(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 236**

(51) Int. CI.:

G06Q 40/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.06.2004 E 04776493 (1)**

(97) Fecha y número de publicación de la concesión europea: **13.04.2016 EP 1636680**

(54) Título: **Sistemas y métodos que permiten efectuar transacciones de pago seguras utilizando una estructura de datos con formato**

(30) Prioridad:

10.06.2003 US 477187 P
04.06.2004 WO PCT/US2004/017756

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.09.2016

(73) Titular/es:

MASTERCARD INTERNATIONAL, INC. (100.0%)
2000 Purchase Street
Purchase, NY 10577, US

(72) Inventor/es:

KRANZLEY, ARTHUR, D.;
ORFEI, STEPHEN, W.;
RUTHERFORD, BRUCE, J. y
WIESMAN, MARK

(74) Agente/Representante:

LÓPEZ CAMBA, María Emilia

DESCRIPCIÓN

Sistemas y métodos que permiten efectuar transacciones de pago seguras utilizando una estructura de datos con formato

ANTECEDENTES DE LA INVENCIÓN

La presente invención se refiere a los sistemas y métodos para la autenticación de las operaciones realizadas por los participantes sobre las redes electrónicas abiertas tales como Internet. En particular, la invención se refiere a la autenticación de las transacciones en Internet en las que los clientes cargan pagos a las tarjetas de pago, incluyendo las tarjetas de crédito.

El comercio electrónico E-commerce es ahora popular. Realizar transacciones en redes electrónicas tales como Internet tiene las reiteradas actualmente ventajas de comodidad, los costes reducidos, el alcance al mercado y la elección, para comerciantes y clientes. Sin embargo, el anonimato de Internet lleva a una venta al por menor o comercial los problemas de fraude y de uso indebido. Un comerciante que está realizando una transacción tiene un deseo de autenticar la venta, certificar la venta, confirmar la venta, garantizar el no rechazo de la venta, asegurar el pago y controlar el anonimato. Asimismo, un comprador tiene un deseo de control de autenticación de la venta, la integridad de la venta, el recurso de una mala venta, la confirmación de la venta, la privacidad y el anonimato.

El documento de solicitud de patente compartida U.S. Patent Application no. 10/096,271 presentado el 11 de marzo de 2002, el cual está incluido en su totalidad en el presente documento como referencia, describe un sistema y método para la realización de las transacciones de pago seguro utilizando software de usuario en un terminal de cliente con el fin de recibir un conjunto de datos de la página Web que será utilizada para la visualización de una página Web, la cual puede incluir uno o varios campos ocultos. La página Web con los datos del usuario de la tarjeta y la transacción es enviada al comerciante como los datos de compra. El comerciante puede enviar los datos de esta página web electrónicamente, por ejemplo, a un emisor, para la autenticación o autorización de la operación de pago.

Los emisores de tarjetas y otras instituciones financieras ofrecen ahora o utilizan protocolos de transacción en Internet estandarizados con el fin de mejorar el rendimiento de las transacciones en línea y acelerar el crecimiento del comercio electrónico. En algunos protocolos estandarizados (por ejemplo, el Protocolo 3-D Secure™ desarrollado por Visa International) los emisores de tarjetas o los bancos emisores pueden autentificar las transacciones reduciendo la probabilidad de fraude y los rechazos de débito asociados a las transacciones no autorizadas atribuidas al titular de la tarjeta. La presencia de una transacción autenticada puede dar como resultado que un emisor asuma la responsabilidad por fraude a pesar de los esfuerzos para autenticar al titular de la tarjeta durante una compra en línea. Los emisores de tarjetas o los bancos emisores pueden asegurar a los comerciantes que serán pagados por las transacciones autenticadas por el emisor. El protocolo 3-D Secure™ es coherente con ello y suscribe los programas de autenticación ofrecidos por los emisores de tarjetas (por ejemplo, Verified by Visa o MasterCard SecureCode™) con el fin de autentificar los clientes para los comerciantes durante las transacciones remotas tales como aquellas asociadas con la Internet. El protocolo 3-D Secure™ aprovecha la funcionalidad de encriptado existente de Secure Sockets layer (SSL) y proporciona una seguridad mejorada a través de la autenticación del titular por el emisor durante la sesión de compra en línea. Una pieza de software llamada MerchantPlug In (MPI) es utilizada por los comerciantes participantes con el fin de intercambiar mensajes, pasar información y consultar a los participantes con el fin de establecer una sesión de autenticación entre titular de la tarjeta y su emisor de su tarjeta de durante una compra en línea.

Los servicios de protocolo 3-D Secure se basan en un modelo de tres dominios -el dominio emisor, la entidad adquiriente y el dominio de interoperabilidad. El emisor es responsable de gestionar la inscripción de los titulares de la tarjeta en el servicio y de la autenticación de los titulares de tarjetas durante las transacciones en línea. La entidad adquiriente es responsable por aceptar la definición de los procedimientos de tal manera que los comerciantes que participan en las transacciones de Internet funcionan bajo un acuerdo con la entidad adquiriente y de proveer el proceso de respaldo posterior para las transacciones autenticadas. El dominio de interoperabilidad facilita el intercambio de transacciones entre los otros dos dominios con un protocolo común y los servicios compartidos. Los titulares de tarjetas y sus bancos pueden aparecer bajo el "dominio del emisor", los comerciantes y sus bancos pueden aparecer bajo el "dominio de la entidad adquiriente". La comunicación entre los bancos emisores o entidad adquiriente o instituciones financieras y la infraestructura del emisor de tarjeta puede aparecer bajo el "Dominio de Interoperabilidad". Mientras se está realizando la transacción los bancos y comerciantes conformes con 3-D Secure, un consumidor puede tener la misma experiencia de compra en Internet como anteriormente, excepto que existe una ventana de autenticación separada o una pantalla emergente desde el banco del titular con el fin de determinar si el participante en la transacción es de hecho el titular de la tarjeta registrada. El flujo de transacción para una transacción de compra en línea en Internet bajo el protocolo puede ser como sigue:

(1) Los clientes rellenan los datos de pago en sitios web de Comerciante en la manera usual, a través de una conexión encriptada Secure Sockets Layer (SSL).

(2) Entonces, el Comerciante envía un mensaje a través de un MPI a un Directorio, que a su vez consulta al emisor de la tarjeta, con el fin buscar si el cliente está inscrito en el programa 3-D Secure.

(3) El emisor de la tarjeta responde al Directorio con un mensaje que indica si el titular de la tarjeta está inscrito y, si es así, proporciona una dirección Web para el Banco que emitió la tarjeta. Este mensaje es entonces procesado y la respuesta enviada al Comerciante.

(4) Entonces, el comerciante envía un mensaje al banco emisor, a través del dispositivo del titular de la tarjeta, con el fin de iniciar y autenticar la sesión entre el titular de la tarjeta y el emisor de la tarjeta en la cual pueden ser presentados los detalles de la transacción tales como el nombre de Comerciante y el importe de la transacción al titular de la tarjeta para la confirmación.

(5) Entonces, el banco emisor mostrará una ventana de autenticación para el titular de la tarjeta que detalla la información relacionada con la transacción tales como el nombre del comerciante e importe, un mensaje de seguridad personal y una zona de respuesta en donde puede ser introducidos por el titular los detalles para la autenticación.

(6) El cliente aprueba la transacción en una de una variedad de maneras, dependiendo de cómo el banco emisor elije como implementar el sistema. Las opciones pueden variar de entrar desde introducir una contraseña estática o número de identificación personal, PIN, con el fin de utilizar una tarjeta inteligente y un Lector de Tarjeta Personal (PCR) para generar una señal de autenticación.

(7) El emisor puede procesar los datos de la transacción y del titular de la tarjeta para la autenticación. Si la autenticación es válida, el emisor envía un mensaje al comerciante indicando que la autenticación ha tenido éxito. El emisor también notifica al comerciante si la autenticación falló o no pudo ser completada. El mensaje puede incluir un Valor de Autorización del Titular de Cuenta (Accountholder Authorization Value) (AAV) codificando los resultados del proceso de autenticación.

En la actualidad deben considerarse las formas de mejorar los sistemas y los métodos para la autenticación de los clientes, que usan tarjetas de crédito o de débito para el pago en las transacciones electrónicas. La atención está dirigida a los datos y a los algoritmos que son utilizados para autenticar con seguridad el cliente o la tarjeta de pago al comerciante. Las soluciones deben ser de manera preferible compatibles con las implementaciones de la industria de los protocolos comunes similares a 3-D Secure y a otros estándares de la industria tales como el estándar EMV para las tarjetas inteligentes.

RESUMEN DE LA INVENCIÓN

De acuerdo con la presente invención y, tal y como está lo definido en las reivindicaciones adjuntas, son proporcionados los programas de autenticación que están conformes con los protocolos 3-D Secure para autenticar las transacciones en línea del titular de la tarjeta. Los programas de autenticación utilizan un servidor de control de acceso (ACS) con el fin de autenticar las transacciones del titular de la tarjeta. Son aplicados los algoritmos de pago Seguro (Secure Payment Algorithms) (SPA) mediante el ACS al titular de la tarjeta y a la información de la transacción con el fin de generar un Accountholder Authentication Value encriptado (AAV), que es asignado a una transacción autenticada. El AAV generado tiene una estructura de datos que es conveniente para su inclusión en los mensajes de protocolo 3-D Secure.

En las realizaciones preferidas de la invención, la estructura de datos tiene una longitud de no más de 20 bytes de caracteres codificados en Base 64. El primer byte puede ser un byte de control, los bytes 2-9 pueden representar un resumen criptográfico de un nombre comercial y el byte 10 identifica el ACS particular que autenticó la transacción del titular de la tarjeta. Pueden ser utilizados varios métodos de autenticación (por ejemplo, basado en contraseña, basado en chip y en los métodos de identificación de PC) por el ACS para autenticar la transacción del titular de la tarjeta. El byte 11 de la estructura de datos AAV identifica el método de autenticación y las claves de encriptación secretas que son utilizadas por el ACS con el fin de generar un código de autenticación de Comerciante (MAC). Los bytes 12-15 de la estructura de datos AAV identifican un número de secuencia de las transacciones procesadas por el ACS y los bytes 16-20 representan el MAC.

Los SPA pueden incluir procesos de encriptación adecuados para generar valores de MAC para una transacción particular. Un proceso de encriptación utiliza una clave secreta para encriptar una concatenación del número de cuenta del titular de la tarjeta y los campos 1-6 (o bytes 1-15) del AAV. Los primeros 40 bits (o bytes binarios 5) del resultado de la encriptación son asignados al campo MAC. En otro proceso de encriptación, es utilizado un par de claves de Encriptación de Datos Estándar (DES) con el fin de encriptar una concatenación del número de cuenta del titular de la tarjeta, fecha de expiración (vencimiento) de la tarjeta y código de servicio con el fin de generar un número de tres dígitos Código de Verificación del Titular de la Tarjeta (CVC2). Este número de tres dígitos es convertido en un decimal codificado binario, que luego se utiliza para llenar uno y una mitad bytes del campo de MAC en la estructura de datos AAV. Los restantes tres y una mitad bytes del campo MAC puede ser rellenados o llenados con ceros binarios.

Los mensajes electrónicos de protocolo 3-D Secure, que incluyen los datos del AAV, pueden ser firmados digitalmente por el Servidor de Control de Acceso (ACS). El comerciante que recibe un mensaje que contiene los datos del AAV puede ser requerido para validar la firma digital de conformidad con el protocolo 3-D Secure antes de extraer o utilizar los datos de AAV. Los Comerciantes pueden transferir los datos del AAV y en particular los datos de MAC a los mensajes de solicitud de autorización de pago.

Otras características de la invención, su naturaleza y varias ventajas serán más aparentes de la descripción detallada siguiente y de los dibujos que la acompañan

DESCRIPCIÓN BREVE DE LOS DIBUJOS

La Figura 1 es una ilustración esquemática de un ejemplo de programa de autenticación utilizando los Algoritmos de Pago Seguro (SPA) para generar los Valores de Autenticación del Titular de la Cuenta (AAV) para las transacciones de pago, de acuerdo con los principios de la presente invención.

La Figura 2 es una ilustración esquemática de la estructura de un Campo de Cuenta del Titular de la Tarjeta Universal (Universal Cardholder Account Field) que es utilizado para transportar la salida de los Algoritmos de Pago Seguro (SPA) de la Figura 1, de acuerdo con los principios de la presente invención.

La Figura 3 es una ilustración de algunos de los pasos y de los enlaces de los mensajes entre las entidades que participan en un ejemplo de proceso de autenticación de transacciones de pago, de acuerdo con los principios de la presente invención.

La Figura 4 es una ilustración esquemática de la interacción entre las entidades del ejemplo de autenticación y autorización y autorización involucradas en la autenticación y autorización de las transacciones de pago en línea.

A lo largo de las figuras, a menos que se indique lo contrario, son usados los mismos numerales de referencia y los caracteres con el fin de denotar similares características, elementos, componentes o partes de las realizaciones ilustradas.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La presente invención proporciona las soluciones para la autenticación de las partes remotas en una transacción electrónica. En particular, las soluciones se relacionan con las Aplicaciones de Pago Seguro (por ejemplo, SPA 135 en la figura 1) que son utilizadas para autenticar un titular de tarjeta que participa de manera remota en la transacción electrónica. Las soluciones pueden ser utilizadas para la autenticación de las transacciones en las plataformas de comercio electrónico estándar de la industria, tales como las plataformas de comercio electrónico (e-commerce) compatibles con 3-D Secure y en entornos de no comercio electrónico tales como los pedidos por correo electrónico y teléfono o en dispositivos móviles donde puede ser utilizado una señal o código de autenticación por el emisor con el fin de autenticar al titular de la tarjeta.

La TABLA 1 es un glosario de algunos de los términos, siglas (acrónimos) o abreviaturas que son utilizadas en la descripción en el presente documento

TABLA 1

AAV	Valor de Autenticación del Titular de la Cuenta
Servidor de Control de Acceso (ACS)	Servicios del Servidor de Control de Acceso con el fin de validar el registro de un número de cuenta (PAN) de un titular de tarjeta específico en 3-D Secure así como las transacciones autenticadas
Valor de Autenticación del Titular de Cuenta (AAV)	Datos del titular de la tarjeta para autenticación requeridos para las transacciones de comercio electrónicos en los que la autenticación del titular de la tarjeta ha sido realizada con éxito
Valor de Verificación de la Autenticación del Titular de la Tarjeta (CAVA)	Datos del titular de la tarjeta para autenticación requeridos por VISA para las transacciones de comercio electrónicos en los que la autenticación del titular de la tarjeta ha sido realizada con éxito
Código de Verificación de la Tarjeta (CPC)	Una característica de seguridad de la tarjeta de dos partes. El CVC 1 es un valor de 3 dígitos codificado en las pistas 1 y 2 en tres posiciones contiguas en el campo "datos discrecionales" de una banda magnética en una tarjeta. El CVC 2 se diferencia del CVC 1 y es una impresión en el margen dentro del panel de firma evidente de forzar en la tarjeta. El CVC pretende inhibir la alteración o mal uso de los datos de la tarjeta y mejora la autentificación de la tarjeta.
Código de Autenticación de Mensaje (MAC)	Código generado criptográficamente que es una función de los contenidos del mensaje y una clave secreta compartida por el autor del mensaje y el destinatario del mensaje. Este valor, generador por el autor y verificado por el destinatario, permite que el destinatario pueda detectar cualquier alteración al mensaje original.

Aplicación de Pago Seguro (SPA)	Especificaciones y algoritmo para la generación de los datos de autenticación del titular de la tarjeta de los componentes de datos del comerciante y del emisor que dan por Resultado la creación de un AA V.
Campo de Autenticación del Titular de Tarjeta Universal	La infraestructura de transporte de datos multi propósito universal y campo definido que es utilizado para comunicar y transporta la información de autenticación, incluyendo el AAV, entre los diversas partes interesadas en una transacción

La SPA 135 puede incluir algoritmos de criptografía (algoritmos denominados, "HMAC" y "CVC2") que son usados con el fin de generar los Valores de Verificación de la Autorización del Titular de la Tarjeta (CAW) en los formatos que son compatibles con los formatos de mensajes 3-D Secure.

La SPA 135 puede ser integrada con cualquier programa de autenticación adecuado que los emisores de tarjetas pueden elegir o implementar para la autenticación de sus titulares de tarjetas. Los programas de autenticación pueden incluir soluciones basadas en tarjetas inteligentes y basadas en contraseña (por ejemplo en la Figura 1, el programa de autenticación basado en el chip 141 y el programa de autenticación 142 3-D Secure basado en contraseña). Los programas de autenticación también pueden incluir otras soluciones basadas, por ejemplo, en la identificación de PC.

Un programa de autenticación en el cual son utilizadas las aplicaciones inventadas de Pago Seguro (SPA 135) puede ser una solución o programa para asegurar las transacciones electrónicas realizadas en las plataformas de comercio electrónico que son compatibles con los protocolos 3-D Secure. Para este propósito la SPA 135 está diseñada para utilizar y generar los resultados de autenticación en los formatos de datos que pueden ser usados para ser leídos electrónicamente en los mensajes 3-D Secure. En particular, puede ser utilizada una estructura de datos con formato con campos definidos y longitud de byte con el fin de facilitar el transporte de los resultados de autenticación en los mensajes 3-D Secure.

Con los propósitos de ilustrar la aplicación de la SPA 135 en un ejemplo de programa de autenticación 1000 (FIG. 1), es utilizada en este documento una transacción de pago con tarjeta como un ejemplo de operación. Los participantes en la transacción de pago con tarjeta incluyen un titular de la tarjeta, un emisor, un comerciante y una entidad adquiriente.

Un titular de la tarjeta es un usuario autorizado de una tarjeta de pago emitida, por ejemplo, por un miembro con licencia del programa de autenticación 1000. El titular de la tarjeta puede utilizar la tarjeta de pago emitida para pagar por una transacción en línea con un comerciante. El programa de autenticación 1000 puede ser parte de un programa de autenticación o de servicios proporcionado por una tercera parte (por ejemplo, MasterCard) que, por ejemplo, puede asegurar que la identidad del titular de la tarjeta y la presencia está correctamente autenticada antes de la terminación de la transacción.

Un emisor es un miembro (por ejemplo, una entidad financiera) que emite la tarjeta de pago, que puede ser de marca (por ejemplo, las tarjetas MasterCard® o Maestro®). El emisor garantiza el pago de una transacción autorizada utilizando la tarjeta de pago de acuerdo con las regulaciones de pago de la marca de la tarjeta y con la legislación local. El emisor puede ser responsable de determinar la elegibilidad del titular de la tarjeta para participar en el programa de autenticación 1000, además de proporcionar los servicios de autenticación a los comerciantes o a otras partes.

Un comerciante es un vendedor al por menor o cualquier otra persona, firma o corporación que, por ejemplo, en virtud de un acuerdo de suscripción de comerciante, está de acuerdo en aceptar tarjetas de pago de emisores para el pago cuando estas se presentan correctamente. Mediante la suscripción al programa de autenticación 1000, un comerciante puede ofrecer a un titular de tarjeta una interacción electrónica autenticada en Internet. Un comerciante que acepta tarjetas de pago puede tener una relación adicional con una entidad adquiriente. Los comerciantes que participan el programa de autenticación 1000 pueden beneficiarse de varias maneras incluyendo el fraude y los costes reducidos de conflictos, un volumen aumentado de transacciones, la protección contra el uso no autorizado de la tarjeta y el acceso a la base de tarjetas del emisor.

La entidad adquiriente es una entidad que mantiene relaciones con los comerciantes y adquiere los datos relativos a una transacción desde el comerciante o el aceptador de la tarjeta. La entidad adquiriente puede ser responsable de determinar la elegibilidad de comerciante para participar en el programa de autenticación 1000.

Tal y como se muestra en la figura 1, el programa ejemplo de autenticación 1000, puede ser implementado como una configuración o una plataforma de comercio electrónico seguro con una serie de capas componentes. Las capas componentes incluyen la capa de transporte de datos 100, la capa de requisitos de comerciante 120, la capa de autenticación 130 y la plataforma del emisor 140. La capa de autenticación 130 se refiere a las Aplicaciones de Pago Seguro (SPA 135) que son desplegadas para autenticar una transacción o pago.

La capa de transporte de datos 100 se refiere a la recopilación de datos y la infraestructura de transporte que es utilizada para comunicar la información de la autenticación y los resultados entre el titular de la tarjeta, el emisor, el comerciante y la entidad adquiriente. El transporte de datos puede estar basado, por ejemplo, en estructuras de datos estandarizados, arquitecturas o mecanismos tales como el Campo de Autenticación de Titular de Tarjeta Universal (UCAF).

El UCAF puede ser definido, en general, como un campo de 32 caracteres de una longitud variable, con un estructura de los datos flexible, la cual puede ser adaptada a medida con el fin de satisfacer las necesidades de una variedad de enfoques de seguridad y de autenticación del emisor. La figura 2 muestra una estructura genérica del UCAF. Un primer byte de control en el UCAF contiene un valor que es específico para cada aplicación de seguridad de pago o aspecto. El resto de los bytes en el UCAF puede incluir los datos específicos de la aplicación. Un proveedor de autenticación o autorización puede ser responsable de la asignación y de la gestión de los valores de byte de control del UCAF y la estructura de datos específicos de la aplicación del UCAF.

Un ejemplo de definición de byte de control puede ser como sigue:

Utilización del AAV de SPA 3-D Secure para la primera y subsecuentes transacciones
Valor j Codificado Base 64
Valor x´8C´Hexadecimal

Otro ejemplo de definición de byte de control puede ser como sigue:

Utilización del AAV de SPA 3-D Secure para intentos
Valor j Codificado Base 64
Valor x´86´Hexadecimal

En las implementaciones convencionales UCAF, la aplicación de los datos específicos puede ser definida como los datos binarios con una longitud máxima de 24 bytes binarios - incluyendo el byte de control. Sin embargo, algunas redes de autorización de transacción limitan el paso de datos binarios en los mensajes de autorización. De acuerdo con ello, todos los datos del UCAF generados por la SPA 135 en el programa de autenticación 1000 pueden ser codificados de Base 64 antes de la inclusión en un mensaje de autorización. La codificación en Base 64 produce una representación de caracteres de los datos binarios asociados. La representación de caracteres resultante es aproximadamente un tercio más larga que el equivalente binario. Por esta razón, el campo UCAF puede, en general, ser definido con una longitud máxima de 32 caracteres. Sin embargo, para la compatibilidad con la mensajería 3-D Secure en el programa de autenticación 1000, el campo UCAF está limitado a una longitud de 28 caracteres.

El Valor de Autenticación de Titular de Cuenta (AAV) es una implementación específica de UCAE relacionada con las plataformas de autenticación del emisor que incorporan el SPA. El AAV puede generado por el emisor y presentado al comerciante para la presentación de una solicitud de autorización de transacción (a la entidad adquiriente) una vez que se ha obtenido el resultado favorable en la autenticación del titular de la tarjeta por el emisor. En el caso de una devolución de cargo u otro proceso potencial de conflicto, el AAV puede ser utilizado con el fin de identificar los parámetros de proceso asociados con la transacción. El UCAF es el mecanismo que se utiliza para transmitir el AAV desde el comerciante al emisor para los propósitos de autenticación durante el proceso de autorización.

Con una referencia renovada a la FIG. 1, la capa de requisito de comerciante 110 se refiere a las posibilidades del comerciante para interactuar con las otras capas y el titular de la tarjeta. Los comerciantes participantes en el programa de autenticación 1000 pueden implementar capacidades de aplicaciones de software (por ejemplo, complementos (plug-ins) para el comerciante (MPI)) que son capaces de procesar los mensajes 3-D Secure. Un MPI puede servir como la aplicación de control para el procesamiento de los mensajes 3-D Secure.

La capa de autenticación 130, que incluye la SPA 135 inventada, representa el proceso de autenticación o los servicios (por ejemplo, proporcionados o contratados por un emisor) para verificar la propiedad de la cuenta del titular de la tarjeta. Un emisor que utiliza, por ejemplo, un servidor de control de acceso (ACS) puede implementar la capa de autenticación 130/SPA 135 junto con un servidor/proceso de validación AAV.

Los ejemplos de componentes de la red de comercio electrónico o las entidades que participan en el proceso de autenticación pueden, para los propósitos de ilustración, estar organizados como pertenecientes a los dominios emisor, entidad adquiriente o de interoperabilidad tal y como se muestra en la TABLA 2.

TABLA 2

Dominio del Emisor	Dominio de Interoperabilidad	Dominio de E. Adquiriente
Navegador del Titular de la Tarjeta Software relacionado Servidor de Inscripción Servidor de Control de Acceso Servidor/proceso de Validación de AAV	Servidor Directorio Autoridad de Certificación	Servidor Validación Plug-in Comerciante

Con referencia a la tabla 2, la funcionalidad presente en el dominio del emisor incluye un navegador del titular de la tarjeta que puede actuar como un conducto para el transporte de mensajes entre el MPI (en el dominio de la entidad adquiriente) y el servidor de control de acceso (en el dominio del emisor). El software relacionado con el titular de la tarjeta, puede incluir, por ejemplo, un software opcional para soportar el uso de tarjetas inteligentes. El servidor de inscripción facilita el proceso de inscripción del titular de la tarjeta para la implementación de un emisor de 3-D Secure bajo el programa de autenticación 1000. El servidor puede ser utilizado para realizar la autenticación inicial del titular de la tarjeta, así como para las actividades administrativas tales como los reajustes y la visualización de la historia de pago 3-D Secure.

El servidor de control de acceso proporciona por lo menos dos funciones básicas en el transcurso de una compra en línea. En primer lugar, el ACS verifica si un número dado de cuenta de titular de la tarjeta está inscrito en el programa 1000. En segundo lugar, el ACS conducirá los procesos de autenticación para la identificación del titular de la tarjeta. Con este propósito, el ACS puede funcionar en conjunción con o incluir un servidor/proceso de validación de AAV. Este proceso/servidor de validación de AAV también puede ser utilizado con el fin de validar los datos de autenticación del titular de la tarjeta recibidos de comerciantes o entidades adquirientes.

La funcionalidad de dominio de entidad adquiriente puede incluir las funciones de un Plug-in de Comerciante (MPI) y un servidor de validación de firma. El MPI puede crear y procesar mensajes de autenticación de pagador y luego devuelve el control al software del comerciante para el proceso adicional de autorización. Los procesos de autenticación de MPI pueden ser invocados después de que de un titular de la tarjeta solicite una petición de compra, incluyendo el número de cuenta que se utilizará para el pago, pero antes de obtener la autorización para la compra. El servidor de validación de firma puede ser usado para validar una firma digital en una solicitud de compra que ha sido autenticada con éxito por el emisor.

La funcionalidad en el ámbito de la interoperabilidad puede incluir un servidor de directorio. El servidor de directorio puede ser un directorio global, que proporciona capacidades de toma de decisión centralizada a los comerciantes inscritos en el programa de autenticación 1000. Basado en el número de la cuenta contenido en un mensaje de solicitud de verificación de comerciante, el directorio puede primero determinar si el número de cuenta es parte de un rango de tarjeta participante del emisor de tarjeta. Entonces puede dirigir solicitudes adecuadas al ACS apropiado del emisor para su posterior procesamiento. El dominio de interoperabilidad también puede incluir una autoridad adecuada de certificación para generar y distribuir toda la jerarquía privada de entidad final y los certificados subordinados, según sea requerido, a los diversos componentes y a otras autoridades de certificación subordinadas en todos los tres dominios.

El proceso de autenticación del Titular de la tarjeta en el programa 1000 consiste en intercambios de mensajes y datos a través de los tres dominios. Los siguientes ejemplos 3-D Secure de mensajes inter dominio pueden ser utilizados paso a paso en el proceso de autenticación:

(1) Solicitud de verificación /Respuesta

Mensaje par: VEReq/VERes

Un primer paso en el proceso de autenticación es comprobar o validar que el número de cuenta del titular de la tarjeta es parte del rango de tarjeta de un emisor que participa en el programa de autenticación 1000. Con este propósito, es enviado un mensaje de Solicitud de Verificación VEReq, desde el MPI al directorio con el fin de comprobar la elegibilidad del rango de la tarjeta. Si el número de la cuenta especificada está contenido dentro de un rango de tarjeta elegible en el directorio, entonces este mensaje puede ser enviado desde el directorio al ACS del emisor con el fin de comprobar adicionalmente comprobar si el número de cuenta especificado está inscrito y/o activado por el emisor como un participante en el programa 1000.

El MPI puede tener una capacidad opcional de almacenar temporalmente localmente rangos de tarjeta por cada emisor participante. En tales casos, los mensajes de SolicitudRangoTarjeta/Respuesta pueden ser utilizados por el MPI con el fin de solicitar actualizaciones para los almacenamientos temporales de rango de tarjeta desde el directorio. Para los comerciantes que almacenan temporalmente rangos de tarjeta, los mensajes de VEReq/VERes pueden no ser utilizados si el almacenamiento temporal indica que el emisor no está inscrito en el programa de autenticación 1000.

2) Solicitud Autenticación Pagador /Respuesta

Mensaje par: PAReq/PARes

Una vez que se ha determinado que el titular de la tarjeta está inscrito por un emisor o es un participante activo en programa 1000, el proceso de autenticación del titular de tarjeta específico implica además al emisor de la tarjeta específico. Los mensajes de Solicitud Autenticación de Pagador/ Respuesta pueden ser enviados desde el MPI al ACS del emisor de la tarjeta específica con el fin de realizar la autenticación. En esta etapa del proceso de autenticación en el programa 1000, el titular de la tarjeta puede ser presentado con una ventana de autenticación. La ventana de autenticación puede ser mostrada en el navegador del titular de la tarjeta y ser rellenada con información relevante por el emisor. Puede ser solicitado al titular de la tarjeta la introducción de una contraseña, un código o símbolo para la identificación personal o de autenticación a través de la ventana mostrada de autenticación. El ACS del emisor de la tarjeta específica puede entonces utilizar, por ejemplo, la SPA 135 con la finalidad de autenticar la información recogida o introducida y de acuerdo con ello generar un Valor Autenticación del Titular de la Cuenta (AAV). El AAV es transportado en el mensaje 3-D Secure PARes (Respuesta de Autenticación de Pagador) en un campo designado de Valor de Verificación de Autenticación de Titular de Tarjeta (CAVV) en un UCAF.

Un CAAV es uno de los campos de datos en la parte de respuesta de Mensaje par PAReq/PARes devuelto por el emisor al comerciante solicitante. El emisor puede colocar firmas digitales convenientes en su respuesta. Además, el comerciante puede incluir el AAV recibido a una entidad adquiriente para enviarlo al emisor como parte de una solicitud de autorización de pago/transacción (véase por ejemplo, la figura 4).

La figura 3 muestra esquemáticamente un ejemplo de proceso de autenticación de tarjeta 300 para una transacción de un titular de tarjeta bajo un programa de autenticación 1000. Para los propósitos de la ilustración, la descripción del proceso 300 asume que el titular de la tarjeta 310 está inscrito por un emisor en el programa de autenticación 1000 y ha obtenido una contraseña o código desde el emisor con el fin de utilizarlo mientras realiza compras en línea en los comerciantes participantes. El proceso 300 también asume que todos los canales de comunicación entre los componentes (por ejemplo, el titular de la tarjeta 310, el MPI 320, el directorio 330 y el ACS del emisor 340) estén asegurados correctamente utilizando los enlaces de protocolos Secure Socket Layer (SSL) (por ejemplo, SSL-1, SSl-2, SSl-3, SSl-4, SSL-5 y SSL-6).

En el proceso 300 en el paso 351, el titular de la tarjeta 310 puede comprar en un sitio web de un comerciante y, cuando esté listo para terminar la compra, introducir la información de la tarjeta de pago (por ejemplo, el número de cuenta) y otra información (por ejemplo, información de envío) mediante el enlace SSL-1. Una vez que ha sido introducida toda la información de pago y envío, el comerciante puede dar al titular de la tarjeta 310 una oportunidad para revisar la compra antes de enviar un pedido.

Lo siguiente en el paso 352, el MPI 320 consulta al directorio 330 vía el enlace SSL-2 con el fin de verificar la inscripción de titular de la tarjeta 310 con un emisor específico utilizando el mensaje de solicitud de verificación VEReq. El paso 352 puede realizarse de manera opcional localmente en MPI 320 través de un almacenamiento temporal local en el directorio de la tarjeta. En las respuestas al mensaje VEReq, el directorio 330 puede determinar que un emisor particular está participando y de acuerdo con ello reenviar una solicitud a través del enlace SSL-3 al ACS 340 del emisor particular con el fin de comprobar el estado actual de la inscripción del titular 310. Las respuestas resultantes pueden fluir de vuelta sobre los mismos enlaces (p. ej., SSL-3 y SSL-2) a MPI 320. Si el ACS 340 indica que el titular de la tarjeta 310 está inscrito en el programa 1000, MPI 320 puede crear mensaje de Solicitud de Autenticación de Pagador y enviarlo al navegador del titular de la tarjeta en el paso 354 vía el enlace SSL-4. A continuación en el paso 355, el navegador del titular de la tarjeta puede redirigir el mensaje al ACS 340 del emisor apropiado con el fin de iniciar la autenticación del titular de la tarjeta. Cuando el ACS 340 recibe el mensaje de solicitud de autenticación de Pagador, ello puede causar un inicio de dialogo de autenticación de usuario. Como parte del cuadro de diálogo de autenticación de usuario, el ACS 340 puede causar que una ventana interactiva separada de autenticación sea mostrada al titular de la tarjeta 310 con el fin de facilitar la contraseña, el código o la introducción de otros datos por el titular de la tarjeta 310.

En el paso 356, el ACS 340 (utilizando la SPA 135) puede autenticar la contraseña o código introducido por el titular de la tarjeta 310. El ACS 340puede construir un AAV SPA de acuerdo con la implementación del proveedor de programa de autenticación de 3-D Secure. El ACS 340 puede crear y firmar digitalmente un mensaje de respuesta de autenticación de pagador apropiado. El mensaje de respuesta de autenticación de pagador es entonces devuelto (a través del enlace SSL-6) a MPI 320. La ventana de autenticación mostrada al titular de la tarjeta 320 puede desaparecer en este punto.

Después de que ha sido completado el proceso de autenticación 300 del titular de la tarjeta, el comerciante puede ser requerido a pasar el AAV SPA a la entidad adquiriente vía el campo UCAF dentro de un mensaje de autorización. El AAV SPA puede entonces ser pasado a lo largo desde la entidad adquiriente al emisor como parte del proceso de mensajes de autorización convencional. Cuando es recibido por emisor, el AAV puede ser validado como parte del proceso de la solicitud de autorización y archivar para su uso en la resolución de cualesquiera conflictos que puedan surgir más adelante.

Los formatos de mensaje y los formatos de datos estándar de la versión 1.0.2 de 3-D pueden ser utilizados para las comunicaciones de datos entre todas las partes o entidades involucradas. Específicamente, el AAV SPA que el ACS 340 crea y devuelve al comerciante para la inclusión en mensajes de UCAF tiene 28 caracteres de largo y contiene un campo de 20 bytes definido para 3-D Secure en codificación base 64.

La TABLA 3 muestra un ejemplo de estructura de datos o formato de 20 bytes de un AAV de SPA.

TABLA 3

Posición	Nombre de Campo	Fuente de los Datos: ACS	Longitud (Bytes)	Número Byte
1	Byte de control	El byte de control se utiliza para indicar el formato y el contenido la estructura asociada de AAV. Un valor hexadecimal x'8C' puede indicar un AAV creado como el resultado de una autentificación con éxito del titular de la tarjeta. Un valor hexadecimal x'86' puede indicar un AAV creado como Resultado del proceso de intentos	1	Byte 1
2	Resumen criptográfico (hash) del Nombre del Comerciante	La 8 bytes de más a la izquierda de un resumen criptográfico (hash) SHA-1 del campo del Nombre del Comerciante de la PAReq.	8	Bytes 2-9
3	Identificador de ACS	Este campo de datos puede permitir que un emisor utilice hasta 256 facilidades diferentes del ACS. Los valores para este campo pueden ser definidos basados en el algoritmo utilizado para crear el MAC: 0 - 7 Reservados para HMAC 8-15 Reservados para CVC2 16 - 255 - Reservado para uso futuro	1	Byte 10
4	Método de Autenticación	Indica cómo fue autenticado el titular de la tarjeta al ACS: 0 = No Realizada Autenticación del Titular de la Tarjeta (válido solamente para un AAV creado utilizando el valor del byte de control x '86' – Proceso de intentos.) 1 = Contraseña 2 = Clave Secreta (por ejemplo, Tarjeta de Chip)	½ (4 bytes)	Byte 11, 1er digito hex
5	Identificador Clave BIN	Indica cual de las posibles 16 claves secretas de conocidas por el emisor para un rango BIN dado fue utilizada por el ACS identificado mediante el identificador ACS para crear el MAC.	½ (4 bytes)	Byte 11, 2º digito hex
6	Número de Secuencia de la Transacción	Número único que puede ser utilizado para identificar la transacción dentro del ACS identificado por el identificador de ACS. Una vez que ha sido alcanzado el valor máximo, número debe reciclar de nuevo a 0. Este número debe ser único para cada PARes creado por un determinado identificador de ACS para un emisor dado durante el tiempo que se puede presentar un contracargo.	4 (8 dígitos hex)	Bytes 12-15
7	MAC	Código de Autenticación de Mensaje, creado por el ACS	5	Bytes 16-20

Los emisores que proporcionan tanto la identificación de PC existente u otras soluciones de autenticación (por ejemplo, en la figura 1) además de la solución 3-D Secure pueden distinguir entre los valores AAV que reciben de las soluciones de autenticación en el mensaje de autorización correspondiente. El AAV de 20 bytes (por ejemplo, TABLA 2) resultante del programa 1000 compatible con 3-D Secure puede diferir de las estructuras comunes de

AAV de 28 bytes (es decir, en los programas no 3-D Secure) de las siguientes maneras: El importe de la transacción y los códigos de la moneda no están incluidos en el AAV de 20 bytes según como esta información es incluida en el mensaje firmado PARes; Un sello de transacción de comerciante (MTS) no está incluido como un identificador de transacción (XID), que es incluido en el mensaje PARes firmado, puede proporcionar la misma funcionalidad. Además, es ampliado el campo de resumen criptográfico (hash) del nombre del comerciante. Ahora, como un resultado, sólo pueden ser necesarias ediciones mínimas del nombre del comerciante antes de crear el resumen criptográfico (hash) SHA-1.

Puede que un comerciante no tenga que modificar el byte de control para las autorizaciones posteriores (por ejemplo, dividir los envíos). Para dividir los envíos, el comerciante puede reenviar un AAV original generado por implementaciones compatibles con 3-D Secure del programa 1000.

El valor del byte de control en el AAV SPA de 20 byte está basado en el Resultado de la solicitud (PAReq) de autenticación del titular de la tarjeta. Este Resultado puede ser indicado en el campo de estado de la transacción de los mensajes de Respuesta de Autenticación del Pagador (PARes). La TABLA 4 muestra los valores ejemplares del campo de estado de la transacción en un mensaje PARes.

TABLA 4

Campo Estado Transacción en PARes	**Valor Byte Control en AAV (hexadecimal)**	**Valor Byte AAV Primero después codificación Base 64**	**Campo Método Autenticación en AAV**
Y	X´8C´	j	Cualquier Valor definido diferente de “No realizada Autenticación Titular Tarjeta”
A	X´86´	h	Debe ser “No realizada Autenticación Titular Tarjeta”
H	No será generado AAV para este valor de estado	-	-
U	No será generado AAV para este valor de estado	-	-

El nombre del comerciante contenido en el mensaje PAReq puede ser editado antes de crear el resumen criptográfico (hash) del nombre del comerciante. Las ediciones pueden abordar específicamente la codificación de Formato de Transformación Universal (UTF-8) pero también la referencia a los caracteres Unicode para otros tipos de codificación.

Una edición puede eliminar cualquier secuencia de bytes UTF-8 que no tiene una representación Unicode. De tal manera una edición puede borrar cualquier bytes UTF-8 empezando con 1111 binarios y todos los posteriores bytes comenzando con binario 10

Otra edición puede eliminar cualquier secuencia de bytes UTF-8 o secuencia de bytes con la siguiente representación Unicode:

0000 a través de 001F (caracteres control ASCI;
007F a través de 00A0 (caracteres control DEL y C1;
00AD (guión discrecional); y
2000 a través de 206F (Puntuación General).

Tal tipo de edición puede borrar los siguientes bytes UTF-8:

Hex 00 a través de 1F
Hex 7F
Hex C2 80 a través de C2 A0
Hex C2 AD
Hex E2 80 a través de E2 81 AF

Aún otra edición puede borrar cualesquiera espacios líderes o finales (por ejemplo, Hex 20 UTF-8 bytes).

En el caso de una devolución de un cargo u otro proceso potencial de conflicto, el AAV de 20 bytes permite identificar los parámetros de proceso asociados con la transacción. Entre otras cosas, los valores de campo AAV pueden identificar:

- La ubicación física en donde fue procesada la transacción.
- El número de secuencia que puede ser utilizado para identificar positivamente la transacción dentro del universo de transacciones para esa ubicación

• la clave secreta utilizada para crear el MAC, que no sólo asegura la integridad de los datos AAV, sino que también une la estructura AAV completa a una específica PAN para las implementaciones de 3-D Secure.

Las dependencias de campo en el AAV pueden ser establecidas para asegurar la identificación correcta de los parámetros de proceso. Estas dependencias de campo pueden ser consideradas cuando la construcción o configuración de las instalaciones del ACS de emisor. Para cada ACS configurado con el mismo identificador de ACS:

- El campo identificador de la clave BIN debe ser único para cada rango BIN procesado por el identificado ACS. La mayoría de emisores puede utilizar un conjunto común de claves para la mayoría o la totalidad sus rangos BIN. Sin embargo, esta configuración permite flexibilidad en una elección de proveedores de software que soportan o emisores que requieren el uso de un conjunto separado de teclas.
  - o El campo Número de Secuencia de Transacciones debe ser único para cada AAV generada por el ACS identificado dentro del tiempo en que puede ocurrir una devolución de un cargo.

Las instalaciones de ACS que tienen la capacidad de compartir claves BIN y un juego común de números de secuencia de transacción a través de múltiples instalaciones lógicas o máquinas físicas pueden ser configuradas de manera ventajosa para usar el mismo identificador de ACS. Alternativamente, pueden ser requeridos un identificador separado de ACS o un conjunto de identificadores de ACS para cada instalación. En los casos donde una instalación de ACS sirve a emisores múltiples, más de un emisor puede compartir un identificador de ACS. En estos casos, el valor de campo BIN para la transacción asociada puede convertirse en un factor determinante en la interpretación de la ubicación de contenido de campo.

Los algoritmos particulares pueden ser utilizados en SPA 135 con el fin de crear un valor de código de la Autentificación del Comerciante (MAC). Por ejemplo, un algoritmo de "HMAC" o un algoritmo "CVC2" puede ser utilizado por el ACS identificado por el subcampo identificador de ACS para crear valores MAC.

El algoritmo HMAC la genera un valor de MAC mediante encriptación basado en una clave secreta, identificada por el sub campo de identificador de clave BIN. Esta clave secreta es compartida con el emisor y une el número de cuenta del titular de la tarjeta al AAV mediante la concatenación de los siguientes datos:

• El número de cuenta, tal y como es recibido por el ACS en el mensaje de solicitud de verificación (VEReq) que corresponde al mensaje actual de Solicitud de Autenticación de Pagador (PAReq). El número de cuenta puede ser representado como un decimal codificado binario, justificado a la izquierda y rellenado a la derecha con hexadecimal 'F' a una longitud de 20 dígitos (total 10 bytes).

• Los 15 bytes de más a la izquierda, siendo construidos campos 1 hasta 6, del AAV.

La longitud de la clave secreta puede ser de manera opcional seleccionada para tener un mínimo de 128 bits (16 bytes) y un máximo de 192 bits (24 bytes). Cualquier tamaño de clave intermedio (por ejemplo 160 bits) puede ser aceptable. El tamaño de la longitud de clave real utilizado puede ser seleccionado de manera independiente por cada implementación. El campo MAC dentro de la AAV de SPA definido para un programa de Autenticación 3-D Secure (por ejemplo, el programa 1000) puede ser rellenado con los 40 bits del extremo izquierdo (5 bytes binarios) del Resultado criptográfico que se obtiene aplicando el algoritmo HMAC.

Los ejemplos 1 y 2 ilustran la aplicación del algoritmo HMAC usando 20 bytes y claves de 16 bytes, respectivamente, para generar valores de AAV SPA.

EJEMPLO 1 (Clave de 20 bytes)

Número de cuenta Asumido: 5432 109876543210
Nombre comerciante Asumido: SPA comerciante, Inc. (todos caracteres ASCII y no requiere edición)
Byte de control del AAV Asumido = 8C
Primeros 8 bytes, SHA-I Resumen criptográfico (hash) del Nombre de Comerciante = 7CA7 FBB6 058B 5114
ACS Id Asumida = 01
Método de Autenticación Asumido = 1 (contraseña)
Clave BIN Id Asumida = I
Número de Secuencia de Transacción Asumido = 0000002F
Clave Asumida (20 Bytes) = OBOBOBOBOBOBOBOBOBOBOBOBOBOBOBOBOBOBOB

Por lo tanto SHA-1HMAC se basa en
5432 109876543210 FFFF 8C 7CA7FBB6058B5114 0111 0000002F

Esto produce un MAC cuyos primeros 5 bytes son:
3547 BAlE FF

Por lo tanto, el AAV completo en hex es:
8 C 7CA7FBB6058B5114 0111 0000002F 3547BAlEFF

Después de la codificación Base-64, es esto:
jHyn+ 7YFiIEUAREAAAAvNUe6Hv8=

EJEMPLO 2 (clave de 16 bytes)

Número de cuenta Asumido: 5432 109876543210
Nombre de Comerciante Asumido: SPA comerciante, Inc. (todos caracteres ASCII y no requiere edición)
Byte de Control Asumido AA V = 8C
Primeros 8 bytes, SHA-1 resumen criptográfico (hash) del Nombre de Comerciante = 7CA7 FBB6 058B 5114
ACS Id Asumida = 01
Método de Autenticación Asumido = 1 (contraseña)
Clave BIN Clave Id Asumida = 1
Número de Secuencia de Transacción Asumido = 0000002F
Clave (16 Bytes) Asumida = 00112233445566778899AABBCCDDEEFF
Por lo tanto, SHA-1HMAC está basado en
5432 109876543210 FFFF 8C 7CA7FBB6058B5114 0111 0000002F
Esto produce un MAC cuyos primeros 5 bytes son:
EB27 FC7F AB
Por lo tanto, el AAV completo en hex es:
8C 7CA7FBB6058B5114 0111 0000002F EB27FC7FA
Después de la codificación Base-64, es esto:
jHyn+ 7YFi1 EUAREAAAA v6yf8f6s =

El algoritmo CVC2 de también crea Criptográficamente los valores de campo de MAC. En contraste con el algoritmo HMAC, que utiliza una clave, el algoritmo CVC2 utiliza dos claves DES de 64 bits identificadas por el sub campo de identificador de clave BIN. En el algoritmo CVC2, todos los pasos de encriptación y des encriptación pueden utilizar formulario de Libro de Código Electrónico (BCE) de DES.

El algoritmo CVC2 genera un valor de tres dígitos 3 dígitos CVC2. Los datos de entrada que son procesados por el algoritmo CVC2 para la generación de este valor de tres dígitos 3 dígitos CVC2 es mostrados en la TABLA 5.

TABLA 5

Nombre de campo CVC2	**Nombre de campo MAC**	**Fuente de Datos**	**Longitud (Dígitos)**
Numero Cuenta Primario	Numero Cuenta Primario	El número de cuenta, tal y como está representado en el mensaje de Solicitud de Verificación (VEReq)	13 a 19 dígitos
Fecha Expiración Tarjeta	Número de Secuencia de la Transacción	Convertir el Número de Secuencia de Transacción, tal y como figura en el AAV, a equivalente decimal BCD. Rellenar este campo con por lo menos los 4 dígitos significativos. Cualquier valor menor de 4 dígitos debe ser justificado correctamente en el campo y rellenado con ceros binarios a 4 dígitos.	4 dígitos
Código de Servicio	Método de Autenticación	Método de Autenticación tal y como está contenido en el AAV. Si el valor del sub campo de Método de Autenticación es mayor que 9, restar 10 para obtener el dígito para ser utilizado	1 dígito
	Byte de Control	Convertir el Byte de Control tal y como está contenido en el AAV a equivalente decimal BCD. Rellenar este campo con los por lo menos 2 dígitos significativos	2 dígitos

El valor de tres dígitos CVC2 resultante es convertido a forma decimal codificado binario y poblado en los bytes de más a la izquierda del sub campo MAC con un 0 binario principal utilizado para rellenar el primer medio byte sin usar. El resto de los bytes del sub campo MAC puede ser llenado con ceros binarios. Por ejemplo: CVC2 = 123 MAC sub campo = 0123000000 (total 10 dígitos).

El EJEMPLO 3 y la TABLA 6 ilustran la aplicación del algoritmo CVC2 y los pasos del proceso involucrados en la aplicación del algoritmo con el fin de generar los valores AAV SPA.

EJEMPLO 3

Número de cuenta Asumido: 5432109876543210
Nombre de Comerciante Asumido: SPA comerciante, Inc. (todos caracteres ASCII y no requiere de edición)
Byte de control Asumido AA V = 8C
Primeros 8 bytes, SHA-1 resumen criptográfico (hash) del Nombre de Comerciante = 7CA7 FBB6 058B 5114
ACS Id Asumido = 7
Método de Autenticación Asumido = 1 (contraseña)
Clave BIN Id Asumida = 1
Número de Secuencia de Transacción Asumido = 0000002F
Clave A = 0011223344556677 Clave B = 8899AABBCCDDEEFF

Por lo tanto, el cálculo del algoritmo CVC2 está basado en
Número de Cuenta= 5432109876543210 Fecha de vencimiento = 0047
Código Servicio = 140

Esto produce un valor de tres dígitos CVC2 = 439 (ver Tabla 6 para el cálculo):
Basado en el valor calculado de CVC2, el campo MAC = 0439000000

Por lo tanto, el completo AA V en hex es:
8 C 7CA7FBB6058B5114 01 0000002F 11

Codificado en Base-64-, esto es:
jHyn+ 7YFi1 EUAREAAAAvBDkAAAA =

El proceso o cálculo de pasos que se utilizan en el ejemplo 3 están mostrados en la TABLA 6

TABLA 6

Paso	Paso del Proceso	Ejemplo
1.	Construir la cadena de bits al concatenar (izquierda a derecha) los 4 bits de más a la derecha de cada carácter de los elementos de datos especificados	54321098765432100047140
2.	Colocar los resultados en un campo de 128-bit, rellenando en la derecha con ceros binario para llenar todos los bits restantes. Dividir el bloque de 128 bits en 2 bloques de 64 bits.	54321098765432100047140000000000 Bloque 1 = 5432109876543210 Bloque 2 = 0047140000000000
3.	Encriptar el Bloque 1 utilizando la Clave A	Bloque 1 = 5432109876543210 Clave A = 0011223344556677 Resultado = 44DD7C814CC62702
4.	XOR los resultados del paso 3 con el Bloque 2. Encriptar este valor utilizando la Clave A	Bloque 2 = 0047140000000000 Paso 3 44DD7C814CC62702 Resultado = Resultado = 449A68814CC62702
5.	Desencriptar el resultado del paso 4 utilizando la Clave B	Paso 4 449A68814CC62702 Resultado = ClaveB = ClaveB = 8899AABBCCDDEEF F Resultado = 191DCA3149A5BD51
6.	Encriptar el resultado del paso 5 utilizando la Clave A	Paso 5 191DCA3149A5BD51 Resultado = Clave A = 0011223344556677 Resultado = 4F AB392CE3C98B41
7.	Desde el resultado del paso 6, yendo de izquierda a derecha, extraer todos los dígitos numéricos (0-9); justificar a la izquierda estos dígitos en un campo de 16 posiciones	439239841
8.	Desde el resultado del paso 6, yendo de izquierda a derecha, extraer todos los caracteres de la A la F. Con el fin de compensar para decimales, restar 10 de cada dígito extraído.	012421
9.	Concatenar los dígitos del paso 7 a la derecha de los dígitos extraídos en el paso 8.	439239841012421
10.	Seleccionar desde los tres primeros dígitos de más a la izquierda del CVC.	439

Tal y como está definido mediante el protocolo 3-D Secure, todos los mensajes de PARes devueltos al comerciante son firmados digitalmente el ACS del emisor del titular de la tarjeta asociado. El comerciante puede ser requerido para validar la firma digital antes de extraer el AAV SPA desde el mensaje de PARes para su inclusión en una solicitud de autorización enviada a la entidad adquiriente. Si un emisor soporta tanto la implementación de 3-D Secure y otras plataformas de autenticación (por ejemplo, plataformas de autenticación de PC) puede ser necesario distinguir entre las dos plataformas de autenticación durante el procesamiento del mensaje de solicitud de

autorización. Esto se puede lograr en una de dos maneras:

1. El primer carácter base 64 codificado es:
    a. "j" o "h" para el AAV de SPA dentro de la aplicación definida de 3-D Secure.
    b. "g" o "A" para el AAV SPA Autenticación de PC
2. El byte de control, convertido a binario, es tanto,
    a. hexadecimal8C o hexadecimal 86 para el AAV definido para la implementación de MasterCard de 3-D Secure.
    b. hexadecimal 82 ó hexadecimal 02 para el AA V SPA Autenticación PC.

Cada emisor que participa en el programa 1000 puede asegurar que el sub campo identificador ACS está debidamente configurado para indicar el algoritmo utilizado para crear el MAC. El fallo para establecer este indicador correctamente puede ocasionar validaciones inadecuadas durante el proceso de autorización de la transacción/pago.

Aunque la presente invención ha sido descrita en relación con los ejemplos específicos de realizaciones, debe ser entendido que podrían ser hecho varios cambios, sustituciones y modificaciones aparentes a aquellos especializados en la Técnica a las realizaciones divulgadas sin apartarse del ámbito de aplicación de la invención de acuerdo con lo que está definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema para autenticar una transacción de titular con un comerciante en una red electrónica, el sistema que comprende:
   Una capa de plataforma de emisor incluyendo por lo menos un programa de autenticación 3-D Secure,
   Un Plug-in de comerciante, "MPI";
   Un algoritmo seguro de pago, «SPA»; y
   Una capa transporte de datos,
   En donde la plataforma de emisor comprende un servidor de control de acceso, "ACS", que utiliza la SPA para procesar la transacción y la información del titular de la tarjeta para la autenticación mediante un método de autenticación y para generar un Valor de Autenticación de Titular de Cuenta, "AAV", y transmite el AAV a través de la capa de transporte de datos a la MPI,
   En donde el AAV es una estructura de datos con formato compatible con los protocolos de mensaje 3-D Secure, en donde la estructura de datos con formato tiene una longitud de más de 20 bytes incluyendo los bytes que identifican un resumen criptográfico (hash) del nombre del comerciante, bytes que identifican el ACS, bytes que identifican el método de autenticación, bytes que identifican las claves criptográficas secretas y bytes que incluyen un código de autenticación del comerciante, "MAC".

2. El sistema de la reivindicación 1, en donde el AAV es una estructura de datos con formato que esta codificada Base 64.

3. El sistema de la reivindicación 1, en donde el SPA comprende un algoritmo de encriptación para generar el MAC, en donde el algoritmo de encriptación utiliza una clave secreta identificada en el AAV para encriptar una concatenación de número de cuenta del titular de la tarjeta y una pluralidad de los campos de los bytes del AAV excluyendo los bytes que representan el MAC, y en donde una parte del resultado de la encriptación forma los bytes de MAC en el AAV.

4. El sistema de la reivindicación 1, en donde el SPA comprende un algoritmo de encriptación para generar el MAC, en donde el algoritmo de encriptación utiliza un par de llaves secretas A y B que están identificadas en el AAV con el fin de encriptar una concatenación número cuenta del titular de la tarjeta, fecha de vencimiento y código de servicio para generar un campo de tres dígitos CVC2 y utiliza el resultado para rellenar dos bytes del MAC.

5. El sistema de la reivindicación 4 en donde el par de claves secretas A y B son claves, "DES" Data Encryption Standard de 64-bit.

6. El sistema de la reivindicación 1 en donde el ACS está configurado con el fin de generar un AAV en respuesta a un mensaje de solicitud de autenticación de pago desde el MPI al ACS.

7. El sistema de la reivindicación 1, que está configurado para el transporte del AAV en un mensaje de respuesta de autenticación de pago desde el ACS.

8. El sistema de la reivindicación 7 donde el ACS esta además configurado para colocar una firma digital en mensaje de respuesta de autenticación de pago.

9. El sistema de la reivindicación 1, en donde el MPI está configurado para verificar la firma digital en un mensaje de respuesta de autenticación de pago recibido.

10. El sistema de la reivindicación 1, en donde el MPI está configurado con el fin de extraer los campos MAC incluidos en un mensaje de respuesta de autenticación de pago desde el ACS y colocar el MAC extraído en mensaje de solicitud de autorización un pago a una tercera parte.

11. Una estructura de datos para el transporte de la información de la autenticación de un titular de tarjeta en la transacción entre las partes interesadas en un entorno 3-D Secure, estructura de datos que comprende 20 bytes de caracteres codificados en Base 64, en donde el primer byte es un byte de control, los bytes 2-9 representan un resumen criptográfico (hash) del nombre del comerciante, el byte 10 identifica un servidor de control de Acceso, ACS, que autentifica la transacción del titular de la tarjeta por un método de autenticación, el byte 11 identifica el método de autenticación y las claves de encriptación secretas que son utilizadas por el ACS para generar un código de autenticación del comerciante "MAC", los bytes 12-15 representan un número de la secuencia de transacción que identifica a un número de transacción procesado por el ACS y los bytes 16-20 representan el MAC.

12. La estructura de datos de la reivindicación 11 en donde el MAC comprende partes de una encriptación de una concatenación de número de cuenta del titular de la tarjeta y una pluralidad de los campos de bytes 1-15 de la estructura de datos y en donde una sola clave identificada en el byte 11 es utilizada para la encriptación.

13. La estructura de datos de la reivindicación 11 en donde el MAC comprende partes de una encriptación de una concatenación de número de cuenta del titular de la tarjeta, fecha de vencimiento de la tarjeta y código de servicio y en donde un par de claves A y B están identificadas en el byte 11 son utilizadas para la encriptación.

14. La estructura de datos de la reivindicación 13 en donde un resultado de encriptación de tres dígitos es utilizado para rellenar dos bytes de los bytes MAC 16-20.

15. La estructura de datos de la reivindicación 13 en donde el par de claves secretas A y B son claves "DES" Data Encryption Standard de 64-bit.

16. Un método para autenticar una transacción de un titular de tarjeta con un comerciante en una red electrónica en un entorno 3-D Secure, método que comprende:

Utilizar un servidor de control de acceso, "ACS", para procesar la información del titular de la tarjeta y de la transacción con el fin de autenticar al titular de la tarjeta por un método de autenticación;

Implementar un algoritmo de pago seguro, «SPA», con la intención de generar un Valor de la Autenticación del Titular de la Cuenta, "AAV", con el fin de representar los resultados de la autenticación y

Transportar el AAV en mensajes 3-D Secure al comerciante, en los que el AAV es un estructura de datos con formato que tiene una longitud de más de 20 bytes, incluyendo bytes que identifican un resumen criptográfico (hash) del nombre del comerciante, bytes que identifican el ACS, bytes que identifican el método de autenticación, bytes que incluyen un código de autenticación del comerciante, "MAC" y bytes que identifican las secretas claves criptográficas que son utilizadas por la SPA para generar el MAC.

17. El método de la reivindicación 16 en donde el AAV es una estructura de datos con formato codificada Base 64.

18. El método de la reivindicación 16 en donde desplegar una SPA incluye:

Utilizar una clave secreta identificada en el AAV con el fin de encriptar una concatenación del número de cuenta del titular de la tarjeta y por lo menos partes de los bytes del AAV excluyendo los bytes que representan el MAC; y asignar una parte del resultado de la encriptación a los bytes de MAC en el AAV.

19. El método de la reivindicación 16 en donde desplegar un SPA comprende:

utilizar un par de par claves secretas A y B que están identificadas en el AAV con la intención de encriptar una concatenación del número cuenta del titular de la tarjeta, fecha del vencimiento y código de servicio con el fin de generar un campo de CVC2 de tres dígitos; y asignar el resultado para rellenar dos bytes del MAC.

20. El método de la reivindicación 17 en donde el par de claves secretas A y B son claves "DES" Data Encryption Standard de 64-bit.

21. El método de la reivindicación 16 en donde el transporte del AAV en mensajes 3-D Secure al comerciante comprende el trasporte del AAV en un mensaje de respuesta de autenticación de pago que está firmado digitalmente por el ACS.

22. El método de la reivindicación 21, que comprende además:

Primero, la verificación por el comerciante de la firma digital en un mensaje de respuesta de autenticación de pago recibido, y

A continuación, la extracción de los campos de MAC del mensaje de respuesta de autenticación de pago recibido por el comerciante.

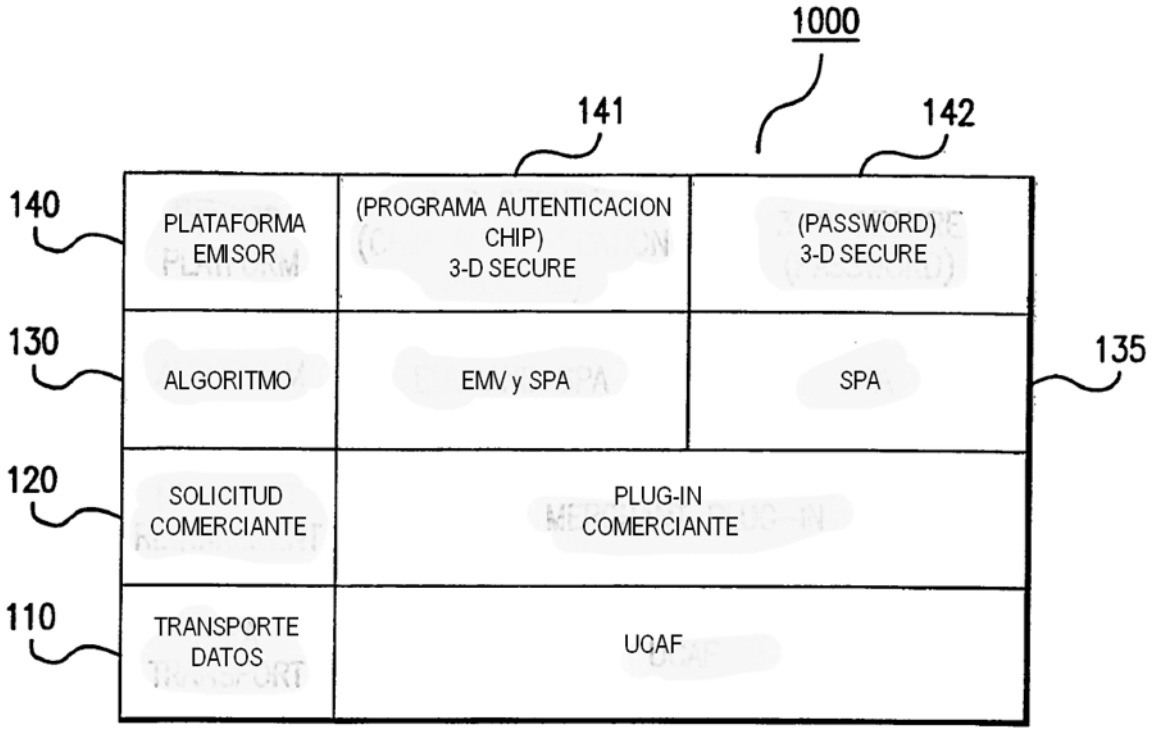
1000
141
142
140
PLATAFORMA EMISOR
(PROGRAMA AUTENTICACION CHIP) 3-D SECURE
(PASSWORD) 3-D SECURE
130
ALGORITMO
EMV y SPA
SPA
135
120
SOLICITUD COMERCIANTE
PLUG-IN COMERCIANTE
110
TRANSPORTE DATOS
UCAF

FIG.1

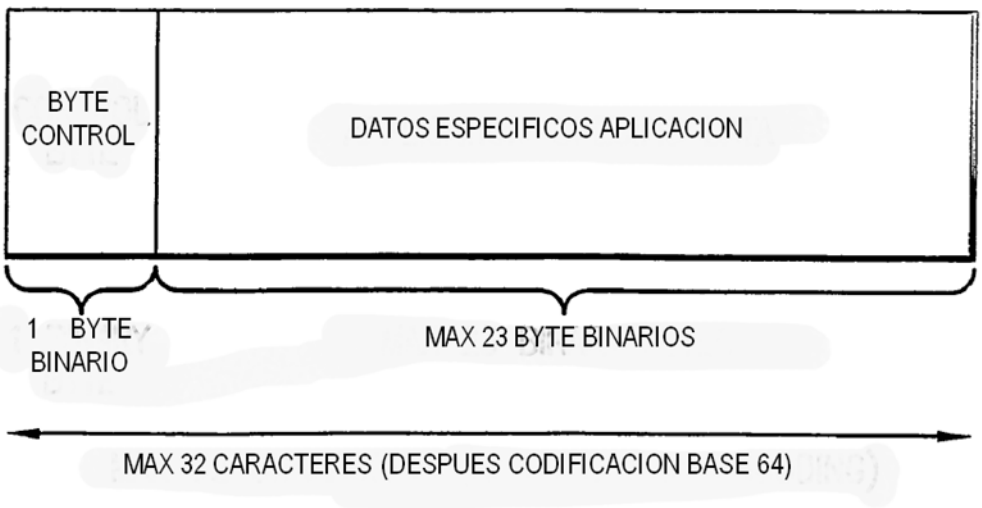
BYTE CONTROL
DATOS ESPECIFICOS APLICACION
1 BYTE BINARIO
MAX 23 BYTE BINARIOS
MAX 32 CARACTERES (DESPUES CODIFICACION BASE 64)

FIG.2

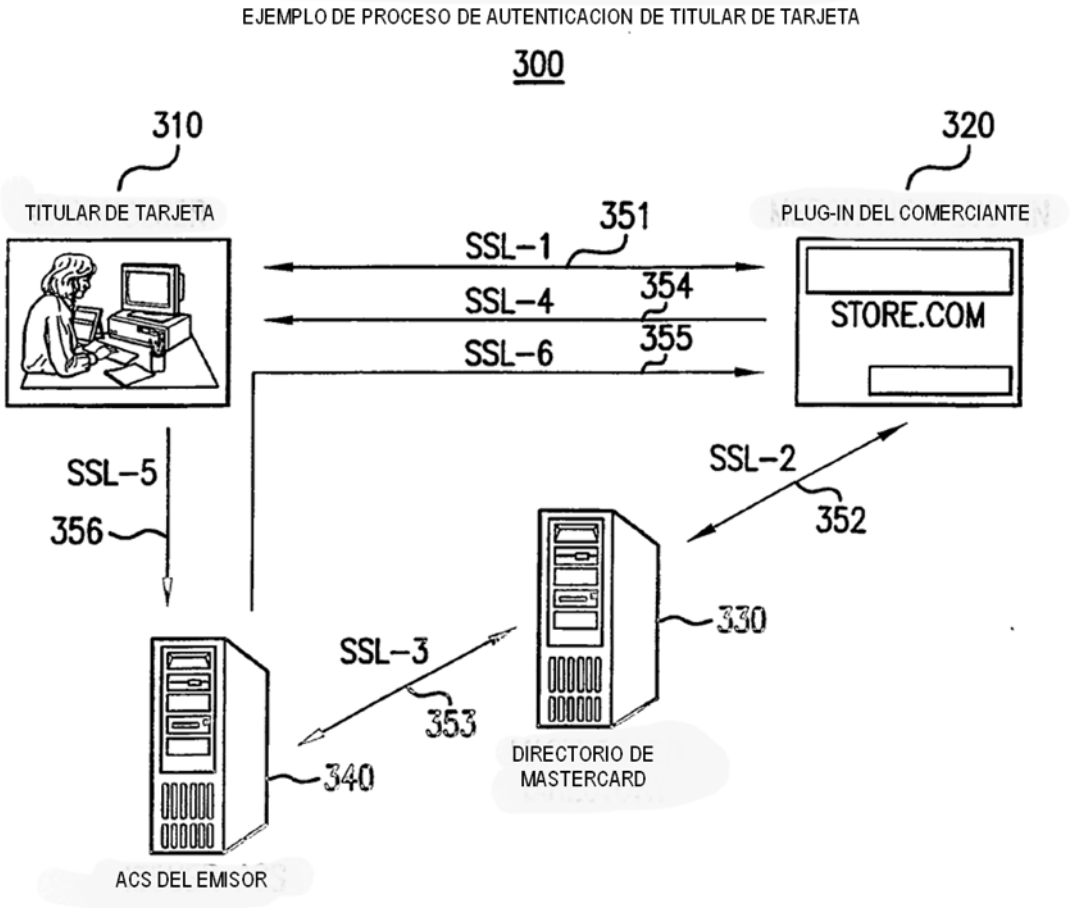
EJEMPLO DE PROCESO DE AUTENTICACION DE TITULAR DE TARJETA
300
310
TITULAR DE TARJETA
320
PLUG-IN DEL COMERCIANTE
351
SSL-1
354
SSL-4
355
SSL-6
STORE.COM
SSL-5
356
SSL-2
352
330
SSL-3
353
340
DIRECTORIO DE MASTERCARD
ACS DEL EMISOR

FIG.3

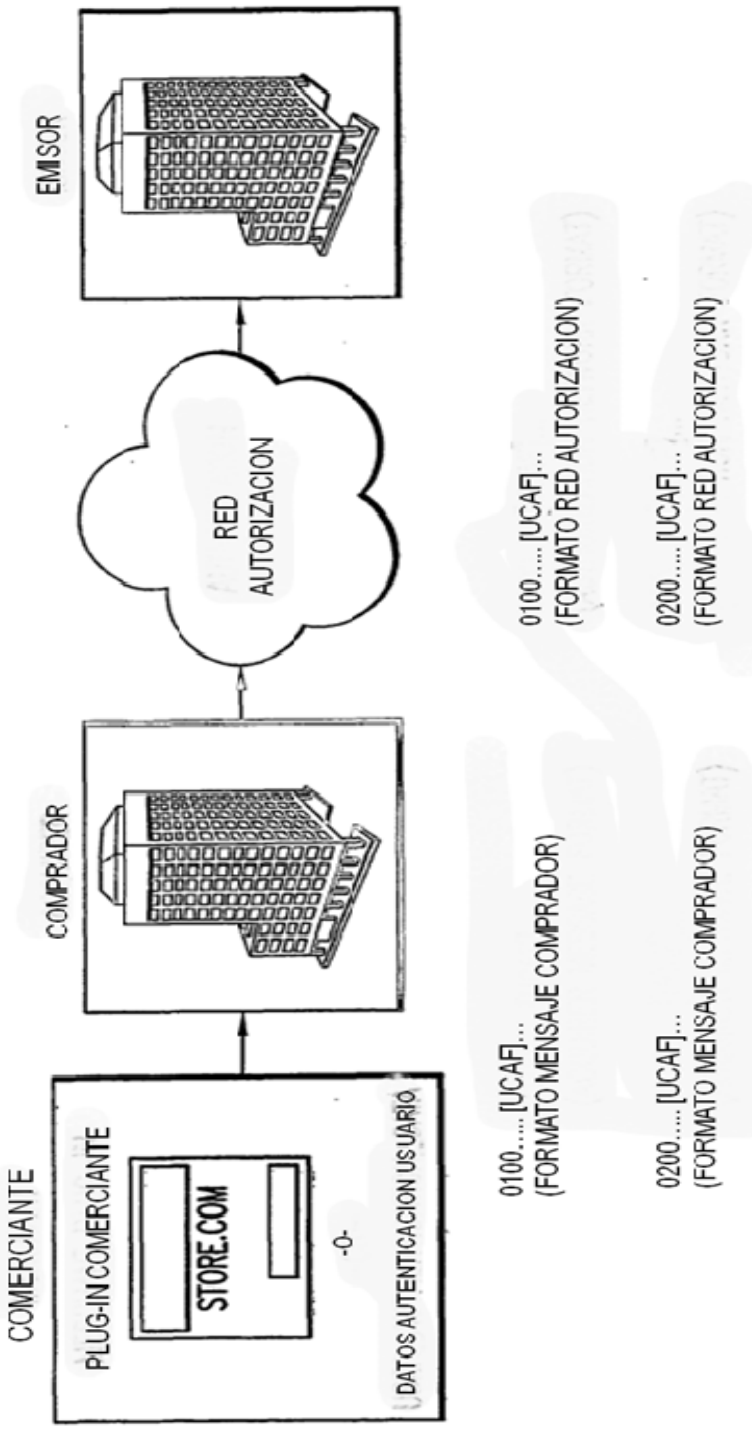
COMERCIANTE
PLUG-IN COMERCIANTE
STORE.COM
-0-
DATOS AUTENTICACION USUARIO
COMPRADOR
RED AUTORIZACION
EMISOR
0100..... [UCAF]...
(FORMATO MENSAJE COMPRADOR)
0200..... [UCAF]...
(FORMATO MENSAJE COMPRADOR)
0100..... [UCAF]...
(FORMATO RED AUTORIZACION)
0200..... [UCAF]...
(FORMATO RED AUTORIZACION)

FIG.4