATA Definición MChip 2.1 de los datos adicionales de autenticación del Emisor.
5B	ISS-AUTH-RESP-CDE	31	34	4	X(4) LVL 6	
5B	INFO	35	46	12	X(12) LVL 6	
5C	MCHIP4-ADDL-DATA				LVL 4	REDEFINE ADDL-DATA Definición MChip 4 de los datos adicionales de autenticación del Emisor
5C	ARPC-RESP-CDE	31	34	4	X(4) LVL 6	
5C	INFO	35	46	12	X(12) LVL 6	
5D	CCD-A-AUTH-DATA	31	46	16	LVL 2	REDEFINES EMV-ISS-AUTH-DATA
5D	EMV-ISS-AUTH-DATA					
	ARPC	15	22	8	X(8) LVL 4	
5D	CRD-STAT-UPDT	23	30	8	X(8) LVL 4	
5D	ADDL-DATA	31	46	16	X(16) LVL 4	Datos adicionales de autenticación del emisor.
6	SEND-CRD-BLK	47	47	1	X(1) LVL 2	Código que indica si un script de bloqueo de la tarjeta va a ser generado por el proceso de autorización y enviado al ICC. Los valores válidos son los siguientes: C = Enviar un script de cambio de PIN N = No enviar un script bloqueo de tarjeta U = Enviar un script de desbloqueo del PIN Y = Enviar un script de bloqueo de tarjeta " " = Campo no utilizado
7	SEND-PUT-DATA	48	48	1	X(1) LVL 2	Código que indica si un script de ingreso de datos va a ser generado por el proceso de autorización y enviado al ICC. Los valores válidos son los siguientes: Y = Enviar un script de ingreso de datos N = No enviar un script de ingreso de datos " " = Campo no utilizado

TOKEN B6: DATOS DE SCRIPT EMV

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. B6 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección datos de Token. valor variable hasta 00260
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	ISS-	11	14	4	X(4)	Longitud de la representación binaria de los datos en el campo siguiente. Las

	SCRIPT-DATA-LGTH				LVL 2	versiones ASCII y binarias del token deben contener el mismo valor en este campo. La versión ASCII del token debe contener la representación del valor de longitud en decimal (no hexadecimal)
2	ISS-SCRIPT-DATA	15	270	256	X(256) LVL 2	Las plantillas de script emisor (Tag 71 y / o 72) enviadas a la terminal para su procesamiento por el chip de la tarjeta. Cada plantilla puede contener un ID de script y una o más scripts de comandos. Los datos se justifica a la izquierda y se rellenan a la derecha con ceros binarios

TOKEN BJ: RESULTADOS DE SCRIPTS EMISOR EMV

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. BJ = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección datos de Token. Fijo = 82
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	NUM-ISS-SCRIPT-RSLTS	11	11	1	X(1)	Número de scripts completados contenidos en el token
2	USER-FLD1	12	12	1	X(1)	Para uso futuro
3	ISS-SCRIPT-RSLTS-DATA	13	92	80	x(80)	Ocurre de 0 a 8 veces dependiendo del campo NUM-ISS-SCRIPT-RSLTS
3a	ISS-SCRIPT-PROC-RSLT	13	13	1	x(1)	Código que indica el resultado del procesamiento del script. Los valores son los siguientes: 0 = Script no ejecutado 1 = Script fallido 2 = Script exitoso 9 = Script desconocido
3a	ISS-SCRIPT-SEQ	14	14	1	x(1)	Detalles del procesamiento del script. Los valores son los siguientes: 0 = Script de secuencia no especificada, script no ejecutado, todos los comandos fueron exitosos. 1-9, A-E = Número de secuencia del 1-14 para comandos fallidos. F = Número de secuencia si es 15 o superior para comandos fallidos.
3a	ISS-SCRIPT-ID	15	22	8	x(8)	Identificador del script Emisor.
3b	ISS-SCRIPT-PROC-RSLT	23	23	1	x(1)	
3b	ISS-SCRIPT-SEQ	24	24	1	x(1)	
3b	ISS-SCRIPT-ID	25	32	8	x(8)	
3c	ISS-SCRIPT-PROC-RSLT	33	33	1	x(1)	
3c	ISS-SCRIPT-SEQ	34	34	1	x(1)	
3c	ISS-SCRIPT-ID	35	42	8	x(8)	
3d	ISS-SCRIPT-PROC-RSLT	43	43	1	x(1)	
3d	ISS-SCRIPT-SEQ	44	44	1	x(1)	
3d	ISS-SCRIPT-ID	45	52	8	x(8)	
3e	ISS-SCRIPT-PROC-RSLT	53	3	1	x(1)	
3e	ISS-SCRIPT-	54	54	1	x(1)	

	SEQ					
3e	ISS-SCRIPT-ID	55	62	8	x(8)	
3f	ISS-SCRIPT-PROC-RSLT	63	63	1	x(1)	
3f	ISS-SCRIPT-SEQ	64	64	1	x(1)	
3f	ISS-SCRIPT-ID	65	72	8	x(8)	
3g	ISS-SCRIPT-PROC-RSLT	73	73	1	x(1)	
3g	ISS-SCRIPT-SEQ	74	74	1	x(1)	
3g	ISS-SCRIPT-ID	75	82	8	x(8)	
3h	ISS-SCRIPT-PROC-RSLT	83	83	1	x(1)	
3h	ISS-SCRIPT-SEQ	84	84	1	x(1)	
3h	ISS-SCRIPT-ID	85	92	8	x(8)	

BJ RESULTADOS DE SCRIPTS EMISOR EMV				
#	Longitud	Inicio	Fin	NOMBRE
H-1	1	1	1	EYE-CATCHER
H-2	1	2	2	USER-FLD1
H-3	2	3	4	ID
H-4	5	5	9	Longitud del token
H-5	1	10	10	USER-FLD2
1	1	1	1	NUM-ISS-SCRIPT-RSLTS
2	1	2	2	USER-FLD1
3	80	3	82	ISS-SCRIPT-RSLTS-DATA

Token BJ subcampo 3 se deriva en las siguientes posibilidades

#	LONGITUD	INICIO	FIN	NOMBRE
3a				ISS-SCRIPT-RSLTS-DATA
3a	1	3	3	ISS-SCRIPT-PROC-RSLT
3a	1	4	4	ISS-SCRIPT-SEQ
3a	8	5	12	ISS-SCRIPT-ID
3b	1	13	13	ISS-SCRIPT-PROC-RSLT
3b	1	14	14	ISS-SCRIPT-SEQ
3b	8	15	22	ISS-SCRIPT-ID
3c	1	23	23	ISS-SCRIPT-PROC-RSLT
3c	1	24	24	ISS-SCRIPT-SEQ
3c	8	25	32	ISS-SCRIPT-ID
3d	1	33	33	ISS-SCRIPT-PROC-RSLT
3d	1	34	34	ISS-SCRIPT-SEQ
3d	8	35	42	ISS-SCRIPT-ID
3e	1	43	43	ISS-SCRIPT-PROC-RSLT
3e	1	44	44	ISS-SCRIPT-SEQ
3e	8	45	52	ISS-SCRIPT-ID
3f	1	53	53	ISS-SCRIPT-PROC-RSLT
3f	1	54	54	ISS-SCRIPT-SEQ
3f	8	55	62	ISS-SCRIPT-ID
3g	1	63	63	ISS-SCRIPT-PROC-RSLT
3g	1	64	64	ISS-SCRIPT-SEQ
3g	8	65	72	ISS-SCRIPT-ID
3h	1	73	73	ISS-SCRIPT-PROC-RSLT
3h	1	74	74	ISS-SCRIPT-SEQ
3h	8	75	82	ISS-SCRIPT-ID

TOKEN 25: SURCHARGE

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. 25 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección datos: 00070 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	TRAN-FEE	11	29	19	X(19)	The transaction surcharge amount assessed. If the amount in this field is a negative amount, it must be preceded by a minus sign (–). En este campo se incluye la tarifa Surcharge
2	ORIG-FEE	30	48	19	X(19)	The original transaction surcharge assessed. If the amount in this field is a negative amount, it must be preceded by a minus sign (–).
3	TERM-SUR-PROFILE	49	52	4	X(04)	The surcharge profile assigned to the terminal.
4	RVSL-CDE	53	53	1	X(01)	A code specifying the surcharge requirements for partial reversals. Valid values are as follows: 0 = No fee on partial reversals 1 = Fee on partial reversals
5	FLAT-FEE	54	72	19	X(19)	The static surcharge amount, in the currency defined. If the amount in this field is a negative amount, it must be preceded by a minus sign (–).
6	PCNT-FEE	73	77	5	X(05)	The surcharge percentage in one hundredths of a percent (for example 100 = 1%). If the value in this field is a negative percentage, it must be preceded by a minus sign (–).
7	MIN-MAX	78	78	1	X(01)	An indicator specifying the interaction between the FLAT-FEE and PCNT-FEE fields. Valid values are as follows: 0 = The surcharge is the greater amount of the flat fee and the percent fee 1 = The surcharge is the lesser amount of the flat fee and the percent fee.
8	AUTH-IND	79	79	1	X(01)	A code specifying the surcharge notification process required by the ATM. Valid values are as follows: " " = Request notification (where " " is a blank character) 0 = Request notification 1 = Response notification D = Fee assessment/notification is complete; surcharge fee declined M = Misconfiguration Z = Fee assessment/notification is complete
9	USER-FLD1	80	80	1	X(01)	Filler, Espacio en blanco

TOKEN B1: NOMBRE DE INSTITUCIÓN EMISORA (USO DE LÍNEA DE CRÉDITO)

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(01)	Header de Token: Identificador inicio de Token. ! = valor fijo (Admiración Cerrada)
H-2	USER-FLD1	2	2	1	X(01)	Header de Token: Primer Separador " " = valor fijo (Espacio en blanco)
H-3	Identificador del Token	3	4	2	X(02)	Header de Token: Identificación del Token que se está enviando. B1 = valor fijo
H-4	Longitud de datos	5	9	5	9(05)	Header de Token: Longitud de la sección datos: 00450 = valor fijo
H-5	USER-FLD2	10	10	1	X(01)	Header de Token: Segundo Separador " " = valor fijo (Espacio en blanco)
1	LGTH	11	13	3	X(03)	La longitud de los datos del Token B1sin incluir el encabezado y el campo LGTH
2	USER-FLD1	14	14	1	X(01)	Campo para uso futuro, rellenar con cero
3	FIID	15	18	4	X(04)	FIID del banco que envía el token
4	BUF	19	460	442	X(442)	Campo utilizado para poner el nombre del banco

TOKEN PO: FACTORES DE AUTENTICACIÓN ADQUIRENTE

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(1)	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	1	X(1)	Header de Token: Separador 1. " " valor fijo
H-3	Identificador del Token	3	4	2	X(2)	Header de Token: Identificación del token que se está enviando. **PO** valor fijo
H-4	Longitud de datos	5	9	5	9(5)	Header de Token: Longitud de la sección de datos del token. **00080** valor fijo
H-5	USER-FLD2	10	10	1	X(1)	Header de Token: Separador 2. " " valor fijo
1	Bandera de capacidad del Adquirente para utilizar FDA.	11	12	2	X(2)	Adquirente graba, Emisor lee. Esta bandera indica la capacidad del Adquirente para utilizar FDA. 00 = El Adquirente no utiliza FDA. 01 = El Adquirente utiliza FDA.
2	Bandera de capacidad del Comercio para utilizar FDA.	13	14	2	X(2)	Comercio indica, Adquirente graba, Emisor lee. Esta bandera indica la capacidad del Comercio para utilizar FDA. 00 = El Comercio no utiliza FDA. 01 = El Comercio utiliza FDA.
3	Bandera de estatus del FDA de parte del comercio	15	16	2	X(2)	Comercio indica, Adquirente graba, Emisor lee. Esta bandera indica el estatus del FDA por parte del Adquirente. 00 = Comercio no utiliza FDA, Adquirente soporta FDA pero no puede enviar FDA. 01 = Comercio utiliza FDA, Adquirente envía FDA. 02 = Comercio utiliza FDA, Adquirente no evía FDA. 03 = Comercio realiza verificación del tarjetahabiente por dispositivo, Adquirente envía FDA. 04 = Comercio no utiliza FDA, Adquirente no envía FDA. 05 = Token generado por default. No construyo el Adquirente. 06 = Reservado para uso futuro.
4	Factor de Autenticación (FDA); Elemento de Verificación del Tarjetahabiente (EVT).	17	32	16	X(16)	Comercio obtiene, Adquirente graba, Emisor lee. Es el Elemento de Verificación del Tarjetahabiente (EVT), el cual es proporcionado al Comercio y enviado como Factor de Autenticación (FDA) al Emisor. El campo debe estar justificado a la izquierda, rellenando con espacios las posiciones que no sean ocupadas. En caso de no ser utilizado, se rellena con espacios.

5	Bandera de uso de los Elementos no convencionales (ENC) por parte del Comercio.	33	33	1	X(1)	Comercio indica, Adquirente graba, Emisor lee. Esta bandera indica si el Comercio utiliza los Elementos No Convencionales (ENC); Estos se utilizan para el Análisis de Riesgo. 0 = No utilizan ENC. 1 = Si utilizan ENC.
6	ENC - Bandera de capacidad del Comercio para ejecutar Análisis de Riesgo.	34	34	1	X(1)	Comercio indica, Adquirente graba, Emisor lee. Esta bandera indica si el Comercio utiliza los ENC para ejecutar el Análisis de Riesgo. " " = No utilizan ENC. 0 = El Comercio no puede ejecutar Análisis de Riesgo con ENC Propios. 1 = El Comercio puede ejecutar Análisis de Riesgo con ENC Propios.
7	ENC - Resultado de Análisis del Comercio en la ejecución del Análisis de Riesgo.	35	35	1	X(1)	Comercio indica, Adquirente graba, Emisor lee. Esta bandera indica el resultado del Comercio al ejecutar el Análisis de Riesgo. " " = No utilizan ENC. 0 = Análisis de Riesgo con ENC no realizada. 1 = Análisis de Riesgo con ENC fallida. 2 = Análisis de Riesgo con ENC exitosa.
8	ENC - Dirección IP del Dispositivo Origen de la compra.	36	50	15	X(15)	Comercio obtiene, Adquirente graba, Emisor lee. Campo utilizado para la dirección IP del Dispositivo Origen de la Compra proporcionada por el Comercio. El campo debe estar justificado a la izquierda, rellenando con espacios las posiciones que no sean ocupadas.
9	ENC - Identificador del Dispositivo Origen de la compra.	51	67	17	X(17)	Comercio obtiene, Adquirente graba, Emisor lee. Campo utilizado para el identificador del Dispositivo Origen de la Compra proporcionada por el Comercio. El campo debe estar justificado a la izquierda, rellenando con espacios las posiciones que no sean ocupadas.
10	USER-FLD3	68	90	23	X(23)	Uso Futuro. Se rellena con espacios.

TOKEN PY: FACTORES DE AUTENTICACIÓN EMISOR

#	NOMBRE	INICIO	FIN	LONG	FORMATO	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	1	X(1)	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	1	X(1)	Header de Token: Separador 1. “ “ valor fijo
H-3	Identificador del Token	3	4	2	X(2)	Header de Token: Identificación del token que se está enviando. **PY** valor fijo
H-4	Longitud de datos	5	9	5	9(5)	Header de Token: Longitud de la sección de datos del token. **00060** valor fijo
H-5	USER-FLD2	10	10	1	X(1)	Header de Token: Separador 2. “ “ valor fijo
1	Bandera de capacidad del Emisor para utilizar FDA.	11	12	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica la capacidad del Emisor para utilizar FDA. 00 = El Emisor no utiliza FDA. 01 = El Emisor utiliza FDA.
2	Bandera de estatus de Elementos de Seguridad.	13	14	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica si el Emisor entrego elementos de seguridad al Tarjetahabiente. 00 = Tarjetahabiente no tiene elementos de seguridad. 01 = Tarjetahabiente tiene elementos de seguridad y no se utilizó. 02 = Tarjetahabiente tiene elementos de seguridad y se utilizó.

3	Bandera de estatus del Emisor y los FDA.	15	16	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el estatus del FDA por parte del Emisor. 00 = Comercio y Adquirente no pueden enviar FDA, Emisor no realiza DFA. 01 = Comercio y Adquirente pueden enviar FDA, Emisor no realiza DFA. 02 = Se generan FDA, Comercio y Adquirente envian FDA, Emisor realiza DFA. 03 = Se generan FDA, Comercio y Adquirente no envía FDA, Emisor realiza DFA. 04 = Comercio no soporta FDA, Adquirente pueden enviar FDA, Emisor no realiza DFA. 05 = Comercio realiza verificación del tarjetahabiente por dispositivo del cliente, Adquirente envía FDA, Emisor genera DFA. 06 = Token generado por default. No construyo el Emisor. 07 = Reservado para uso futuro.
4	Factor "A" - Primer Factor; Algo que **"tiene"** el tarjetahabiente.	17	18	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el primer método de validación del Factor "A" del DFA; Algo que **"tiene"** el tarjetahabiente. " " = No se utiliza Factor "A" para DFA. 00 = CVV Dinámico. 01 = Tarjeta Tokenizada. 02 = Tarjeta Dinámica. 03 = One Time Password (OTP). 04 = Autenticación por SMS. 05 = Autenticación por Banca por internet (Banca Electrónica de la institución). 06 = Dispositivo registrado. 07 = Reservado para uso futuro.
5	Factor "A" - Segundo Factor; Algo que **"tiene"** el tarjetahabiente.	19	20	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el segundo método de validación del Factor "A" del DFA; Algo que **"tiene"** el tarjetahabiente. " " = No se utiliza Factor "A" para DFA. 00 = CVV Dinámico. 01 = Tarjeta Tokenizada. 02 = Tarjeta Dinámica. 03 = One Time Password (OTP). 04 = Autenticación por SMS. 05 = Autenticación por Banca por internet (Banca Electrónica de la institución). 06 = Dispositivo registrado. 07 = Reservado para uso futuro.
6	Resultado Verificación Factor "A"; Algo que **"tiene"** el tarjetahabiente.	21	21	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica el resultado de la validación del Factor "A" del DFA; Algo que **"tiene"** el tarjetahabiente. " " = El emisor no realiza DFA por Factor A. 0 = No se recibió FDA de Factor A. 1 = Validación exitosa con un Factor A. 2 = Validación exitosa con más de un Factor A. 3 = Validación no exitosa.
7	Factor "B" - Primer Factor; Algo que **"sabe"** el tarjetahabiente.	22	23	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el primer método de validación del Factor "B" del DFA; Algo que **"sabe"** el tarjetahabiente. " " = No se utiliza Factor "B" para DFA. 00 = Contraseña. 01 = Pregunta de seguridad. 02 = NIP. 03 = Otros. 04 = Reservado para uso futuro.
8	Factor "B" - Segundo Factor; Algo que **"sabe"** el tarjetahabiente.	24	25	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el segundo método de validación del Factor "B" del DFA; Algo que **"sabe"** el tarjetahabiente. " " = No se utiliza Factor "B" para DFA. 00 = Contraseña. 01 = Pregunta de seguridad. 02 = NIP. 03 = Otros. 04 = Reservado para uso futuro.
9	Resultado de Verificación Factor "B"; Algo que **"sabe"** el tarjetahabiente.	26	26	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica el resultado de la validación del Factor "B" del DFA; Algo que **"tiene"** el tarjetahabiente. " " = El emisor no realiza DFA por Factor B. 0 = No se recibió FDA de Factor B. 1= Validación exitosa con un Factor B. 2 = Validación exitosa con más de un Factor B. 3 = Validación no exitosa.

10	Factor "C" - Primer Factor; Algo que **"es"** el tarjetahabiente. (Biométrico).	27	28	2	X(02)	Emisor graba, Adquirente lee. Esta bandera indica el primer método de validación del Factor "C" del DFA; Algo que **"es"** el tarjetahabiente. " " = No se utiliza Factor "C" para DFA. 00 = Biometría Huella Dactilar. 01 = Biometría Vascular Huella Dactilar. 02 = Biometría Facial. 03 = Biometría Ocular (Iris/Retina). 04 = Biometría del Comportamiento. 05 = Reconocimiento Biométrico de Voz. 06 = Reconocimiento Biométrico de la Palma de la Mano. 07 = Sistema de reconocimiento de Firma. 08 = Reservado para uso futuro.
11	Factor "C" - Segundo Factor; Algo que **"es"** el tarjetahabiente. (Biométrico).	29	30	2	X(2)	Emisor graba, Adquirente lee. Esta bandera indica el segundo método de validación del Factor "C" del DFA; Algo que **"es"** el tarjetahabiente. " " = No se utiliza Factor "C" para DFA. 00 = Biometría Huella Dactilar. 01 = Biometría Vascular Huella Dactilar. 02 = Biometría Facial. 03 = Biometría Ocular (Iris/Retina). 04 = Biometría del Comportamiento. 05 = Reconocimiento Biométrico de Voz. 06 = Reconocimiento Biométrico de la Palma de la Mano. 07 = Sistema de reconocimiento de Firma. 08 = Reservado para uso futuro.
12	Resultado de Verificación Factor "C"; Algo que **"es"** el tarjetahabiente.	31	31	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica el resultado de la validación del Factor "C" del DFA; Algo que **"es"** el tarjetahabiente. " " = El emisor no realiza DFA por Factor C. 0 = No se recibió FDA de Factor C. 1= Validación exitosa con un Factor C. 2 = Validación exitosa con más de un Factor C. 3 = Validación no exitosa.
13	Resultado del DFA.	32	32	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica el resultado del DFA. " " = El emisor no realizó DFA. 0 = Validación no exitosa. 1 = Validación exitosa.
14	Bandera de uso de los Elementos no convencionales (ENC) por parte del Emisor.	33	33	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica si el Emisor utiliza los Elementos No Convencionales (ENC); Estos se utilizan para el Análisis de Riesgo. 0 = No utilizan ENC. 1 = Si utilizan ENC.
15	ENC - Bandera de capacidad del Emisor para ejecutar Análisis de Riesgo.	34	34	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica si el Emisor utiliza los ENC para ejecutar Análisis de Riesgo. " " = No utilizan ENC. 0 = El Emisor no puede ejecutar Análisis de Riesgo con ENC Propios. 1 = El Emisor puede ejecutar Análisis de Riesgo con ENC Propios.
16	ENC - Resultado de Análisis del Emisor en la ejecución del Análisis de Riesgo.	35	35	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica el resultado del Emisor al ejecutar el Análisis de Riesgo. " " = No utilizan ENC. 0 = Análisis de Riesgo con ENC no realizada. 1 = Análisis de Riesgo con ENC fallida. 2 = Análisis de Riesgo con ENC exitosa.
17	ENC - Dirección IP del Dispositivo Origen de la compra.	36	36	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica si el Emisor recibió la Dirección IP del Dispositivo Origen. " " = No utiliza ENC - Dirección IP del Dispositivo Origen. 0 = El Comercio no mandó Dirección IP del Dispositivo Origen. 1 = El Comercio mandó Dirección IP del Dispositivo Origen.
18	ENC - Identificador del Dispositivo Origen de la compra.	37	37	1	X(1)	Emisor graba, Adquirente lee. Esta bandera indica si el Emisor recibió el Identificador del Dispositivo Origen. " " = No utiliza ENC - Identificador del Dispositivo Origen. 0 = No se recibió ENC - Identificador del Dispositivo Origen. 1 = Si se recibió ENC - Identificador del Dispositivo Origen.
19	USER-FLD3	38	70	33	X(33)	Uso Futuro. Se rellena con espacios.

TOKEN TV: FACT ADITIONAL DATA – VISA

#	NOMBRE	INICIO	FIN	FORMATO	LONG	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	X(01)	1	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	X(01)	1	Header de Token: Separador 1. " " valor fijo
H-3	Identificador del Token	3	4	X(02)	2	Header de Token: Identificación del token que se está enviando. TV valor fijo
H-4	Longitud de datos	5	9	9(05)	5	Header de Token: Longitud de la sección de datos del token. 00230 valor fijo
H-5	USER-FLD2	10	10	X(01)	1	Header de Token: Separador 2. " " valor fijo
1	Network Identification Code DE-63.1	11	14	Numérico	4	0002 VISA
2	Message Reason Code DE-63.3	15	18	Numérico	4	Reason Code/Description 3700 Token create 3701 Token deactivate 3702 Token suspend 3703 Token resume 3711 Device provisioning result 3712 OTP verification result 3713 Call Center activation 3714 Mobile banking app activation 3715 Replenishment confirmation of limited-use keys
3	File Name DE-101	19	35	ANS	17	PAN = Card Data. TERMS-CONDITIONS = Token Terms and Conditions TK = Token
Verification & Token Data Dataset ID = 68 DE-123						
4	Elapsed Time To Live DE-123.1F31	36	39	Numérico	4	This tag contains the elapsed time in hours since the current limited-use key (LUK) is provisioned on the device.
5	Count of Number of Transactions DE-123.1F32	40	42	Numérico	3	This tag contains the cumulative count of transactions for the current limited-use key (LUK).
6	Cumulative Transaction Amount DE-123.1F33	43	49	Numérico	7	This tag contains the cumulative total of transaction amounts in USD for the current limited-use key (LUK).
7	Token DE-123.01	50	68	x-nVar	19	This tag contains the token that is used to replace the cardholder PAN and is a required data element for token processing.
8	Token Assurance Level DE-123.02	69	70	Numérico	2	Reserved for future use. This field contains spaces.
9	Token Requestor ID DE-123.03	71	81	Numérico	11	This tag contains the Token requestor ID.
10	Primary Account Number, Account Range DE-123.04	82	100	x-nVar	19	This tag contains the first nine digits of the cardholder PAN or the full cardholder PAN. V.I.P. forwards the cardholder PAN data to the acquirer in the original response message. Acquirers must not forward the first nine digits of the cardholder PAN or the full PAN to their merchants For MasterCard, this tag contains the full cardholder PAN in 0110 response messages.
11	Token Reference ID DE-123.05	101	132	x-nVar	32	This tag contains the Token reference ID.
12	Token Expiration Date DE-123.06	133	136	Numérico	4	This tag will contain the Token expiration date. The date is in yymm format, where yy = year (00–99) and mm = month (01–12).
13	Token Type DE-123.07	137	138	x-nVar	2	This tag contains one of the following valid values: 01 = ECOM/COF (e-commerce/ card on file). 02 = SE (secure element). 03 = CBP (cloud-based payment). 05 = E-commerce enabler

14	Token Status DE-123.08	139	139	x-nVar	1	This tag contains the token status. Valid values: A = Active for payment I = Inactive for payment (not yet active) S = Temporarily suspended for payments D = Permanently deactivated for payments
15	Last Updated By DE-123.0A	140	140	x-nVar	1	This tag is present in the response when the token is located.
16	PAN Reference ID DE-123.0B	141	172	ANS	32	This tag contains a unique reference ID generated by Visa for the card account number. This tag is required in 0302 Token File Inquiry Messages if Field 2—Primary Account Number is not present.
17	Activation Code DE-123.1A	173	180	x-nVar	8	This tag is present in the response when the token is located and contains obfuscated version of the activation code (OTP) on file. This tag is present when the activation code is expired. See activation code expiry date/time.
18	Activation Code Expiry Date/Time Tab 1B	181	192	N, BCD	12	This tag contains the date and time that the activation code expires. The format is yymmddhhmmss expressed in GMT.
19	Activation Code Verification Attempts DE-123.1C	193	194	N, BCD	2	This tag contains the number of attempts to verify the current activation code.
20	Number of Activation Codes Issued DE-123.1D	195	196	N, BCD	2	This tag contains the total number of token activation codes issued.
21	Visa Token Score DE-123.10	197	198	Numérico	2	This tag contains the degree of risk associated with the token. The valid values are from 01–99.
22	Visa Token Decisioning DE-123.11	199	200	Numérico	2	This tag contains the results of the token provisioning decision. The valid values are: 00 = Provision and activate. 05 = Do not provision. 85 = Provision inactive state – requires further consumer authentication before activation.
23	Number of Active Tokens DE-123.12	201	202	Numérico	2	This tag contains the number of device tokens currently active for this PAN.
24	Number of Inactive Tokens DE-123.13	203	204	Numérico	2	This tag contains the number of device tokens currently inactive (device tokens that have not been activated) for this PAN.
25	Number of Suspended Tokens DE-123.14	205	206	Numérico	2	This tag contains the number of device tokens that were activated, but are suspended for payments for this PAN.
PAN—PAN File Maintenance DE-127						
26	Replacement PAN DE-127.1	207	225	Numérico	19	This field contains the replacement primary account number. This field is required when the PAN contained in Field 2—Primary Account Number is being replaced with a new PAN.
27	Replacement PAN Expiration Date DE-127.2	226	229	Numérico	4	This field contains the expiration date of the new PAN in tag 01 or the updated expiration date of the existing PAN. Format = yymm.
COF + Tokenización						
28	Transaction Indicator DE-60.6	230	230	ANS	1	0 = No aplicable. En el mensaje VISA los campos subsecuentes del campo 60 están presentes. 1 = En el mensaje VISA el tercer mapa de bits estándar o campo 55 es utilizado para enviar datos de chips. 2 = En el mensaje VISA el tercer mapa de bits expandido es utilizado para enviar datos de chips. 3 = Los datos de chips fueron perdidos debido a un formato no válido para el tipo de tarjeta con chip. 4 = La transacción está basada en token. Se utiliza este código en función de la presencia de un token emitido por VisaNet.
29	Merchant Verification Value [MVV] DE-62.20	231	240	ANS	10	Contiene el valor de verificación del comercio (MVV) utilizado para identificar a los comercios que participan en una variedad de programas. El MVV es único para el comercio. Visa asigna las primeras seis posiciones y asiste al adquirente en asignar los últimos cuatro.

TOKEN TM: FACT ADITIONAL DATA – MASTERCARD

#	NOMBRE	INICIO	FI N	FORMATO	LONG	VALORES VÁLIDOS
H-1	EYE-CATCHER	1	1	X(01)	1	Header de Token: Identificador de inicio de token. ! valor fijo
H-2	USER-FLD1	2	2	X(01)	1	Header de Token: Separador 1. " " valor fijo
H-3	Identificador del Token	3	4	X(02)	2	Header de Token: Identificación del token que se está enviando. TM valor fijo
H-4	Longitud de datos	5	9	9(05)	5	Header de Token: Longitud de la sección de datos del token. 00230 valor fijo
H-5	USER-FLD2	10	10	X(01)	1	Header de Token: Separador 2. " " valor fijo
1	Transaction Category Code DE-48	11	11	ANS	1	T
2	Payment Initiation Channel DE-48 SE 23	12	13	AN	2	Value indicating the type of device for which the consumer is requesting tokenization of a primary account number. 00 = Card 01 = Mobile Network Operator (MNO) controlled removable secure element (SIM or UICC) personalized for use with a mobile phone or smartphone 02 = Key Fob 03 = Watch using a contactless chip or a fixed (non-removable) secure element not controlled by the MNO 04 = Mobile Tag 05 = Wristband 06 = Mobile Phone Case or Sleeve 07 = Mobile phone or smartphone with a fixed (non-removable) secure element controlled by the MNO, for example, code division multiple access (CDMA) 08 = Removable secure element not controlled by the MNO, for example, memory card personalized for used with a mobile phone or smartphone 09 = Mobile Phone or smartphone with a fixed (non-removable) secure element not controlled by the MNO 10 = MNO controlled removable secure element (SIM or UICC) personalized for use with a tablet or ebook 11 = Tablet or e-book with a fixed (non-removable) secure element controlled by the MNO 12 = Removable secure element not controlled by the MNO, for example, memory card personalized for use with a tablet or e-book 13 = Tablet or e-book with fixed (non-removable) secure element not controlled by the MNO 14 = Mobile phone or smartphone with a payment application running in a host processor 15 = Tablet or e-book with a payment application running in a host processor 16 = Mobile phone or smartphone with a payment application running in the Trusted Execution Environment (TEE) of a host processor 17 = Tablet or e-book with a payment application running in the TEE of a host processor 18 = Watch with a payment application running in the TEE of a host processor 19 = Watch with a payment application running in a host processor 20 = Card 21 = Phone - Mobile phone 22 = Tablet/e-reader - Tablet computer or e-reader

						23 = Watch/Wristband - Watch or wristband, including a fitness band, smart strap, disposable band, watch add-on, and security/ID band 24 = Sticker 25 = PC - PC or laptop 26 = Device Peripheral - Mobile phone case or sleeve 27 = Tag - Key fob or mobile tag 28 = Jewelry - Ring, bracelet, necklace, and cuff links 29 = Fashion Accessory - Handbag, bag charm, and glasses 30 = Garment - Dress 31 = Domestic Appliance - Refrigerator, washing machine 32 = Vehicle - Vehicle, including vehicle attached devices 33 = Media/Gaming Device - Media or gaming device, including a set top box, media player, and television 34–99 = Reserved for future form factors. Any value in this range may occur
3	wallet ID DE-48 SE 26	14	16		3	103 = Apple Pay 216 = Android Pay 217 = Samsung Pay 327 = Merchant tokenization program
4	**Token Transaction ID** **DE-48 SE 30**	17	18	Numerico	2	44 = A 44 byte base 64 value will be sent for Mastercard BIN ranges. 64 = A 64 byte value will be sent for Visa BIN ranges
	PAN Mapping File Information DE-48 SE 33					
5	**Account Number Indicator** **DE-48 SE 33 SF 1**	19	19	an	1	C = (MasterCard Digital Enablement Service Token) or H= (MasterCard Digital Enablement Service Cloud-Based Payments Token Account) or F = (Mastercard Digital Enablement Service Card on File Token) M = Primary Account Number
6	Account Number DE-48 SE 33 SF 2	20	38	an	19	The token rather than the primary account number, if Account Number Indicator value is C, H, or F.
7	**Token Expiration Date** **DE-48 SE 33 SF 3**	39	42	Numerico	4	May contain virtual card number or token expiration date only if acquirer provided in P-35 of the authorization message ISO 8583. For contactless transit transactions, Token Expiration Date is the expiration date of the embossed number rather than the virtual number, if Account Number Indicator value is E. format YYMM

8	**Token Assurance Level** **DE-48 SE 33 SF 5**	43	44	Numerico	2	Contains a value indicating the confidence level of the token to PAN/cardholder relationship
9	**Token Requestor ID** **DE-48 SE 33 SF 6**	45	55	Numerico	11	Contains the ID assigned by the Token Service Provider to the Token Requestor. The Token Requestor ID is required for Card-on-File Token Request messages and is optional for all others.
10	**Storage Technology** **DE-48 SE 33 SF 8**	56	66	Numerico	11	Describes the Storage Technology of a requested or created token. 01 = Device Memory 02 = Device Memory protected by Trusted Platform Module (TPM) 03 = Server 04 = Trusted Execution Environment (TEE) 05 = Secure Element (SE) 06 = Virtual Execution Environment (VEE)
11	Cryptogram Validation Indicator Global 581 DE-48 SE 33 SF 9	67	67	AN	1	M - Token Requestor Cryptogram validation applied. N - Cryptogram validation not applied.
	ATC Information DE-48 SE 34					
12	**ATC Value** **DE-48 SE 34 SF 1**	68	72	Numerico	5	Contains the derived full ATC Value used in the validation
13	**Discrepancy Value** **DE-48 SE 34 SF 2**	73	77	Numerico	5	Is the differential between the transaction ATC and the maximum value allowed by the issuer when the transaction ATC is above the previous ATC, or the differential between the transaction ATC and the minimum value allowed by the issuer when the transaction ATC is below the previous ATC. ATC Discrepancy Value will be zero when the transaction ATC is within the issuer-defined limits.
14	**ATC inside issuer definitions** **DE-48 SE 34 SF 3**	78	78	an	1	Indicates if the ATC Discrepancy Value is above, below or within the maximum values allowed by the issuer. G = Indicates that the ATC value is greater than the maximum value allowed L = Indicates that the ATC value is lower than the minimum value allowed W = Indicates that the ATC value is within the issuer-defined limits
	Electronic Commerce Indicators DE-48 SE 42					
15	Security Protocol DE-48 SE 42 SF 1	79	79	Numérico	1	The electronic commerce security level indicators: 0 = Reserved for existing Mastercard Europe/Visa definitions 1 = Reserved for future use 2 = Channel 3–8 = Reserved for future use 9 = None (no security protocol)
16	Cardholder Authentication DE-48 SE 42 SF 2	80	80	Numérico	1	The cardholder authentication indicator: 0 = Reserved for future use 1 = eCommerce / SecureCode 2 = Processed through Masterpass 3 = Reserved for future use 4 = Digital Secure Remote Payment (DSRP) with UCAF data 5–9 = Reserved for future use

17	UCAF Collection Indicator DE-48 SE 42 SF 3	81	81	Numérico	1	The UCAF collection indicator: 0 = UCAF data collection is not supported by the merchant or a SecureCode merchant has chosen not to undertake SecureCode on this transaction 1 = UCAF data collection is supported by the merchant, and UCAF data must be present (DE 48, subelement 43 must be present and contain an attempt AAV for Mastercard SecureCode) 2 = UCAF data collection is supported by the merchant, and UCAF data must be present (DE 48, subelement 43 must contain a fully authenticated AAV) 3 = UCAF data collection is supported by the merchant, and UCAF (Mastercard assigned Static Accountholder Authentication Value) data must be present. 4 = Reserved for future use 5 = Issuer Risk Based Decisioning 6 = Merchant Risk Based Decisioning 7 = Partial shipment or recurring payment (DE 48, subelement 43 not required "Universal Cardholder Authentication Field [UCAF]"). Liability will depend on the original UCAF values provided and matching with the initial transaction. 8–9 = Reserved for future use
	Universal Cardholder Authentication Field [UCAF] Global 581 DE-48 SE 43					
18	Electronic Commerce Security Level Indicator and UCAF Collection Indicator DE-48 SE 43 SF 1	82	82	an	1	will be used to support the new Card on File Token Requestor Cryptogram.
	Time Validation Information –For SS Pay Only Global 580 DE-48 SE 49					
19	Time Value DE-48 SE 49 SF 1	83	90	Numerico	8	Contains the time data derived from the acquirer transaction to be used in the time validation Right-justified, leading zeros
20	Time Discrepancy DE-48 SE 49 SF 2	91	95	Numerico	5	Contains a positive value representing the differential in minutes between the transaction time data and servicecalculated time. Right-justified, leading zeros
21	Time Discrepancy Indicator DE-48 SE 49 SF 3	96	97	Numerico	2	Contains a value that indicates if the time discrepancy value is below, above, or within the minimum and maximum values for the time validation window or that indicates time validation was not performed. 01 = Positive value within time validation window 02 = Positive value outside time validation window 03 = Negative value within time validation window 04 = Negative value outside time validation window 05 = Unknown (time validation not performed)
	Merchant On-behalf Services DE-48 SE 51					
22	Merchant On-behalf (OB) Service Global 581 DE-48 SE 51 SF 1	98	99	AN	2	54 = MDES Card on File Token Requestor Cryptogram Validation Service 53 = Mastercard Digital Enablement Service Card on File PAN Mapping

23	Merchant On-behalf (OB) Result 1 Global 581 New Values DE-48 SE 51 SF 2	100	100	AN	1	Values in DE-48 SE 51 SF1 = 54 MDES Card on File Token Requestor Cryptogram Validation Service, then; A = ATC outside allowed range. E = ATC replay. F = Format Error—Card on File Token Requestor Cryptogram DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) must be present and properly formatted (base 64 encoded, correct length). I = Invalid—Card on File Token Requestor Cryptogram DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) must be valid. K = Card on File Token Requestor Cryptogram key record not found for the Token Requestor. U = Unable to process. V = Valid. Values in DE-48 SE 51 SF 1 = 53 Mastercard Digital Enablement Service Card on File PAN Mapping, then; C = Conversion of token to PAN completed successfully. F = Format error; Incorrect POS Entry Mode (not equal to 81 or 82) applicable to Authorization Request/0100, Authorization Advice/0120 Acquirer-generated, and Reversal Request/0400 messages. F = Format error; Token Requestor ID required (based on Token Requestor ID validation bypass parameter), not present (DE 48, subelement 33 not present), or not formatted correctly (DE 48, subelement 33 not formatted correctly). I = Invalid; Token suspended or deactivated. I = Invalid; Token not found on mapping table. T = Invalid; Token Requestor ID/Token combination invalid. U = Unable to process—Mapping Table unreachable/ unavailable. U = Unable to process—Token expired.
	On-behalf Services (First Occurrence –MDES OBS Mapping) DE-48 SE 71					
24	On-behalf [OB] Service DE-48 SE 71 SF 1	101	102	AN	2	50 = Mastercard Digital Enablement Service PAN Mapping 51 = Mastercard Digital Enablement Service Chip Pre-Validation 61 = Mastercard Digital Enablement Service Cloudbased Payments Chip Pre-Validation Service

25	On-behalf Result 1 DE-48 SE 71 SF 2	103	103	AN	1	Values in DE-48 SE 71 SF 1 = 50 Mastercard Digital Enablement Service PAN Mapping; C = Conversion of Token to PAN completed successfully F = Format Error I = Invalid Token U = Unable to process Values in DE-48 SE 71 SF 1 = 51 Mastercard Digital Enablement Service Chip Pre-Validation; A = ATC outside allowed range (applicable when ATC value is dynamic [varying] value) E = ATC Replay F = Format Error G = Application Cryptogram is valid but not an ARQC nor a TC, status of TVR/CVR unknown I = Invalid Cryptogram K = No matching key file for this PAN, PAN expiry date and KDI combination T = Valid ARQC/TC and ATC; TVR/CVR invalid U = Unable to process V = Valid ARQC/TC and ATC and TVR/CVR Values in DE-48 SE 71 SF 1 = 61 Mastercard Digital Enablement Service Cloudbased Payments Chip Pre-Validation Service; D = ATC Invalid—Not in list of currently active Single-Use Keys E = ATC Replay F = Format Error I = Invalid MD AC and UMD AC K = No matching key file for this PAN, PAN expiry date and KDI combination L = Invalid MD AC; Valid UMD AC M = Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit Reached, Token Suspended) P = Valid MD AC; Invalid UMD AC (Invalid Mobile PIN) T = Invalid TVR/CVR U = Unable to process V = Valid
26	On-behalf Result 2 DE-48 SE 71 SF 3	104	104	ANS	1	Mastercard use only. May contain a space or a value.
27	Address Verification Service Request DE-48 SE 82	105	106	Numerico	2	52 = AVS and Authorization Request/0100
28	The AVS response code DE-48 SE 83	107	107	A	1	A = Address matches, postal code does not. B = Visa only. Street address match. Postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.) C = Visa only. Street address and postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.) D = Visa only. Street address and postal code match. F = Visa only. Street address and postal code match. Applies to U.K. only. G = Visa only. Non-AVS participant outside the U.S.; address not verified for international transaction. I = Visa only. Address information not verified for international transaction. M = Visa only. Street addresses and postal code match. N = Neither address nor postal code matches. P = Visa only. Postal codes match. Street address not verified because of incompatible formats. (Acquirer sent both street address and postal code.) R = Retry, system unable to process. S = AVS currently not supported. U = No data from issuer/Authorization Platform W = For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not. X = For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match. Y = For U.S. addresses, five-digit postal code and address matches. Z = For U.S. addresses, five-digit postal code matches, address does not.

29	The CVC 2 result code DE-48 SE 87	108	108	A	1	CVC 1 Y = Invalid CVC 1 (only if DE 35 (Track 2 Data) or DE 45 (Track 1 Data) is present in the Authorization Request/0100 message.) CVC 2 M = Valid CVC 2 (match) N = Invalid CVC 2 (non-match) P = CVC 2 not processed (issuer temporarily unavailable) U = CVC 2 Unverified—Mastercard Use Only CVC 3 E = Length of unpredictable number was not a valid length P = Unable to process Y = Invalid
30	CVC 2 DE-48 SE 92	109	111	Numerico	3	CVC 2 value from the signature panel of the card when applicable Must be the same value as the original Authorization Request/0100
31	Advice Reason Code DE-60 SF 1	112	114	Numerico	3	value 141 (Mastercard Digital Enablement Service Advice to Issuer)
32	Advice Detail Code DE-60 SF 2	115	118	Numerico	4	Values in Mastercard Digital Enablement Service 0201 = Reject: Invalid Token—Primary Account Number mapping relationship 0202 = Reject: Token in suspended status 0203 = Reject: Token deactivated 0204 = Reject: ATC Invalid—Not in List of Currently Active Single Use Keys 0205 = Reject: ATC Replay 0206 = Reject: Invalid MD AC and UMD AC (Invalid Mobile PIN) 0207 = Reject: Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit not Reached, Token not Suspended) 0208 = Reject: Invalid MD AC; Valid UMD AC 0209 = Reject: Valid MD AC; Invalid UMD AC (Mobile PIN Try Counter Max Limit Reached, Token Suspended) 0210 = Reject: Unpredictable Number Length Indicator Mismatch 0211 = Reject: TVR/CVR validation failed 0212 = Reject: Unable to Process 0213 = Reject: Invalid Token 0215 = Reject: Declined by Transaction Analysis 0032 = Reject: Chip Data Processing Error 0034 = Reject: Chip validation failed 0035 = Reject: TVR/CVR validation failed 0039 = Reject: Cryptogram not ARQC 0042 = Reject: CVC 3 Unable to process 0043 = Reject: CVC 3 ATC outside allowed range 0044 = Reject: CVC 3 Invalid 0045 = Reject: CVC 3 Unpredictable number mismatch 0046 = Reject: CVC 3 ATC Replay 0250 = Activation Code Notification 0251 = Tokenization Complete Notification 0252 = Tokenization Event Notification
33	Advice Detail Text SF3	119	171	ans	53	Advice message text
	Point of Service (POS) Data DE-61					
34	POS Transaction Status DE-61 SF 7	172	172	Numérico	1	8 = Account Status Inquiry Service (ASI) 9 = Tokenization Request/Notification
35	Receiving Institution ID Code DE-100	173	183	Numérico	11	Administrative Advice/0620. Must contain a valid five-digit Mastercard customer ID number. It identifies the destination CPS or INF to receive the message.

36	AVS Service Indicator 1 DE-120 SF 1	184	212	ANS	29	Positions 1–9: Postal Code Postal Code Cardholder postal/ZIP code Positions 10–29 Address (Mastercard) Address Cardholder address
	Card On File (Datos Adicionales)					
37	PAN SEQ Number DE-23	213	215	Numérico	3	DE 23 (Card Sequence Number) distinguishes among separate cards having the same DE 2 or DE 34. Acquirers with chip-reading capability may pass this information encoded on the chip in DE 23 of Authorization Request messages.
38	FILLER	216	240	ANS	25	USO FUTURO