



HU000029807T2

(19) **HU****MAGYARORSZÁG**
Szellemi Tulajdon Nemzeti Hivatala(11) Lajstromszám: **E 029 807**(13) **T2**

EURÓPAI SZABADALOM SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 04 776493**(22) A bejelentés napja: **2004. 06. 10.**

(96) Az európai bejelentés bejelentési száma:

EP 20040776493

(97) Az európai bejelentés közzétételi adatai:

EP 1636680 A2 **2005. 01. 06.**

(97) Az európai szabadalom megadásának meghirdetési adatai:

EP 1636680 B1 **2016. 04. 13.**(51) Int. Cl.: **G06Q 40/00** (2006.01)

(86) A nemzetközi (PCT) bejelentési szám:

PCT/US 04/018658

(87) A nemzetközi közzétételi szám:

WO 05001635

(30) Elsőbbségi adatok:

477187 P **2003. 06. 10.** **US**
PCT/US2004/017756 **2004. 06. 04.** **WO**

(72) Feltaláló(k):

KRANZLEY, Arthur, D., Pound Ridge, NY 10576 (US)
ORFEI, Stephen, W., Katonah, NY 10536 (US)
RUTHERFORD, Bruce, J., Stamford, CT 06903 (US)
WIESMAN, Mark, Chesterfield, MO 63017 (US)

(73) Jogosult(ak):

MASTERCARD INTERNATIONAL, INC.,
Purchase, NY 10577 (US)

(74) Képviselő:

Danubia Szabadalmi és Jogi Iroda Kft.,
Budapest(54) **Rendszerek és eljárások biztonságos fizetési tranzakció végrehajtására formázott adatszerkezet felhasználásával**

Az európai szabadalom ellen, megadásának az Európai Szabadalmi Közlönyben való meghirdetésétől számított kilenc hónapon belül, felszólalást lehet benyújtani az Európai Szabadalmi Hivatalnál. (Európai Szabadalmi Egyezmény 99. cikk(1))

A fordítást a szabadalmas az 1995. évi XXXIII. törvény 84/H. §-a szerint nyújtotta be. A fordítás tartalmi helyességét a Szellemi Tulajdon Nemzeti Hivatala nem vizsgálta.



(11) **EP 1 636 680 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
13.04.2016 Bulletin 2016/15

(21) Application number: **04776493.1**

(22) Date of filing: **10.06.2004**

(51) Int Cl.:
G06Q 40/00 (2012.01)

(86) International application number:
PCT/US2004/018658

(87) International publication number:
WO 2005/001635 (06.01.2005 Gazette 2005/01)

(54) **SYSTEMS AND METHODS FOR CONDUCTING SECURE PAYMENT TRANSACTIONS USING A FORMATTED DATA STRUCTURE**

SYSTEME UND VERFAHREN ZUR DURCHFÜHRUNG VON SICHEREN
BEZAHLUNGSTRANSAKTIONEN UNTER VERWENDUNG EINER FORMATIERTEN
DATENSTRUKTUR

SYSTEMES ET PROCEDES PERMETTANT D'EFFECTUER DES TRANSACTIONS DE PAIEMENT
SECURISE AU MOYEN D'UNE STRUCTURE DE DONNEES FORMATEE

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PL PT RO SE SI SK TR**

(30) Priority: **10.06.2003 US 477187 P**
04.06.2004 PCT/US2004/017756

(43) Date of publication of application:
22.03.2006 Bulletin 2006/12

(73) Proprietor: **MASTERCARD INTERNATIONAL, INC.**
Purchase, NY 10577 (US)

(72) Inventors:
• **KRANZLEY, Arthur, D.**
Pound Ridge, NY 10576 (US)
• **ORFEI, Stephen, W.**
Katonah, NY 10536 (US)
• **RUTHERFORD, Bruce, J.**
Stamford, CT 06903 (US)
• **WIESMAN, Mark**
Chesterfield, MO 63017 (US)

(74) Representative: **Beresford, Keith Denis Lewis**
Beresford Crump LLP
16 High Holborn
London WC1V 6BX (GB)

(56) References cited:
US-A1- 2001 032 154 US-A1- 2001 032 154
US-A1- 2002 194 138 US-A1- 2002 194 138
US-A1- 2003 212 642 US-A1- 2003 212 642

- **GPayments: "A comparison of VisaCard 3-D Secure and Mastercard SPA Security Architecture", Internet, 1 March 2002 (2002-03-01), XP002690680, Retrieved from the Internet:
URL:www.3mfuture.com/articles_epayment/GPayments_3-D_vs_SPA_Whitepaper.pdf [retrieved on 2013-01-21]**
- **Mark Patrick - Vice President - Interactive Services MasterCard International: "Guaranteed Payments for E-Commerce Transactions", Internet, 1 April 2003 (2003-04-01), XP002690681, Retrieved from the Internet:
URL:www.cnsg.com.sg/archive/MasterCard.ppt [retrieved on 2013-01-21]**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 636 680 B1

Description**BACKGROUND OF INVENTION**

5 **[0001]** The present invention relates to systems and methods for authenticating transactions conducted by parties over open electronic networks such as the Internet. In particular, the invention relates to authentication of Internet transactions in which customers charge payments to payment cards, including credit cards.

[0002] E-commerce is now popular. Conducting transactions over electronic networks such as the Internet has the now oft-stated advantages of convenience, lower costs, market reach and choice, for both merchants and customers. However, the anonymity of the Internet brings to a commercial or retail sale the issues of fraud and misuse. A transacting merchant has a desire to authenticate the sale, certify the sale, confirm the sale, ensure non-repudiation of the sale, ensure payment, and control anonymity. Similarly, a buyer has a desire to control authentication of the sale, integrity of the sale, recourse of a bad sale, confirmation of the sale, privacy, and anonymity.

[0003] Commonly assigned U.S. patent application No. 10/096,271 filed March 11, 2002, which is hereby incorporated by reference in its entirety herein, describes a system and method for conducting secure payment transactions utilizing user software at a customer terminal to receive a set of Web page data to be used for displaying a Web page, which may include one or more hidden fields. The Web page with transaction and cardholder data is sent to the merchant as the purchase data. The merchant may submit this web page data electronically, for example, to an issuer, for authentication or authorization of the payment transaction.

20 **[0004]** Card issuers and other financial institutions now offer or use standardized Internet transaction protocols to improve on-line transaction performance and to accelerate the growth of electronic commerce. Under some standardized protocols (e.g., 3-D Secure™ Protocol developed by Visa International) card issuers or issuing banks may authenticate transactions thereby reducing the likelihood of fraud and associated chargebacks attributed to cardholder not-authorized transactions. The presence of an authenticated transaction may result in an issuer assuming liability for fraud should it occur despite efforts to authenticate the cardholder during an online purchase. Card issuers or issuing banks may assure merchants that they will be paid for issuer-authenticated transactions. The 3-D Secure™ protocol is consistent with and underlies the authentication programs offered by card issuers (e.g., Verified by Visa or MasterCard SecureCode™) to authenticate customers for merchants during remote transactions such as those associated with the Internet. The 3-D Secure™ Protocol leverages existing Secure Sockets layer (SSL) encryption functionality and provides enhanced security through issuer authentication of the cardholder during the online shopping session. A piece of software called the Merchant Plug In (MPI) is used by participating merchants to exchange messages, pass information and query participants in order to establish an authentication session between the cardholder and their card issuer during an online purchase.

30 **[0005]** The 3-D Secure Protocol services are based on a three-domain model - the issuer domain, the acquirer and the interoperability domain. The issuer is responsible for managing the enrollment of cardholders in the service, and for authenticating cardholders during on-line transactions. The acquirer is responsible for defining procedures so that merchants participating in Internet transactions operate under an agreement with the acquirer, and for providing back end processing for authenticated transactions. The interoperability domain facilitates the transaction exchange between the other two domains with a common protocol and shared services. Cardholders and their banks may come under "issuer domain", merchants and their banks may come under the "acquirer domain". Communication between issuing and acquiring banks or financial institutions and card issuer infrastructure may come under "Interoperability Domain". While transacting with 3-D Secure compliant banks and merchants, a consumer may have the same Internet shopping experience as previously, except that there is a separate authentication window or pop-up screen from the cardholder's bank to determine if the transacting party is indeed the cardholder of record. The transaction flow for an on-line Internet purchase transaction under the protocol may be as follows:

45 (1) Customers fill in payment data at Merchant web sites in the usual fashion, via an encrypted Secure Sockets Layer (SSL) connection.

(2) The Merchant then sends a message through an MPI to a Directory, which in turn queries the card issuer, to find out whether the customer is enrolled in the 3-D Secure program.

50 (3) The card issuer responds to the Directory with a message indicating whether the cardholder is enrolled and, if so, provides a Web address for the bank that issued the card. This message is then processed and a response forwarded to the Merchant.

(4) The Merchant then sends a message to the issuing bank, through the cardholder device, to initiate and authentication session between the cardholder and the card issuer in which transaction details such as Merchant name and transaction amount may also be presented to the cardholder for confirmation.

55 (5) The issuing bank will then populate an authentication window to the cardholder detailing information related to the transaction such as merchant name and amount, a personal security message, and a response area where authentication details can be entered by the cardholder.

(6) The customer approves the transaction in one of a variety of ways, depending on how the issuing bank chooses to implement the system. Options may range from entering a static password or PIN to utilizing a smart card and a Personal Card Reader (PCR) to generate an authentication token.

(7) The issuer may process the transaction and cardholder data for authentication. If the authentication is valid, the issuer sends a message to the merchant indicating the authentication was successful. The issuer also notifies the merchant if the authentication failed or was unable to be completed. The message may include an Accountholder Authorization Value (AAV) encoding the authentication process results.

[0006] Consideration is now being given to ways of enhancing the systems and methods for authenticating customers, who use credit or debit cards for payment in electronic transactions. Attention is directed to the data and the algorithms that are used to securely authenticate the customer or card for payment to the merchant. The solutions should preferably be compatible with industry implementations of common protocols like 3-D Secure and other industry standards such as the EMV standard for smart cards.

SUMMARY OF THE INVENTION

[0007] In accordance with the present invention as defined in the appended claims authentication programs that are consistent with 3-D Secure protocols are provided for authenticating on-line cardholder transactions. The authentication programs use an access control server (ACS) to authenticate cardholder transactions. Secure Payment Algorithms (SPA) are applied by the ACS to cardholder and transaction information to generate an encrypted Accountholder Authentication Value (AAV), which is assigned to an authenticated transaction. The generated AAV has a data structure that is suitable for inclusion in 3-D Secure protocol messages.

[0008] In preferred embodiments of the invention, the data structure has a length of no more than about 20 bytes of Base 64 encoded characters. The first byte may be a control byte, bytes 2-9 may represent a hash of a merchant name, and byte 10 identifies the particular ACS that authenticated the cardholder transaction. Various authentication methods (e.g., password based, chip based, or PC identification methods) may be used by the ACS to authenticate the cardholder transaction. Byte 11 of the AAV data structure identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication Code (MAC). Bytes 12-15 of the AAV data structure identifies a sequence number of transactions processed by the ACS, and bytes 16-20 represent the MAC.

[0009] SPA may include suitable encryption processes to generate MAC values for a particular transaction. One encryption process uses a secret key to encrypt a concatenation of the card holder's account number and fields 1-6 (or bytes 1-15) of the AAV. The first 40 bits (or 5 binary bytes) of the encryption result are assigned to the MAC field. In another encryption process, a pair of Data Encryption Standard (DES) keys is used to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit Cardholder Verification Code (CVC2) number. This three digit number is converted into binary coded decimal which then is used to populate one and one half bytes of the MAC field in the AAV data structure. The remaining three and one half bytes of the MAC field may be padded or populated with binary zeros.

[0010] 3-D Secure Protocol electronic messages, which include AAV data, may be digitally signed by the Access control server (ACS). The merchant receiving a message containing the AAV data may be required to validate the digital signature in conformity with the 3-D Secure Protocol before extracting or using the AAV data. Merchants may transfer the AAV data and in particular MAC data to payment authorization request messages.

[0011] Further features of the invention, its nature, and various advantages will be more apparent from the following detailed description and the accompanying drawings

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

FIG. 1 is a schematic illustration of an exemplary authentication program utilizing Secure Payment Algorithms (SPA) to generate Accountholder Authentication Values (AAV) for payment transactions, in accordance with the principles of the present invention.

FIG. 2 is a schematic illustration of the structure of a Universal Cardholder Account Field, which is used for transporting the output of the Secure Payment Algorithms (SPA) of FIG. 1, in accordance with the principles of the present invention.

FIG. 3 is an illustration of some of the steps and message links between entities that are involved in an exemplary payment transaction authentication process, in accordance with the principles of the present invention.

FIG. 4 is a schematic illustration of interaction between exemplary authentication and authorization entities involved in the authentication and authorization of on-line payment transactions.

[0013] Throughout the figures, unless otherwise stated, the same reference numerals and characters are used to denote like features, elements, components, or portions of the illustrated embodiments.

DETAILED DESCRIPTION OF THE INVENTION

[0014] The present invention provides solutions for authenticating remote parties in an electronic transaction. In particular, the solutions relate to Secure Payment Applications (e.g., FIG. 1 SPA 135) that are used to authenticate a cardholder who remotely participates in the electronic transaction. The solutions may be used for transaction authentication on industry standard e-commerce platforms, such as 3-D Secure compliant e-commerce platforms, and in non e-commerce environments such as mail order and telephone order or mobile devices where an authentication token or code can be used by the issuer to authenticate the cardholder.

[0015] TABLE 1 is a glossary of several of the terms, acronyms or abbreviations that are used in the description herein.

TABLE 1

AAV	Accountholder Authentication Value
Access control server (ACS)	The Access control server services to validate the enrollment of a specific cardholder account number (PAN) in 3-D Secure, as well as authenticate transactions.
Accountholder Authentication Value (AAV)	Cardholder authentication data required for electronic commerce transactions in which cardholder authentication has been successfully performed.
Cardholder Authentication Verification Value (CAVA)	Cardholder authentication data required by Visa for electronic commerce transactions in which cardholder authentication has been successfully performed.
Card Verification Code (CVC)	A two-part card security feature. CVC 1 is a 3-digit value encoded on tracks 1 and 2 in three contiguous positions in the "discretionary data" field of a magnetic stripe on a card. CVC 2 differs from CVC 1 and is indent-printed into the tamper-evident signature panel on the card. The CVC is intended to inhibit the alteration or misuse of card data and enhance the authentication of the card.
Message Authentication Code (MAC)	Cryptographically generated code that is a function of the message contents and a secret key shared by the message originator and the message recipient. This value, generated by the originator and verified by the recipient, enables the recipient to detect any alteration to the original message.
Secure Payment Application (SPA)	Specifications and algorithm for generating cardholder authentication data from merchant and issuer data components resulting in the creation of an AAV.
Universal Cardholder Authentication Field (UCAF)	The universal multi-purpose data transport infrastructure and defined field that is used to communicate and transport authentication information, including AAV, among various stakeholders in a transaction.

[0016] SPA 135 may include cryptography algorithms (namely "HMAC" and "CVC2" algorithms) that are used to generate Cardholder Authorization Verification Values (CAV) in formats that are compatible with 3-D Secure message formats.

[0017] SPA 135 may be integrated with any suitable authentication program that card issuers may choose or implement for authenticating their cardholders. The authentication programs may include smart card-based and password based solutions (e.g., FIG. 1 chip based authentication program 141 and 3-D Secure password-based authentication program 142). The authentication programs also may include other solutions based, for example, on PC identification.

[0018] An authentication program in which the inventive Secure Payment Applications (SPA 135) are utilized may be a solution or program for securing electronic transactions conducted on e-commerce platforms that are compliant with the 3-D Secure protocols. For this purpose SPA 135 is designed to use and generate authentication results in data format that can be readily used in 3-D Secure messages. In particular, a formatted data structure with defined fields and byte length may be used to facilitate transportation of authentication results in 3-D Secure messages.

[0019] For purposes of illustrating the application of SPA 135 in an exemplary authentication program 1000 (FIG. 1), a card payment transaction is used herein as an exemplary transaction. The participants in the card payment transaction may include a cardholder, an issuer, a merchant and an acquirer.

[0020] A cardholder is an authorized user of a payment card issued, for example, by a licensed member of authentication program 1000. The cardholder may use the issued payment card to pay for an on-line transaction with a merchant. Authentication program 1000 may be part of an authentication program or services provided by a third party (e.g., MasterCard) who, for example, can ensure that the cardholder's identity and presence is properly authenticated prior to the completion of the transaction.

[0021] An issuer is a member (e.g., a financial institution) that issues the payment card, which may be branded (e.g., MasterCard® and/or Maestro® cards). The issuer guarantees payment for an authorized transaction using the payment card in accordance with payment card brand regulations and local legislation. The issuer may be responsible for determining cardholder eligibility to participate in authentication program 1000, in addition to providing authentication services to merchants or other parties.

[0022] A merchant is a retailer, or any other person, firm, or corporation who, for example, pursuant to a merchant subscription agreement, agrees to accept issuers' payment cards for payment when they are properly presented. By subscribing to authentication program 1000, a merchant can offer a cardholder an authenticated electronic interaction over the Internet. A merchant who accepts payment cards may have a further relationship with an acquirer. Merchants who participate in authentication program 1000 may benefit in several ways including reduced fraud and dispute costs, increased transaction volume, protection from unauthorized card use, and access to the issuer's card base.

[0023] An acquirer is an entity who maintains relationships with merchants and acquires the data relating to a transaction from the merchant or card acceptor. The acquirer may be responsible for determining the merchant eligibility to participate in authentication program 1000.

[0024] As shown in FIG. 1, exemplary authentication program 1000, may be implemented as a secure e-commerce arrangement or platform with a number of layered components. The layered components include data transport layer 100, merchant requirement layer 120, authentication layer 130, and issuer platform 140. Authentication layer 130 relates to the Secure Payment Applications (SPA 135) that are deployed to authenticate a transaction or payment.

[0025] Data transport layer 100 relates to data collection and transport infrastructure that is used to communicate authentication information and results amongst the cardholder, issuer, merchant and acquirer. The data transport may, for example, be based on standardized data structures, architectures or mechanisms such as the Universal Cardholder Authentication Field (UCAF).

[0026] UCAF may in general be defined as a variable length, 32-character field with a flexible data structure that can be tailored to support the needs of a variety of issuer security and authentication approaches. FIG. 2 shows a generic structure of UCAF. A first control byte in UCAF contains a value that is specific to each security payment application or aspect. The remainder of the bytes in UCAF may include application specific data. An authentication or authorization provider may be responsible for assigning and managing UCAF control byte values and the structure of UCAF application specific data.

[0027] An exemplary control byte definition may be as follows:

Usage 3-D Secure SPA AAV for first and subsequent transactions
Base 64 Encoded Value j
Hexadecimal Value x'8C'

[0028] Another exemplary control byte definition may be as follows:

Usage 3-D Secure SPA AAV for attempts
Base64 Encoded Value j
Hexadecimal Value x'86'

[0029] In conventional UCAF implementations, the application specific data may be defined as binary data with a maximum length of 24 binary bytes - including the control byte. However, some transaction authorization networks limit the passing of binary data in authorization messages. Accordingly, all UCAF data generated by SPA 135 in authentication program 1000 may be Base 64 encoded prior to inclusion in an authorization message. The Base 64 encoding produces a character representation of the associated binary data. The resulting character representation is approximately a third larger than the binary equivalent. For this reason, the UCAF field may in general be defined with a maximum length of 32 characters. However for compatibility with 3-D Secure messaging in authentication program 1000, the UCAF field is limited to 28 characters in length.

[0030] The Accountholder Authentication Value (AAV) is a specific implementation of UCAE related to issuer authentication platforms that incorporate the SPA. AAV may be generated by the issuer and presented to the merchant for placement in a transaction authorization request (to the acquirer) upon successful authentication of the cardholder by the issuer. In the case of a chargeback or other potential dispute processing, AAV may be used to identify the processing parameters associated with the transaction. UCAF is the mechanism that is used to transmit the AAV from the merchant

to issuer for authentication purposes during the authorization process.

[0031] With renewed reference to FIG. 1, merchant requirement layer 110 relates to merchant capabilities for interacting with the other layers and the cardholder. Merchants participating in authentication program 1000 may implement application software capabilities (e.g., merchant plug-ins (MPI)) that are capable of processing 3-D Secure messages. A MPI may serve as the controlling application for the processing of 3-D Secure messages.

[0032] Authentication layer 130, which includes the inventive SPA 135, represents the authentication process or services (e.g., provided by or contracted for by an issuer) for verifying cardholder account ownership. An issuer using, for example, an access control server (ACS) may implement authentication layer 130/SPA135 in conjunction with an AAV validation server/process.

[0033] Exemplary e-commerce network components or entities that are involved in the authentication process may for purposes illustration be organized as belonging to issuer, acquirer or interoperability domains as shown in TABLE 2.

TABLE 2

Issuer Domain	Interoperability Domain	Acquirer Domain
Cardholder Browser Related Cardholder Software Enrollment Server Access Control Server AAV Validation Server/Process	Directory Server Certificate Authority	Merchant Plug-In Signature Validation Server

[0034] With reference to TABLE 2, the functionality present in the issuer domain includes a cardholder browser which can act as a conduit for transporting messages between the MPI (in the acquirer domain) and the access control server (in the issuer domain). Related cardholder software, for example, may include optional software to support use of smart cards. The enrollment server facilitates the process of cardholder enrollment for an issuer's implementation of 3-D Secure under authentication program 1000. The server may be used to perform initial cardholder authentication, as well as for administrative activities such as resets and viewing 3-D Secure payment history.

[0035] The access control server provides at least two basic functions during the course of an online purchase. First, ACS will verify whether a given cardholder account number is enrolled in program 1000. Secondly, ACS will conduct authentication processes for cardholder identification. For this purpose, ACS may operate in conjunction with or include an AAV validation server/process. This AAV validation server/process also may be used to validate cardholder authentication data received from merchants or acquirers.

[0036] The functionality in the acquirer domain may include the functions of a Merchant Plug-in (MPI) and a signature validation server. The MPI may create and process payer authentication messages and then returns control to merchant software for further authorization processing. MPI authentication processes may be invoked after a cardholder submits a purchase request, including the account number to be used for payment, but prior to obtaining authorization for the purchase. The signature validation server may be used to validate a digital signature on a purchase request that has been successfully authenticated by the issuer.

[0037] The functionality in the interoperability domain may include a directory server. The directory server may be a global directory sever, which provides centralized decision making capabilities to merchants enrolled in the in authentication program 1000. Based on the account number contained in a merchant verification request message, the directory may first determine whether the account number is part of a participating card issuer's card range. It may then direct eligible requests to the appropriate issuer's ACS for further processing. The interoperability domain also may include a suitable certificate authority for generating and distribute all private hierarchy end-entity and subordinate certificates, as required, to the various components and to other subordinate certificate authorities across all three domains.

[0038] The cardholder authentication process in program 1000 involves exchanges of messages and data across the three domains. The following exemplary 3-D Secure inter domain messages may be used step-by-step in the authentication process:

(1) Verification Request/Response

Message Pair: VEReq/VERes

[0039] A first step in the authentication process is to check or validate that the cardholder account number is part of the card range of an issuer participating in authentication program 1000. For this purpose, a Verification Request message VEReq, is sent from the MPI to the directory to check card range eligibility. If the specified account number is contained within an eligible card range in the directory, this message then may be forwarded from the directory to the issuer's ACS to further check if the specified account number is enrolled and/or activated by the issuer as a participant in program 1000.

[0040] The MPI may have an optional capability to locally cache card ranges by each participating issuer. In such

cases, Card Range Request/Response messages may be used by the MPI to request updates to the card range caches from the directory. For merchants who cache card ranges, the VEReq/VERes messages may not be utilized if the local cache indicates that the issuer is not enrolled in authentication program 1000.

(2) Payer Authentication Request/Response

Message Pair: PAREq/PARes

[0041] Once it has been determined that the cardholder is enrolled by an issuer or is an active participant in program 1000, the process of authenticating the specific cardholder further involves the specific card issuer. Payer Authentication Request/Response messages may be sent from the MPI to the specific card issuer's ACS to perform authentication. At this stage of the authentication process in program 1000, the cardholder may be presented with an authentication window. The authentication window may be displayed on the cardholder browser and be populated with relevant information by the issuer. The cardholder may be requested to enter a password, code or token for personal identification or authentication through the displayed authentication window. The specific card issuer's ACS may then use, for example, SPA 135 to authenticate the collected or entered information, and accordingly generate an Accountholder Authentication Value (AAV). The AAV is transported in the 3-D Secure PARes (Payer Authentication Response) message in a designated Cardholder Authentication Verification Value (CAVV) field in an UCAF.

[0042] CAAV is one of the data fields in the response portion of the message pair PAREq/PARes returned by the issuer to the requesting merchant. The issuer may place suitable digital signatures on their response. The merchant may, further, include the received AAV to an acquirer for forwarding to the issuer as part of a payment/transaction authorization request (See e.g., FIG. 4).

[0043] FIG. 3 schematically shows an exemplary card authentication process 300 for a cardholder transaction under authentication program 1000. For purposes of illustration, the description of process 300 assumes that cardholder 310 is enrolled by an issuer in authentication program 1000 and has obtained a password or code from the issuer to use while shopping online at participating merchants. Process 300 also assumes that all communication channels between components (e.g., cardholder 310, MPI 320, directory 330 and issuer ACS 340) are properly secured using the Secure Socket Layer protocol (SSL) links (e.g., SSL-1, SSI-2, SSI-3, SSI-4, SSL-5 and SSL-6).

[0044] In process 300 at step 351, cardholder 310 may shop at a merchant web site and, when ready to checkout, enter payment card information (e.g., the account number) and other information (e.g., shipping information) via link SSL-1. Once all of the payment and shipping information has been entered, the merchant may give cardholder 310 an opportunity by to review the purchase before submitting an order.

[0045] Next at step 352, MPI 320 queries directory 330 via link SSL-2 to verify the enrollment of cardholder 310 with a specific issuer using the verification request message VEReq. Step 352 optionally may be performed locally at MPI 320 via a local card directory cache. In responses to the VEReq message, directory 330 may determine that a particular issuer is participating, and accordingly forward a request via link SSL-3 to the particular issuer's ACS 340 to check on the current enrollment status of cardholder 310. The resulting responses may flow back over the same links (e.g., SSL-3 and SSL-2) to MPI 320. If ACS 340 indicates that cardholder 310 is enrolled in program 1000, MPI 320 may create a Payer Authentication Request message and send it to the cardholder's browser at step 354 via link SSL-4. Next at step 355, the cardholder's browser may redirect the message to the appropriate issuer's ACS 340 to initiate cardholder authentication. When ACS 340 receives the Payer authentication request message, it may cause a user authentication dialog to begin. As part of the user authentication dialog, ACS 340 may cause a separate interactive authentication window to be displayed to cardholder 310 to facilitate password, code or other data input by cardholder 310.

[0046] At step 356, ACS 340 (using SPA 135) may authenticate the password or code entered by cardholder 310. ACS 340 may construct a SPA AAV according to the authentication program provider's implementation of 3-D Secure. ACS 340 may build and digitally sign an appropriate payer authentication response message. The payer authentication response message is then returned (via link SSL-6) to MPI 320. The authentication window displayed to cardholder 320 may disappear at this point.

[0047] After cardholder authentication process 300 has been completed, the merchant may be required to pass the received SPA AAV to the acquirer via the UCAF field within an authorization message. The SPA AAV may then passed along from the acquirer to the issuer as part of conventional authorization message processing. When received by the issuer, the AAV can be validated as part of authorization request processing, and archived for use in resolving any cardholder disputes that may arise later on.

[0048] Standard 3-D Secure version 1.0.2 message formats and data formats may be used for all data communications between the involved parties or entities. Specifically, the SPA AAV that ACS 340 creates and returns back to the merchant for inclusion in UCAF messages is 28 characters long and contains a 20-byte field defined for 3-D Secure in base 64 encoding.

[0049] TABLE 3 shows an exemplary data structure or format of a 20-byte SPA AAV.

TABLE 3

Position	Field Name	Data Source: ACS	Length (Bytes)	Byte Number
1	Control Byte	The control byte is used to indicate the format and content of the associated AAV structure. A hexadecimal value x'8C' may indicate an AAV created as the result of a successful cardholder authentication. A hexadecimal value x'86' may indicate an AAV created as the result of attempts processing.	1	Byte 1
2	Hash of Merchant Name	The left most 8 bytes of an SHA-1 hash of the Merchant Name field from the PAREq.	8	Bytes 2-9
3	ACS Identifier	This data field may allow an issuer to use up to 256 different ACS facilities. Values for this field may defined based on the algorithm used to create the MAC: 0 - 7 Reserved for HMAC 8-15 Reserved for CVC2 16 - 255 - Reserved for future use	1	Byte 10
4	Authentication Method	Indicates how the cardholder was authenticated to the ACS: 0 = No Cardholder Authentication Performed (valid only for an AAV created using control byte value x'86' - Attempts processing.) 1 = Password 2 = Secret Key (e.g. Chip Card)	½ (4 bits)	Byte 11, 1st hex digit
5	BIN Key Identifier	Indicates which one of the possible 16 issuer-known secret keys for a given BIN range was used by the ACS identified by the ACS identifier to create the MAC.	½ (4 bits)	Byte 11, 2nd hex digit
6	Transaction Sequence Number	Unique number that can be used to identify the transaction within the ACS identified by the ACS identifier. Once the maximum value has been reached, the number should recycle back to 0. This number must be unique for every PAREs created for a given ACS identifier for a given issuer during the time that a chargeback can occur.	4 (8 hex digits)	Bytes 12-15
7	MAC	Message Authentication Code, created by ACS.	5	Bytes 16-20

[0050] Issuers providing both existing PC identification or other authentication solutions (e.g., FIG. 1) in addition to a 3-D Secure solution may differentiate between the AAV values they receive from different authentication solutions in the corresponding authorization message. The 20-byte AAV (e.g., TABLE 2) resulting from 3-D Secure compatible program 1000 may differ from common 28-byte AAV structures (i.e., in non 3-D Secure programs) in the following ways: The transaction amount and currency codes are not included in the 20-byte AAV as this information is included in the signed PAREs message; A merchant transaction stamp (MTS) is not included as a transaction identifier (XID), which is included in the signed PAREs message, can provide the same functionality. Further, the hash of the merchant name field is expanded. As a result, only minimal edits of the merchant name may now be required prior to creating the SHA-1 hash.

[0051] A merchant may not have to modify the control byte for subsequent authorizations (e.g. split shipments). For split shipments, the merchant may resend an original AAV generated by 3-D Secure compliant implementations of program 1000.

[0052] The control byte value in the 20-byte SPA AAV is based on the result of the cardholder authentication request (PAREq). This result may be indicated in the transaction status field of the Payer Authentication Response (PAREs) messages. TABLE 4 shows exemplary values of the transaction status field in a PAREs message.

TABLE 4

Transaction Status Field in PAREs	Control Byte Value in AAV (hexadecimal)	First AAV Byte Value After Base64 Encoding	Authentication Method Field in AAV
Y	x'8C'	j	Any defined value other than "No Cardholder Authentication Performed"
A	x'86'	h	Must be "No Cardholder Authentication Performed"
N	No AAV is to be generated for this status value	-	-
U	No AAV is to be generated for this status value	-	-

[0053] The merchant name contained in the PAREq message may be edited prior to creating the merchant name hash. The edits may specifically address Universal Transformation Format (UTF-8) encoding but also reference Unicode characters for other encoding types.

[0054] An edit may delete any UTF-8 byte sequence that does not have a Unicode representation. Such an edit may delete any UTF-8 bytes beginning with binary 1111 and all subsequent bytes beginning with binary 10

[0055] Another edit may delete any UTF-8 byte sequence or byte sequence with the following Unicode representation:

0000 through 001F (ASCII control characters;

007F through 00A0 (DEL and C1 control characters;

00AD (soft hyphen); and

2000 through 206F (General Punctuation).

[0056] Such an edit may delete the following UTF-8 bytes:

Hex 00 through 1F

Hex 7F

Hex C2 80 through C2 A0

Hex C2 AD

Hex E2 80 through E2 81 AF

[0057] Still another edit may delete any leading or trailing spaces (e.g., UTF-8 bytes Hex 20).

[0058] In the case of a chargeback or other potential dispute processing, the 20-byte AAV may be used to identify the processing parameters associated with the transaction. Among other things, the AAV field values may identify:

- The physical location of where the transaction was processed.
- The sequence number that can be used to positively identify the transaction within the universe of transactions for that location
- The secret key used to create the MAC, which not only ensures AAV data integrity but also binds the entire AAV structure to a specific PAN for implementations of 3-D Secure.

[0059] Field dependencies in the AAV may be established to ensure proper identification of the processing parameters. These field dependencies may be considered when building or configuring issuer ACS installations. For every ACS

configured with the same ACS identifier:

- The BIN Key Identifier field must be unique for each BIN range processed by the identified ACS. Most issuers may use a common set of keys for most or all of their BIN ranges. However, this configuration allows for flexibility in a choice of software vendors that support or issuers that require the use a separate set of keys.
- The Transaction Sequence Number field must be unique for each AAV generated by the identified ACS within the time that a chargeback can occur.

[0060] ACS installations that have the capability to share BIN keys and a common set of transaction sequence numbers across multiple logical installations or physical machines may be advantageously configured to use the same ACS identifier. Alternatively, a separate ACS identifier or set of ACS identifiers may be required for each installation. In cases where one ACS facility serves multiple issuers, more than one issuer may share an ACS identifier. In these cases, the BIN field value for the associated transaction may become a determining factor in interpreting the field content location.

[0061] Particular algorithms may be utilized in SPA 135 to create a Merchant Authentication code (MAC) value. For example, an "HMAC" algorithm or an "CVC2" algorithm may be used by the ACS identified by the ACS identifier sub field to create MAC values.

[0062] The HMAC algorithm generates a MAC value cryptographically based on a secret key identified by the BIN Key Identifier sub field. This secret key is shared with the issuer and binds the cardholder account number to the AAV by the concatenation of the following data:

- The account number, as received by the ACS in the Verification Request (VEReq) message that corresponds to the current Payer Authentication Request (PAREq) message. The account number may be represented as binary-coded decimal, left justified and padded on the right with hexadecimal 'F's to a length of 20 digits (10 total bytes).
- The left-most 15 bytes, fields 1 through 6, of the AAV being constructed.

[0063] The secret key length may be optionally selected be a minimum of 128 bits (16 bytes) and a maximum of 192 bits (24 bytes). Any intervening key size (e.g. 160 bits) may be acceptable. The actual key length size used may be independently selected by each implementation. The MAC field within the SPA AAV defined for a 3-D secure authentication program (e.g., Program 1000) may be populated with the left-most 40 bits (5 binary bytes) of the cryptographic result obtained by applying algorithm HMAC.

[0064] EXAMPLES 1 and 2 illustrate the application of the HMAC algorithm using 20 byte and 16 byte keys, respectively, to generate SPA AAV values.

EXAMPLE 1 (20 Byte Key)

[0065]

Assumed account number: 5432 109876543210
Assumed Merchant Name: SPA Merchant, Inc. (All ASCII characters, and no editing required)
Assumed AAV control byte = 8C
First 8 bytes, SHA-1 hash of Merchant Name = 7CA7 FBB6 058B 5114
Assumed ACS Id = 01
Assumed Authentication Method = 1 (Password)
Assumed BIN Key Id = I
Assumed Transaction Sequence Number = 0000002F
Assumed key (20 Bytes) =
QBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQBQB

[0066] Therefore SHA-1HMAC is based on
5432 109876543210 FFFF 8C 7CA7FBB6058B5114 0111 0000002F

[0067] This produces a MAC whose first 5 bytes are:

3547 BAIE FF

[0068] Therefore, the complete AAV in hex is:

EP 1 636 680 B1

8C 7CA7FBB6058B5114 0111 0000002F 3547BAIEFF

after Base-64-encoding, this is:

jHyn+7YFiEUAREAAAAvNUe6Hv8=

EXAMPLE 2 (16 Byte Key)

[0069]

Assumed account number: 5432 109876543210
 Assumed Merchant Name: SPA Merchant, Inc. (All ASCII characters, and no editing required)
 Assumed AA V control byte = 8C
 First 8 bytes, SHA-1 hash of Merchant Name = 7CA7 FBB6 058B 5114
 Assumed ACS Id = 01
 Assumed Authentication Method = 1 (Password)
 Assumed BIN Key Id = 1
 Assumed Transaction Sequence Number = 0000002F
 Assumed key (16 Bytes) = 00112233445566778899AABBCCDDEEFF

Therefore SHA-1HMAC is based on

5432 109876543210 FFFF 8C 7CA7FBB6058B5114 0111 0000002F

This produces a MAC whose first 5 bytes are:

EB27 FC7F AB

Therefore the complete AAV in hex is:

8C 7CA7FBB6058B5114 0111 0000002F EB27FC7FAB

after Base-64-encoded, this is:

jHyn+ 7YFi1 EUAREAAAA v6yf8f6s=

[0070] The CVC2 algorithm also Cryptographically creates the MAC field values. In contrast to the HMAC algorithm, which uses one key, the CVC2 algorithm use two 64 bit DES keys identified by the BIN Key Identifier sub field. In the CVC2 algorithm, all encryption and decryption steps may use Electronic Code Book (ECB) form of DES.

[0071] The CVC2 algorithm generates a three digit 3 digit CVC2 value. The input data which is processed by CVC2 algorithm for generating this three digit 3 digit CVC2 value is shown in TABLE 5.

TABLE 5

CVC2 Field Name	MAC Field Name	Data Source	Length (Digits)
Primary Account Number	Primary Account Number	The account number, as presented in the Verification Request (VEReq) message	13 to 19 digits
Card Expiration Date	Transaction Sequence Number	Convert Transaction Sequence Number, as contained in AAV, to BCD decimal equivalent. Populate this field with the 4 least significant digits. Any value less than 4 digits should be right justified in the field and padded with binary zeros to 4 digits.	4 digits
Service Code	Authentication Method	Authentication Method as contained in the AAV. If the value of the Authentication Method sub field is greater than 9, subtract 10 to obtain the digit to be used.	1 digit

EP 1 636 680 B1

(continued)

CVC2 Field Name	MAC Field Name	Data Source	Length (Digits)
	Control Byte	Convert Control Byte, as contained in the AAV, to BCD decimal equivalent. Populate this field with the 2 least significant digits.	2 digits

[0072] The resultant three digit CVC2 value is converted to binary coded decimal form and populated in the left most two bytes of the MAC sub field with a leading binary 0 used to fill the first unused half byte. The remaining three bytes of the MAC sub field may be filled with binary zeros. For example: CVC2 = 123 MAC sub field = 0123000000 (10 total digits).

[0073] EXAMPLE 3 and TABLE 6 illustrate the application of the CVC2 algorithm and the process steps involved in application of the algorithm to generate SPA AAV values.

EXAMPLE 3

[0074]

Assumed account number: 5432109876543210

Assumed Merchant Name: SPA Merchant, Inc. (All ASCII characters, and no editing required)

Assumed AA V control byte = 8C

First 8 bytes, SHA-1 hash of Merchant Name = 7CA7 FBB6 058B 5114

Assumed ACS Id = 7

Assumed Authentication Method = 1 (Password)

Assumed BIN Key Id = 1

Assumed Transaction Sequence Number = 0000002F

Key A = 0011223344556677 Key B = 8899AABBCCDDEEFF

Therefore, the CVC2 algorithm calculation is based on

Account Number = 5432109876543210 Expiration Date = 0047

Service Code = 140

This produces a CVC2 three digit value = 439 (see Table 6 for calculation):

Based on the calculated CVC2 value, the MAC field = 0439000000

Therefore, the complete AA V in hex is:

8C 7CA7FBB6058B5114 01 11 0000002F 0439000000

Base-64-encoded, this is:

jHyn+7YFi1 EUAREAAAAvBDkAAAA=

The processing or calculation steps that are used in EXAMPLE 3 are shown in TABLE 6

TABLE 6

Step	Processing Step	Example
1.	Construct string of bits by concatenating (left to right) the right-most 4 bits of each character of the specified data elements.	54321098765432100047140
2.	Place the results in a 128-bit field, padding on the right with binary zeros to fill all remaining bits. Split the 128-bit block into 2 64-bit blocks.	54321098765432100047140000000000 Block 1 = 5432109876543210 Block 2 = 0047140000000000

(continued)

Step	Processing Step	Example
3.	Encrypt Block 1 using Key A	Block 1 = 5432109876543210 Key A = 0011223344556677 Result = 44DD7C814CC62702
4.	XOR the results of Step 3 with Block 2. Encrypt this value using Key A.	Block 2 = 0047140000000000 Step 3 = 44DD7C814CC62702 Result = 449A68814CC62702 Result = 449A68814CC62702
5.	Decrypt the result of step 4 using Key B.	Step 4 = 449A68814CC62702 Result = 8899AABBCCDDEEF F KeyB = KeyB = 8899AABBCCDDEEF F Result = 191DCA3149A5BD51
6.	Encrypt the result of step 5 using Key A.	Step 5 = 191DCA3149A5BD51 Result = 0011223344556677 Key A = 0011223344556677 Result = 4F AB392CE3C98B41
7.	From the result of step 6, going from left to right, extract all numeric digits (0-9); left justify these digits in a 16-position field	439239841
8.	From the result of step 6, going from left to right, extract all characters of A through F. To compensate for decimals, subtract 10 from each extracted digit.	012421
9.	Concatenate the digits from step 7 to the right of the digits extracted in step 8.	439239841012421
10.	Select from the first three left-most digits of the CVC.	439

[0075] As defined by the 3-D Secure protocol, all PAREs messages returned to the merchant are digitally signed by the associated cardholder's issuer ACS. The merchant may be required to validate the digital signature prior to extracting the SPA AAV from the PAREs message for inclusion in an authorization request sent to the acquirer. If an issuer supports both implementation of 3-D Secure and other authentication platforms (e.g., PC Authentication platforms) it may be necessary to distinguish between the two authentication platforms during processing of the authorization request message. This may be accomplished in one of two ways:

1. The first base64 encoded character is

- a. "j" or "h" for the SPA AAV within the defined implementation of 3-D Secure
- b. "g" or "A" for the PC Authentication SPA AAV

2. The control byte, converted to binary, is either

- a. hexadecimal 8C or hexadecimal 86 for the AAV defined for MasterCard's implementation of 3-D Secure
- b. hexadecimal 82 or hexadecimal 02 for the PC Authentication SPA AA V.

[0076] Each issuer participating in program 1000 may assure that the ACS identifier sub field is appropriately set to indicate the algorithm used to create the MAC. Failure to set this indicator correctly may result in improper validations during the transaction/payment authorization process.

[0077] Although the present invention has been described in connection with specific exemplary embodiments, it should be understood that various changes, substitutions, and alterations apparent to those skilled in the art could be

made to the disclosed embodiments without departing from the scope of the invention as defined in the appended claims.

Claims

1. A system for authenticating a cardholder transaction with a merchant on an electronic network, the system comprising:
 - an issuer platform layer including at least one 3-D Secure authentication program;
 - a merchant plug-in, "MPI";
 - a secure payment algorithm, "SPA"; and
 - a data transport layer,

wherein the issuer platform comprises an access control server, "ACS", that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value, "AAV", and conveys the AAV through the data transport layer to the MPI,

wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code, "MAC".
2. The system of claim 1 wherein the AAV is a formatted data structure that is Base 64 encoded.
3. The system of claim 1, wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and a plurality of the fields of the bytes of the AAV excluding bytes that represent the MAC, and wherein a portion of the encryption result forms the MAC bytes in the AAV.
4. The system of claim 1, wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a pair of secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field, and uses the result to populate two bytes of the MAC.
5. The system of claim 4 wherein the pair of secret keys A and B are 64-bit Data Encryption Standard, "DES", keys.
6. The system of claim 1 wherein the ACS is configured to generate an AAV in response to a payment authentication request message from the MPI to the ACS.
7. The system of claim 1, which is configured to transport the AAV in a payment authentication response message from the ACS.
8. The system of claim 7 wherein the ACS is further configured to place a digital signature on the payment authentication response message.
9. The system of claim 1 wherein the MPI is configured to verify the digital signature on a received payment authentication response message.
10. The system of claim 1 wherein the MPI is configured to extract the MAC fields included in a payment authentication response message from the ACS and to place the extracted MAC in a payment authorization request message to a third party.
11. A data structure for conveying cardholder transaction authentication information amongst stakeholders in a 3-D Secure environment, the data structure comprising 20 bytes of Base 64 encoded characters, wherein the first byte is a control byte, bytes 2-9 represent a hash of a merchant name, byte 10 identifies an Access control server, ACS, that authenticates the cardholder transaction by an authentication method, byte 11 identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication Code, "MAC", bytes 12-15 represent a transaction sequence number identifying a transaction number processed by the ACS, and bytes 16-20 represent the MAC.

12. The data structure of claim 11 wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number and a plurality of the fields of bytes 1-15 of the data structure, and wherein a single key identified in byte 11 is used for encryption.

13. The data structure of claim 11 wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number, card expiration date and service code, and wherein a pair of keys A and B that are identified in byte 11 is used for encryption.

14. The data structure of claim 13 wherein a three-digit encryption result is used to populate two bytes of the MAC bytes 16-20.

15. The data structure of claim 13 wherein the pair of secret keys A and B are 64 bit Data Encryption Standard, "DES", keys.

16. A method for authenticating a cardholder transaction with a merchant on an electronic network in an 3-D Secure environment, the method comprising:

using an Access control server, "ACS", to process cardholder and transaction information to authenticate the cardholder by an authentication method;
 deploying a secure payment algorithm, "SPA", to generate an Accountholder Authentication Value, "AAV", to represent the authentication results, and
 transporting the AAV in 3-D Secure messages to the merchant, wherein the AAV is a formatted data structure that has a length of at most 20 bytes, including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that include a merchant authentication code, "MAC", and bytes that identify secret cryptographic keys that are used by the SPA to generate MAC.

17. The method of claim 16 wherein the AAV is a formatted data structure that is Base 64 encoded.

18. The method of claim 16 wherein deploying a SPA comprises:

using a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and at least portions of the bytes of the AAV excluding bytes that represent the MAC; and
 assigning a portion of the encryption result to the MAC bytes in the AAV.

19. The method of claim 16 wherein deploying a SPA comprises:

using a pair of pair secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field; and
 assigning the result to populate two bytes of the MAC.

20. The method of claim 17 wherein the pair of secret keys A and B are 64 bit Data Encryption Standard, "DES", keys.

21. The method of claim 16 wherein transporting the AAV in 3-D Secure messages to the merchant comprises transporting the AAV in a payment authentication response message that is digitally signed by the ACS.

22. The method of claim 21, further comprising:

first, verification by the merchant of the digital signature on a received payment authentication response message; and
 next, extraction of the MAC fields from the received payment authentication response message by the merchant.

Patentansprüche

1. System zum Authentifizieren einer Transaktion eines Karteninhabers mit einem Händler in einem elektronischen Netzwerk, wobei das System umfasst:

eine Ausstellerplattformschicht (issuer platform layer), die mindestens ein 3-D Secure-Authentifizierungspro-

gramm aufweist;
 ein Händler-Plug-in (merchant plug-in, MPI);
 einen Algorithmus für sichere Zahlungen (secure payment algorithm, SPA) sowie eine Datentransportschicht,
 wobei die Ausstellerplattform einen Zugangskontrollserver (access control server, ACS) umfasst, der den SPA
 verwendet, um Transaktions- und Karteninhaberinformationen zur Authentifizierung mithilfe eines Authentifi-
 zierungsverfahrens zu verarbeiten und einen Kontoinhaber-Authentifizierungswert (accountholder authentica-
 tion value, AAV) zu erzeugen, und den AAV durch die Datentransportschicht zu dem MPI weiterleitet,
 wobei es sich bei dem AAV um eine formatierte Datenstruktur handelt, die kompatibel mit 3-D Secure-Nach-
 richtenprotokollen ist, wobei die formatierte Datenstruktur eine Länge von höchstens 20 Bytes aufweist, darunter
 Bytes, die einen Hash-Wert des Händlernamens bezeichnen, Bytes, die den ACS bezeichnen, Bytes, die das
 Authentifizierungsverfahren bezeichnen, Bytes, die geheime kryptografische Schlüssel bezeichnen, und Bytes,
 die einen Händler-Authentifizierungscode (merchant authentication code, MAC) aufweisen.

2. System nach Anspruch 1, wobei es sich bei dem AAV um eine formatierte Datenstruktur handelt, die Base-64-codiert ist.
3. System nach Anspruch 1, wobei der SPA einen Verschlüsselungsalgorithmus zum Erzeugen des MAC umfasst, wobei der Verschlüsselungsalgorithmus einen geheimen Schlüssel verwendet, der in dem AAV bezeichnet ist, um eine Verkettung aus der Kontonummer des Karteninhabers und mehreren der Felder der Bytes des AAV zu verschlüsseln, mit Ausnahme von Bytes, die den Mac repräsentieren, und wobei ein Teil des Verschlüsselungsergebnisses die MAC-Bytes in dem AAV bildet.
4. System nach Anspruch 1, wobei der SPA einen Verschlüsselungsalgorithmus zum Erzeugen des MAC umfasst, wobei der Verschlüsselungsalgorithmus ein Paar geheime Schlüssel A und B verwendet, die in dem AAV bezeichnet sind, um eine Verkettung aus der Kontonummer des Karteninhabers, dem Kartenablaufdatum und dem Servicecode zu verschlüsseln, um ein dreistelliges CVC2-Feld zu erzeugen, und das Ergebnis verwendet, um zwei Bytes des MAC zu füllen (populate).
5. System nach Anspruch 4, wobei es sich bei dem Paar geheime Schlüssel A und B um 64-Bit-DES-Schlüssel (64-bit data encryption standard keys) handelt.
6. System nach Anspruch 1, wobei der ACS derart konfiguriert ist, dass er einen AAV als Reaktion auf eine Zahlungsauthentifizierungs-Anforderungsnachricht von dem MPI an den ACS erzeugt.
7. System nach Anspruch 1, das derart konfiguriert ist, dass es den AAV in einer Zahlungsauthentifizierungs-Antwortnachricht von dem ACS transportiert.
8. System nach Anspruch 7, wobei der ACS ferner derart konfiguriert ist, dass er eine digitale Signatur in der Zahlungsauthentifizierungs-Antwortnachricht platziert.
9. System nach Anspruch 1, wobei das MPI derart konfiguriert ist, dass es die digitale Signatur in einer empfangenen Zahlungsauthentifizierungs-Antwortnachricht verifiziert.
10. System nach Anspruch 1, wobei das MPI derart konfiguriert ist, dass es die in einer Zahlungsauthentifizierungs-Antwortnachricht von dem ACS enthaltenen MAC-Felder extrahiert und den extrahierten MAC in einer Zahlungsautorisierung-Anforderungsnachricht an einen Dritten platziert.
11. Datenstruktur zum Weiterleiten von Karteninhaber-Transaktions-Authentifizierungsinformationen unter Beteiligten (stakeholders) in einer 3-D Secure-Umgebung, wobei die Datenstruktur 20 Bytes Base-64-codierte Zeichen umfasst, wobei das erste Byte ein Steuer-Byte ist, die Bytes 2 bis 9 einen Hash-Wert eines Händlernamens repräsentieren, Byte 10 einen Zugangskontrollserver, ACS, bezeichnet, der die Transaktion eines Karteninhabers mithilfe eines Authentifizierungsverfahrens authentifiziert, Byte 11 das Authentifizierungsverfahren und die geheimen Verschlüsselungsschlüssel bezeichnet, die von dem ACS zum Erzeugen eines Händler-Authentifizierungscode, MAC, verwendet werden, die Bytes 12 bis 15 eine Transaktionssequenznummer repräsentieren, die eine von dem ACS verarbeitete Transaktionsnummer bezeichnet, und die Bytes 16 bis 20 den MAC repräsentieren.
12. Datenstruktur nach Anspruch 11, wobei der MAC Teile einer Verschlüsselung einer Verkettung aus der Kontonummer des Karteninhabers und mehreren der Felder der Bytes 1 bis 15 der Datenstruktur umfasst, und wobei ein einzelner

in Byte 11 bezeichneter Schlüssel zur Verschlüsselung verwendet wird.

13. Datenstruktur nach Anspruch 11, wobei der MAC Teile einer Verschlüsselung einer Verkettung aus der Kontonummer des Karteninhabers, dem Kartenablaufdatum und dem Servicecode umfasst, und wobei ein Paar Schlüssel A und B, die in Byte 11 bezeichnet sind, zur Verschlüsselung verwendet wird.

14. Datenstruktur nach Anspruch 13, wobei ein dreistelliges Verschlüsselungsergebnis zum Füllen von zwei Bytes der MAC-Bytes 16 bis 20 verwendet wird.

15. Datenstruktur nach Anspruch 13, wobei es sich bei dem Paar geheime Schlüssel A und B um 64-Bit-DES-Schlüssel (64-bit data encryption Standard keys) handelt.

16. Verfahren zum Authentifizieren einer Transaktion eines Karteninhabers mit einem Händler in einem elektronischen Netzwerk in einer 3-D Secure-Umgebung, wobei das Verfahren umfasst:

Verwenden eines Zugangskontrollservers, ACS, zum Verarbeiten von Karteninhaber- und Transaktionsinformationen, um den Karteninhaber mithilfe eines Authentifizierungsverfahrens zu authentifizieren;
Bereitstellen eines Algorithmus für sichere Zahlungen, SPA, um einen Kontoinhaber-Authentifizierungswert, AAV, zu erzeugen, um die Ergebnisse der Authentifizierung zu repräsentieren, und
Transportieren des AAV in 3-D Secure-Nachrichten zu dem Händler, wobei der AAV eine formatierte Datenstruktur ist, die eine Länge von höchstens 20 Bytes aufweist, darunter Bytes, die einen Hash-Wert des Händlernamens bezeichnen, Bytes, die den ACS bezeichnen, Bytes, die das Authentifizierungsverfahren bezeichnen, Bytes, die einen Händler-Authentifizierungscode, MAC, aufweisen, und Bytes, die geheime kryptografische Schlüssel bezeichnen, die von dem SPA zum Erzeugen des MAC verwendet werden.

17. Verfahren nach Anspruch 16, wobei es sich bei dem AAV um eine formatierte Datenstruktur handelt, die Base-64-codiert ist.

18. Verfahren nach Anspruch 16, wobei ein Bereitstellen eines SPA umfasst: Verwenden eines in dem AAV bezeichneten geheimen Schlüssels zum Verschlüsseln einer Verkettung aus der Kontonummer des Karteninhabers und mindestens Teilen der Bytes des AAV, mit Ausnahme von Bytes, die den MAC repräsentieren, und
Zuweisen eines Teils des Verschlüsselungsergebnisses zu den MAC-Bytes in dem AAV.

19. Verfahren nach Anspruch 16, wobei ein Bereitstellen eines SPA umfasst: Verwenden eines in dem AAV bezeichneten Paares geheime Schlüssel A und B zum Verschlüsseln einer Verkettung aus der Kontonummer des Karteninhabers, dem Kartenablaufdatum und dem Servicecode, um ein dreistelliges CVC2-Feld zu erstellen, und
Zuweisen des Ergebnisses, um zwei Bytes des MAC zu füllen.

20. Verfahren nach Anspruch 17, wobei es sich bei dem Paar geheime Schlüssel A und B um 64-Bit-DES-Schlüssel (64-bit data encryption standard keys) handelt.

21. Verfahren nach Anspruch 16, wobei ein Transportieren des AAV in 3-D Secure-Nachrichten an den Händler ein Transportieren des AAV in einer Zahlungsauthentifizierungs-Antwortnachricht umfasst, die von dem ACS digital signiert ist.

22. Verfahren nach Anspruch 21, das ferner umfasst:

als Erstes eine Verifizierung der digitalen Signatur in einer empfangenen Zahlungsauthentifizierungs-Antwortnachricht durch den Händler und
als Nächstes ein Extrahieren der MAC-Felder aus der empfangenen Zahlungsauthentifizierungs-Antwortnachricht durch den Händler.

Revendications

1. Système permettant d'authentifier une transaction de titulaire de carte avec une entité commerciale sur un réseau électronique, le système comprenant :

une couche de plateforme d'émetteur incluant au moins un programme d'authentification « 3-D Secure » ;
un module d'extension d'entité commerciale, « MPI » ;
un algorithme de paiement sécurisé, « SPA » ; et
une couche de transport de données ;

- 5 dans lequel la plate-forme d'émetteur comprend un serveur de commande d'accès, « ACS », qui utilise l'algorithme SPA en vue de traiter des informations de transaction et de titulaire de carte à des fins d'authentification par un procédé d'authentification, et de générer une valeur d'authentification de titulaire de compte, « AAV », et achemine la valeur AAV à travers la couche de transport de données vers le module MPI ;
- 10 dans lequel la valeur AAV correspond à une structure de données formatée compatible avec des protocoles de messages « 3-D Secure », dans lequel la structure de données formatée présente une longueur de 20 octets tout au plus, incluant des octets qui identifient un hachage du nom de l'entité commerciale, des octets qui identifient le serveur ACS, des octets qui identifient le procédé d'authentification, des octets qui identifient des clés cryptographiques secrètes, et des octets qui incluent un code d'authentification d'entité commerciale, « MAC ».
- 15 2. Système selon la revendication 1, dans lequel la valeur AAV correspond à une structure de données formatée laquelle est codée en base 64.
- 20 3. Système selon la revendication 1, dans lequel l'algorithme SPA comprend un algorithme de chiffrement destiné à générer le code MAC, dans lequel l'algorithme de chiffrement utilise une clé secrète identifiée dans la valeur AAV en vue de chiffrer une concaténation du numéro de compte du titulaire de carte et d'une pluralité des champs des octets de la valeur AAV, à l'exclusion des octets qui représentent le code MAC, et dans lequel une partie du résultat de chiffrement forme les octets de code MAC dans la valeur AAV.
- 25 4. Système selon la revendication 1, dans lequel l'algorithme SPA comprend un algorithme de chiffrement pour générer le code MAC, dans lequel l'algorithme de chiffrement utilise une paire de clés secrètes A et B, qui sont identifiées dans la valeur AAV, en vue de chiffrer une concaténation du numéro de compte du titulaire de carte, d'une date d'expiration de la carte et d'un code de service, afin de générer un champ CVC2 à trois chiffres, et utilise le résultat pour remplir deux octets du code MAC.
- 30 5. Système selon la revendication 4, dans lequel la paire de clés secrètes A et B correspond à des clés à norme de chiffrement de données, « DES », de 64 bits.
- 35 6. Système selon la revendication 1, dans lequel le serveur ACS est configuré de manière à générer une valeur AAV en réponse à un message de demande d'authentification de paiement du module MPI au serveur ACS.
7. Système selon la revendication 1, lequel est configuré de manière à transporter la valeur AAV dans un message de réponse d'authentification de paiement en provenance du serveur ACS.
- 40 8. Système selon la revendication 7, dans lequel le serveur ACS est en outre configuré de manière à placer une signature numérique sur le message de réponse d'authentification de paiement.
9. Système selon la revendication 1, dans lequel le module MPI est configuré de manière à vérifier la signature numérique sur un message de réponse d'authentification de paiement reçu.
- 45 10. Système selon la revendication 1, dans lequel le module MPI est configuré de manière à extraire les champs de code MAC, inclus dans un message de réponse d'authentification de paiement, du serveur ACS, et à placer le code MAC extrait dans un message de demande d'autorisation de paiement à un tiers.
- 50 11. Structure de données pour acheminer des informations d'authentification de transaction de titulaire de carte entre des parties prenantes dans un environnement « 3-D Secure », la structure de données comprenant 20 octets de caractères codés en base 64, dans laquelle le premier octet est un octet de commande, les octets 2 à 9 représentent un hachage d'un nom d'entité commerciale, l'octet 10 identifie un serveur de commande d'accès, ACS, qui authentifie la transaction de titulaire de carte par le biais d'un procédé d'authentification, l'octet 11 identifie le procédé d'authentification et les clés de chiffrement secrètes qui sont utilisées par le serveur ACS en vue de générer un code d'authentification d'entité commerciale, « MAC », les octets 12 à 15 représentent un numéro de séquence de transaction identifiant un numéro de transaction traité par le serveur ACS, et les octets 16 à 20 représentent le code MAC.
- 55

12. Structure de données selon la revendication 11, dans laquelle le code MAC comprend des parties d'un chiffrement d'une concaténation du numéro de compte du titulaire de carte et d'une pluralité des champs d'octets 1 à 15 de la structure de données, et dans laquelle une clé unique identifiée dans l'octet 11 est utilisée à des fins de chiffrement.

13. Structure de données selon la revendication 11, dans laquelle le code MAC comprend des parties d'un chiffrement d'une concaténation du numéro de compte du titulaire de carte, d'une date d'expiration de la carte et d'un code de service, et dans laquelle une paire de clés A et B qui sont identifiées dans l'octet 11 est utilisée à des fins de chiffrement.

14. Structure de données selon la revendication 13, dans laquelle un résultat de chiffrement à trois chiffres est utilisé en vue de remplir deux octets des octets de code MAC 16 à 20.

15. Structure de données selon la revendication 13, dans laquelle la paire de clés secrètes A et B correspond à des clés à norme de chiffrement de données « DES », de 64 bits.

16. Procédé d'authentification d'une transaction de titulaire de carte avec une entité commerciale sur un réseau électronique dans un environnement « 3-D Secure », le procédé comprenant les étapes ci-dessous consistant à :

utiliser un serveur de commande d'accès, « ACS », en vue de traiter des informations de transaction et de titulaire de carte afin d'authentifier le titulaire de carte par le biais d'un procédé d'authentification ;
déployer un algorithme de paiement sécurisé, « SPA », en vue de générer une valeur d'authentification de titulaire de compte, « AAV », afin de représenter les résultats d'authentification ; et
transporter la valeur AAV dans des messages « 3-D Secure » vers l'entité commerciale, dans lequel la valeur AAV correspond à une structure de données formatée qui présente une longueur de 20 octets tout au plus, incluant des octets qui identifient un hachage du nom de l'entité commerciale, des octets qui identifient le serveur ACS, des octets qui identifient le procédé d'authentification, des octets qui incluent un code d'authentification d'entité commerciale, « MAC », et des octets qui identifient des clés cryptographiques secrètes qui sont utilisées par l'algorithme SPA en vue de générer le code MAC.

17. Procédé selon la revendication 16, dans lequel la valeur AAV correspond à une structure de données formatée qui est codée en base 64.

18. Procédé selon la revendication 16, dans lequel le déploiement d'un algorithme SPA comprend les étapes ci-dessous consistant à :

utiliser une clé secrète identifiée dans la valeur AAV en vue de chiffrer une concaténation du numéro de compte du titulaire de carte et d'au moins des parties des octets de la valeur AAV, à l'exclusion des octets qui représentent le code MAC ; et
affecter une partie du résultat de chiffrement aux octets de code MAC dans la valeur AAV.

19. Procédé selon la revendication 16, dans lequel le déploiement d'un algorithme SPA comprend les étapes ci-dessous consistant à :

utiliser une paire de clés secrètes A et B qui sont identifiées dans la valeur AAV en vue de chiffrer une concaténation du numéro de compte du titulaire de carte, d'une date d'expiration de la carte et d'un code de service afin de générer un champ CVC2 à trois chiffres ; et
affecter le résultat en vue de remplir deux octets du code MAC.

20. Procédé selon la revendication 17, dans lequel la paire de clés secrètes A et B correspond à des clés à norme de chiffrement de données, « DES », de 64 bits.

21. Procédé selon la revendication 16, dans lequel l'étape de transport de la valeur AAV dans des messages « 3-D Secure » vers l'entité commerciale comprend l'étape consistant à transporter la valeur AAV dans un message de réponse d'authentification de paiement qui est signé numériquement par le serveur ACS.

22. Procédé selon la revendication 21, comprenant en outre :

en premier lieu, la vérification, par l'entité commerciale, de la signature numérique sur un message de réponse

EP 1 636 680 B1

d'authentification de paiement reçu ; et
ensuite, l'extraction des champs de code MAC du message de réponse d'authentification de paiement reçu,
par l'entité commerciale.

5

10

15

20

25

30

35

40

45

50

55

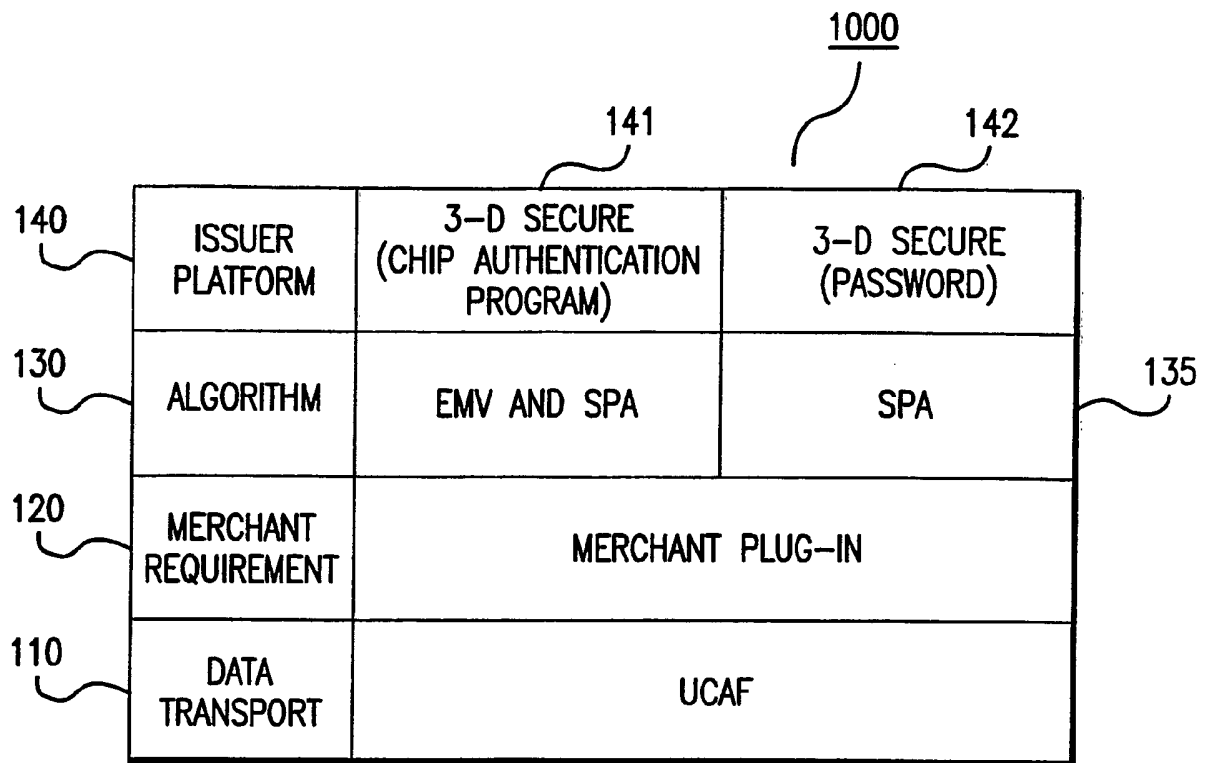


FIG. 1

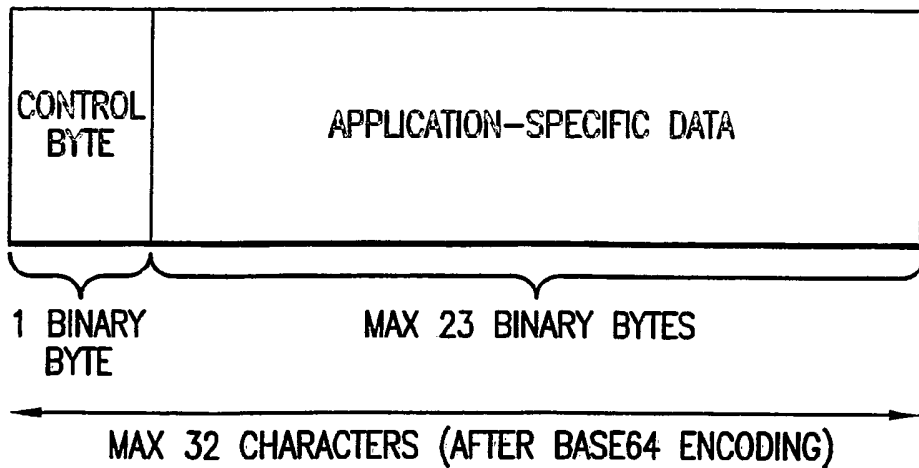


FIG. 2

SAMPLE CARDHOLDER AUTHENTICATION PROCESS

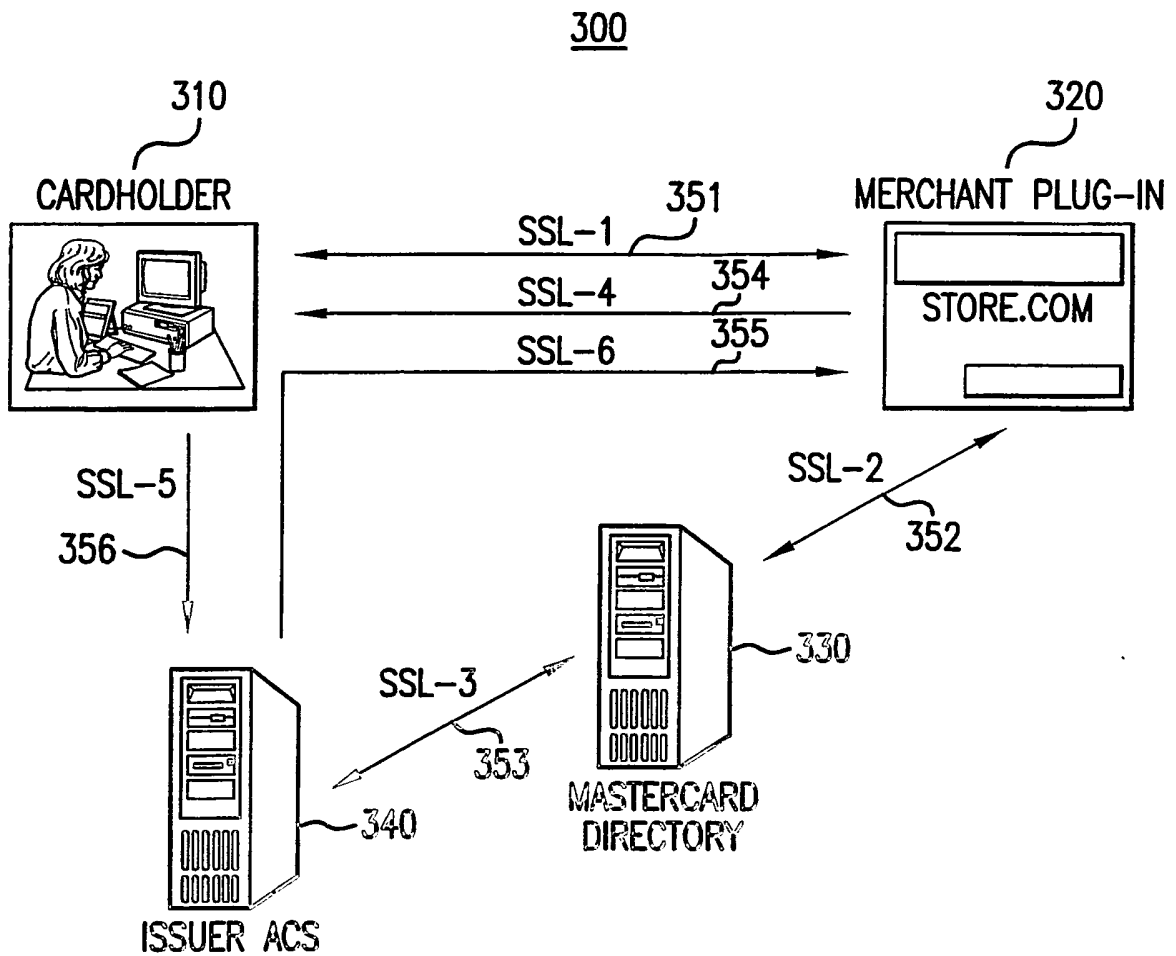


FIG.3

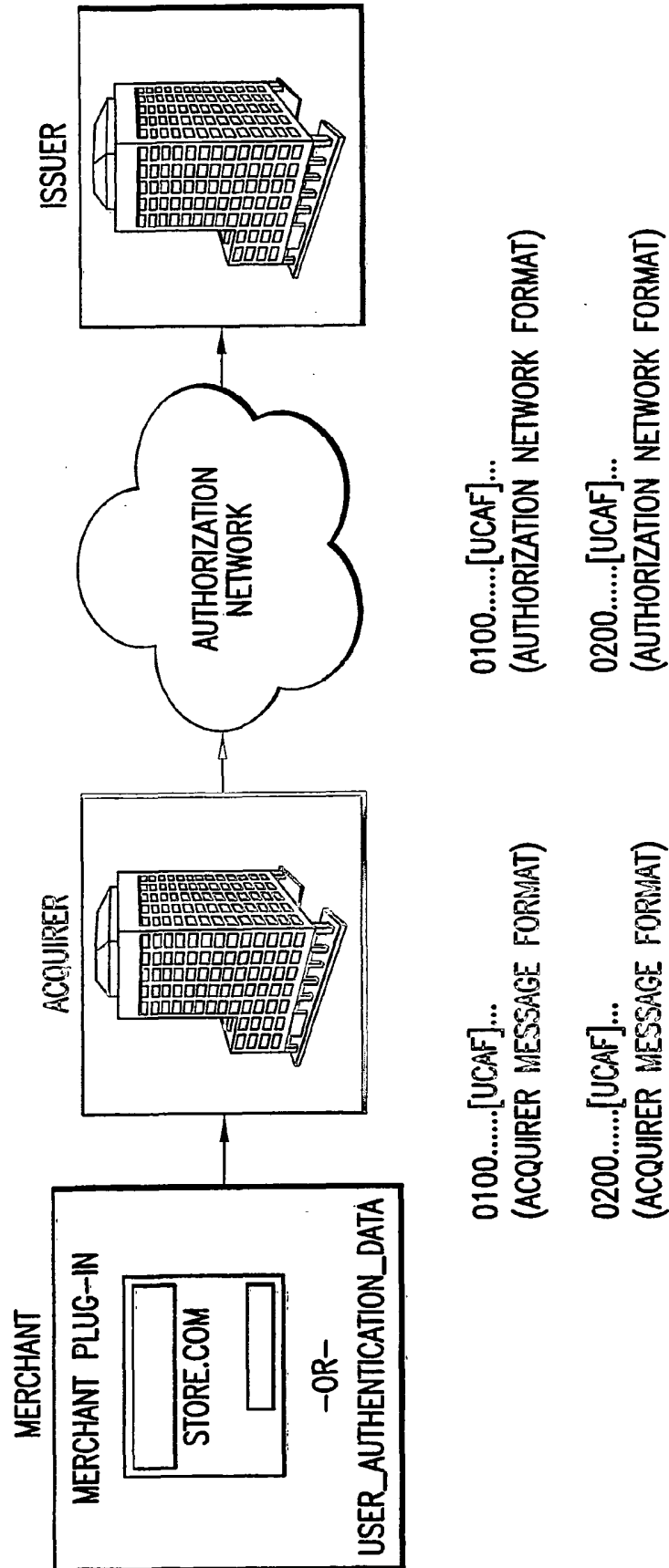


FIG.4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 09627102 A [0003]

RENDSZEREK ÉS ELJÁRÁSOK BIZTONSÁGOS FIZETÉSI TRANZAKCIÓ VÉGREHAJTÁSÁRA FORMÁZOTT ADATSZERKEZET FELHASZNÁLÁSÁVAL

SZABADALMI IGÉNYPONTOK

1. Rendszer egy kereskedővel egy elektronikus hálózaton zajló kártyatulajdonosi tranzakció hitelesítésére, ahol a rendszer tartalmaz:

egy kibocsátó platform réteget, amely legalább egy 3-D Secure hitelesítő programot foglal magába;

egy kereskedői beépítő (*plug-in*) modult, „MPI”;

egy biztonságos fizetési algoritmust, „SPA”, és

egy adatszállítási réteget,

ahol a kibocsátó platform tartalmaz egy hozzáférés-vezérlő szervert, „ACS”, amely az SPA-t használja a tranzakcióra és a kártyatulajdonosra vonatkozó információ feldolgozására egy hitelesítő eljárással való hitelesítéshez egy számlatulajdonost hitelesítő érték (*Accountholder Authentication Value*), „AAV”, előállítására céljából, és amely az AAV-t az adatszállítási rétegen keresztül továbbítja az MPI-hez,

ahol az AAV egy olyan formázott adatszerkezet, amely 3-D Secure üzenetküldési protokollokkal kompatibilis, ahol a formázott adatszerkezet legfeljebb 20 bájt hosszúságú és tartalmaz a kereskedő nevének egy hash kódját azonosító bájtokat, az ACS-t azonosító bájtokat, a hitelesítő eljárást azonosító bájtokat, titkos rejtjelező kulcsokat azonosító bájtokat és kereskedői hitelesítő kódot (*merchant authentication code*), „MAC”, azonosító bájtokat.

2. Az 1. igénypont szerinti rendszer, ahol az AAV egy olyan formázott adatszerkezet, amely a Base64 szabvány szerint van kódolva.

3. Az 1. igénypont szerinti rendszer, ahol az SPA tartalmaz egy titkosító algoritmust az MAC előállítására, ahol a titkosító algoritmus egy az AAV-ben azonosított titkos kulcsot használ a kártyatulajdonos számlaszámából és AAV bájtjai által alkotott mezőkből képezett láncolat titkosítására, ahol az AAV bájtjai közül nem vesszük figyelembe azokat, amelyek az MAC-t reprezentálják, és ahol a titkosítás eredményének egy része a MAC bájtjait képezi az AAV-ben.

4. Az 1. igénypont szerinti rendszer, ahol az SPA egy titkosító algoritmust tartalmaz az MAC előállításához, ahol a titkosító algoritmus egy az AAV-ben azonosított A és B titkos kulcsból álló kulcspárt használ a kártyatulajdonos számlaszámának, a kártya lejáratási időpontjának és egy szolgáltatási kód láncolatának titkosításához egy három helyi értékű CVC2 mező előállítása céljából, és az eredményt az MAC két bájtjának kitöltésére használja.

5. A 4. igénypont szerinti rendszer, ahol a kulcspár A és B titkos kulcsa egy-egy 64 bites DES

(Data Encryption Standard) szabvány szerinti kulcs.

6. Az 1. igénypont szerinti rendszer, ahol az ACS úgy van konfigurálva, hogy egy az MPI-ből az ACS-nek küldött, fizetéshitelesítés iránti kérést tartalmazó üzenetre adott válaszként előállít egy AAV-t.

7. Az 1. igénypont szerinti rendszer, amely úgy van konfigurálva, hogy az AAV-t egy az ACS-ből elküldött fizetéshitelesítő válaszüzenetben továbbítja.

8. A 7. igénypont szerinti rendszer, ahol az ACS továbbá úgy van konfigurálva, hogy a fizetéshitelesítő válaszüzenetre egy digitális aláírást tesz.

9. Az 1. igénypont szerinti rendszer, ahol az MPI úgy van konfigurálva, hogy leellenőrzi a beérkező fizetéshitelesítő válaszüzeneten lévő digitális aláírást.

10. Az 1. igénypont szerinti rendszer, ahol az MPI úgy van konfigurálva, hogy kinyeri az ACS-től származó fizetéshitelesítő válaszüzenetben foglalt MAC mezőket, és a kinyert MAC-t elhelyezi egy harmadik félnek szóló fizetéshitelesítő válaszüzenetben.

11. Adatszerkezet kártyatulajdonosi tranzakciót hitelesítő információ továbbítására az érintettek között egy 3-D Secure környezetben, ahol az adatszerkezet 20 bájtnyi Base64 szabvány szerint kódolt karaktert tartalmaz, ahol az első bájtnál egy vezérlő bájtnál, a 2-9. bájtok egy kereskedőnév hash kódját reprezentálják, a 10. bájtnál egy olyan hozzáférés-vezérlő szerver, ACS, azonosít, amely egy hitelesítő eljárás révén hitelesíti a kártyatulajdonos tranzakcióját, a 11. bájtnál az ACS által használt hitelesítő eljárást és a titkosító kulcsokat azonosítja, melyeket az ACS egy kereskedői hitelesítő kód, „MAC”, előállítására használ, a 12-15. bájtok egy olyan tranzakciósorszámot reprezentálnak, amely egy az ACS által feldolgozott tranzakciósorszámot azonosít, a 16-20. bájtok pedig az MAC-t reprezentálják.

12. A 11. igénypont szerinti adatszerkezet, ahol az MAC a kártyatulajdonos számlaszám és az adatszerkezet 1-15. bájtaiban tartalomzó mezők titkosított láncolatának részeit tartalmazza, ahol egyetlen, a 11. bájtnál azonosított kulcs van a titkosításra használva.

13. A 11. igénypont szerinti adatszerkezet, ahol az MAC a kártyatulajdonos számlaszámának, a kártya lejáratát idejének és egy szolgáltatási kódjának a titkosított láncolatának a részeit tartalmazza, ahol titkosításra a 11. bájtnál azonosított A és B kulcsokból álló kulcspár van felhasználva.

14. A 13. igénypont szerinti adatszerkezet, ahol egy három helyi értékű titkosítási eredmény van az MAC 16-20. bájtaiban közül két bájtnál kitöltéséhez felhasználva.

15. A 13. igénypont szerinti adatszerkezet, ahol a kulcspár A és B titkos kulcsa egy-egy 64 bites DES (Data Encryption Standard) szabvány szerinti kulcs.

16. Eljárás kereskedővel egy elektronikus hálózatban 3-D Secure környezetben zajló kártyatulajdonosi tranzakció hitelesítésére, ahol az eljárás során:

egy hozzáférés-vezérlő szervert, „ACS”, használunk a kártyatulajdonosra és a tranzakcióra vonatkozó információ feldolgozásához a kártyatulajdonosnak egy hitelesítő eljárással történő hitelesítése céljából;

egy biztonságos fizetési algoritmust, „SPA”, alkalmazunk egy a számlatulajdonost hitelesítő érték, „AAV”, előállításához a hitelesítési eredmények reprezentálása céljából; és

az AAV-t 3-D Secure üzenetekben továbbítjuk a kereskedőhöz, ahol az AAV egy olyan formázott adatszerkezet, amely legfeljebb 20 bájt hosszúságú és tartalmaz a kereskedő nevének egy hash kódját azonosító bájtokat, az ACS-t azonosító bájtokat, a hitelesítő eljárást azonosító bájtokat, egy kereskedői hitelesítő kódot (*merchant authentication code*), „MAC”, azonosító bájtokat és olyan titkos rejtjelező kulcsokat azonosító bájtokat, melyeket az SPA az MAC előállításához használ.

17. A 16. igénypont szerinti eljárás, ahol az AAV egy olyan formázott adatszerkezet, amely a Base64 szabvány szerint van kódolva.

18. A 16. igénypont szerinti eljárás, ahol egy SPA alkalmazása során:

egy az AAV-ben azonosított titkos kulcsot használunk a kártyatulajdonos számlaszámából és az AAV bájtjainak legalább egy részéből képezett láncolat titkosításához, ahol az AAV bájtjai közül figyelmen kívül hagyjuk azokat, amelyek az MAC-t reprezentálják;

a titkosítási eredmény egy részét a MAC-nak az AAV-ben lévő bájtjaiként használjuk.

19. A 16. igénypont szerinti eljárás, ahol egy SPA alkalmazása során:

az AAV-ben azonosított A és B titkos kulcsokat használjuk a kártyatulajdonos számlaszámának, a kártya lejáratú időpontjának és egy szolgáltatási kód láncolatának titkosításához egy három helyi értékű CVC2 mező előállítása céljából, és

az eredményt az MAC két bájtjának kitöltésére használjuk.

20. A 17. igénypont szerinti eljárás, ahol a kulcspár A és B titkos kulcsa egy-egy 64 bites DES (*Data Encryption Standard*) szabvány szerinti kulcs.

21. A 16. igénypont szerinti eljárás, ahol az AAV-nek a kereskedőhöz 3D biztonságos üzenetekben való továbbítása során az AAV-t egy olyan fizetэшitelesítő válaszüzenetben továbbítjuk, amelyet az ACS digitálisan aláírt.

22. A 21. igénypont szerinti eljárás, amely tartalmazza továbbá:

a beérkezett fizetэшitelesítő válaszüzenetben lévő digitális aláírásnak a kereskedő általi ellenőrzését; majd ezt követően

az MAC mezők kereskedő általi kinyerését a beérkezett fizetэшitelesítő válaszüzenetből.