(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2001 (19.04.2001)

PCT

(10) International Publication Number
WO 01/27887 A1

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number: PCT/US00/27458

(22) International Filing Date: 5 October 2000 (05.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/158,608 8 October 1999 (08.10.1999) US
60/163,886 5 November 1999 (05.11.1999) US

(71) Applicant: MASTERCARD INTERNATIONAL INCORPORATED [US/US]; 2000 Purchase Street, Purchase, NY 10577-2509 (US).

(72) Inventors: HARRIS, Michael, D., S.; 1521 Pennsylvania Avenue, Paoli, PA 19301 (US). WANKMUELLER, John; 11 Evergreen Lane, New Hyde Park, NY 11040 (US).

(74) Agents: SCHEINFELD, Robert, S. et al.; Baker & Botts, LLP, 30 Rockefeller Plaza, New York, NY 10112-0228 (US).

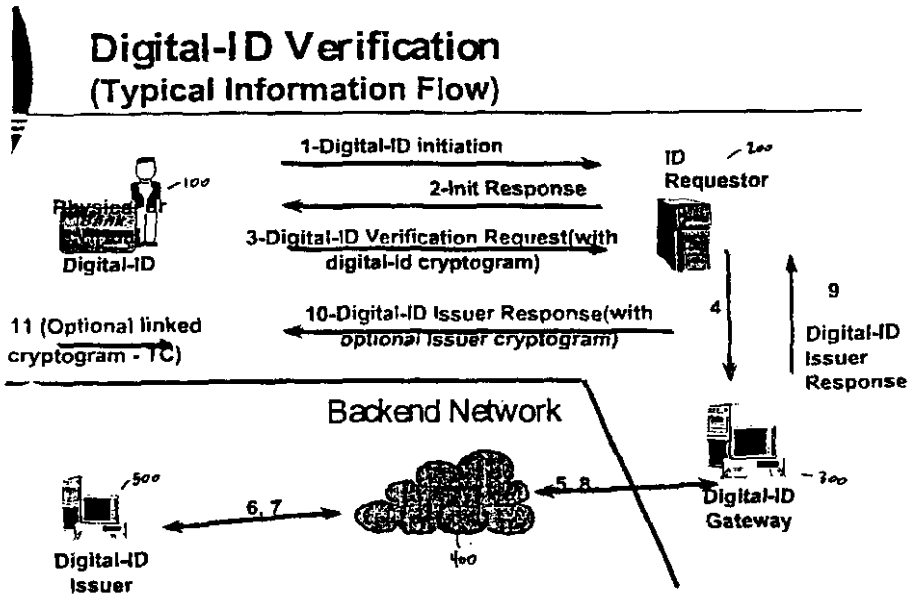
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *With amended claims.*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR GLOBAL INTERNET DIGITAL IDENTIFICATION



(57) Abstract: A system and method for authenticating a digital ID can utilize a central switch to transmit data between a network connected to a service provider and a network connected to a digital ID issuer. The system can be configured to provide a "yes/no" authorization or a validation at a selected validation level. The system can receive an encrypted authorization request message, and can generate an encrypted authorization response message. The authorization response message can be used by the service provider to decide whether to provide a service to a digital ID holder.

WO 01/27887 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR GLOBAL INTERNET DIGITAL IDENTIFICATION

SPECIFICATION

FIELD OF THE INVENTION

This invention relates to digital identification (hereinafter "digital ID") applications used to purchase goods or services.

BACKGROUND OF THE INVENTION

A digital ID is a set of digital data associated with an individual or entity. The ID can be, for example, a digital document (e.g., a digital certificate) which associates a digital key with the individual or entity. Digital ID applications for use over the Internet and elsewhere are proliferating. One model for digital ID applications allows a third party service provider on the Internet to perform an exchange with a cardholder accessing the third party site and to retrieve from the cardholder a digital ID that the service provider can then validate with a "central point" before providing service. The service provider goes to the "central point" for each validation and is charged based on the level of assurance that the "central point" is prepared to provide (e.g., 0.10¢ for a guarantee that digital ID is good for $100, 1¢ for a guarantee that digital ID is good for $1000, etc.).

Currently, some parties are attempting to fill a need for new hierarchical/trust models based on new commercial relationships. In contrast, the present invention provides a unique system and method for performing a digital ID function using currently existing payment system building blocks (such as the "EMV" standard promulgated jointly by Europay International S.A., MasterCard International Incorporated, and Visa International Service Association, and the "SET" standard

promulgated by SET Secure Electronic Transaction, LLC) and currently existing credit/debit card payment system contractual relationships. It is assumed that the reader is familiar with the EMV and SET standards, which are described in detail in the EMV and SET "References" listed in the "Related References" section below. These documents are incorporated by reference.

SUMMARY OF THE INVENTION

It is an object of the present invention to leverage existing investments and infrastructure to provide a unique system and method for providing digital ID applications.

It is another object of the present invention to enable banks with a way to issue digital IDs at an assurance level with which they are comfortable, without the investment required to set up a new infrastructure or without the requirement to join a new consortium.

It is another object of the present invention to simplify contractual relationships required for providing digital ID applications. Under the present invention, each digital ID issuer has one contractual relationship with a "central switch" and each service provider has one contractual relationship with the "central switch."

It is another object of the present invention to provide standardized assurance levels for service providers. With the present invention, issuers of digital IDs may choose to use some or all of the assurance levels.

It is another object of the present invention to provide a digital ID application that provides a high level of authentication while, at the same time, allowing the digital ID holder to remain anonymous to a digital ID verification requestor.

BRIEF DESCRIPTION OF THE DRAWING

Further objects, features, and advantages of the invention will become apparent from the following detailed description taken in conjunction with the

accompanying figure showing illustrative embodiments of the invention, in which:

FIG. 1 is a diagram of information flow in an exemplary system for performing digital ID in accordance with the invention.

In the figure, unless otherwise stated, the same reference numerals and characters are used to denote like features, elements, components, or portions of the illustrated embodiments. Moreover while the subject invention will now be described in detail with reference to the figure and in connection with the illustrative embodiments, changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

DETAILED DESCRIPTION OF THE INVENTION

According to the present invention, a digital ID issuer issues a digital ID to a digital ID holder. When a party desires to authenticate a digital ID holder, the request for digital ID verification is routed to the digital ID issuer over a distributed communication network. The distributed communication network may include the Internet and an existing legacy payment system infrastructure (such as the Banknet infrastructure of MasterCard International Incorporated). The Internet and the existing legacy payment system infrastructure are connected by a "central switch" or gateway (such as a SET gateway).

Digital ID holders are, with the present invention, able to anonymously identify themselves in remote environments, such as the Internet, to other parties. The digital ID is a portable identity object that is simple for digital ID holders to use and can eliminate the need by digital ID holders to remember different passwords and user-ID combinations required to gain access to protected Internet sites. While not revealing any other details of the identity to the identity verification requester, the present invention can release only agreed identity data to the identity verification requester. It is the digital ID issuer who provides and controls all data.

In transmitting the request for digital ID verification, the present invention uses a set of separate, stand-alone, non-payment messages which utilize existing legacy payment system message formats and payment-related data. The digital ID

verification request involves the use of a shared secret (of any type) possessed only by the digital ID issuer and the digital ID holder. High security is enabled since the number and types of secrets shared and algorithms used by the parties are varied and potentially non-standard. The digital ID issuer will receive and validate a digital ID payment object, which is created by the digital ID holder with the shared secret. Advantageously, the digital ID payment object is passed as an opaque block (an object that cannot be read) through all intermediary nodes to the digital ID issuer.

When a digital ID issuer receives a digital ID verification request, the digital ID issuer has a number of response options available to it. One option is to simply respond with a binary "yes" or "no" to the digital ID verification request. A second option is to respond with other data which is related to the digital ID holder, such as demographic data, payment history data, and/or other marketing data. Preferably, this other data is non-personally identifiable data, and the dissemination of this other data is pre-approved by the digital ID holder. The data may also include passwords for accessing a service provider's web site.

Previous digital identification technology has employed asymmetric key technology with private/public key pairs and digital certificates, sometimes combined with secured integrated circuit (IC) chip cards. Advantageously, the present invention can be deployed without chip cards or any secure hardware deployed by the digital ID issuer. Moreover, the present invention may use shared symmetric key technology, instead of asymmetric key technology, to provide a digital ID function.

Another unique feature of the present invention is that digital ID verification may occur before and/or after a payment transaction, and the digital ID verification is capable of being linked with the payment transaction through cryptography. The linking is accomplished through the use of a cryptogram, which is an object containing the result of a cryptographic operation. Preferably, the present invention uses time-sensitive data.

A preferred embodiment of the present invention will now be described. In this preferred embodiment, the basic cryptographic techniques utilize parts of the EMV credit or debit payment specification and an EMV infrastructure. An EMV-compliant chip card may be used with this embodiment, but (as already mentioned)

chip card use is not required. Instead, an digital ID application may be stored, for example, on a computer that is connected to the Internet. The stored digital ID application stored on the computer could function as a "virtual" chip card.

With reference to Fig. 1, a digital ID issuer 500 (such as a bank) preferably issues a physical or virtual chip card 100 based on the EMV specification. The chip card 100 can, optionally, be direct mailed to an end user. The chip card 100 may contain a single application or multiple applications on it, and can, optionally, be based on the MULTOS™ operating system or on another operating system. It is assumed that the reader is familiar with the MULTOS™ standard, which is maintained by the MAOSCO Consortium. The standard is described in the MULTOS™ "References" listed in the "Related References" section below. These documents are incorporated by reference.

The digital ID issuer 500 assigns a payment-related or non-payment-related digital ID account number within the MasterCard Payment Application (MCPA) function in the chip card 100. However, the digital ID account number is not required to be a credit/debit card account number (and, indeed, for security purposes, it is preferred that the digital ID not be such a number). In essence, the digital ID issuer may deploy digital ID EMV-based applications which do not use credit/debit card account numbers but assign an account number only for digital ID use.

After the digital ID is issued, the cardholder logs onto the Internet and requests a service from a service provider web site (this request represented by arrow 1 of Fig. 1).

Before providing the requested service, the service provider 200 may decide to verify the cardholder's identity. It is up to the service provider to decide the frequency with which it requests verification from its customers. The service provider may request verification each and every time a service is requested, or it may request verification only occasionally.

If the service provider 200 decides to request verification, the service provider preferably initiates a SET specification based transaction (for confidentiality and integrity of messaging over the Internet) and asks the cardholder (this request represented by arrow 2 of Fig. 1) to use its chip card (virtual or physical) to initiate a

digital ID verification transaction (shown as arrow 3). The digital ID verification transaction uses the credit/debit payment message formats of the MCPA and EMV specifications. These message formats may be used in a number of ways. For example, the payment amount field may be set to zero and the request may be treated as an authorization for a payment transaction of zero amount. Alternatively, a new message type may be added (for example, a "digital ID request" type) to the existing payment infrastructure. This new message type can be used to redefine certain fields. In particular, the payment field may no longer represent a payment amount, but a validation level amount. For example, if the payment field contains $100, the digital ID issuer will validate the identity of the digital ID at this validation level.

When a cardholder receives a request to initiate a digital ID verification transaction, the cardholder produces an EMV-formatted cryptogram (shown as arrow 3) (such as an authorization request cryptogram or an "ARQC" cryptogram) and provides it to the service provider 200. The cryptogram is then transported (arrow 4) securely over the Internet, protected by (for example) the SET protocol. The cryptogram can be a digital certificate.

The service provider passes this transaction request (arrow 4) over the Internet, using (preferably) the SET protocol, to a "central switch" 300, which may provide a SET payment gateway function. Since the transaction is not a payment, a bank-provided payment gateway is not necessary. The central switch 300 can, optionally, be a SET acquirer.

The switch 300 reformats the verification transaction request to the format for message transmission over a trusted back-end network 400 (such as MasterCard International Inc.'s Banknet network). For example, if the back-end network is MasterCard International Inc.'s Banknet network, the verification request message is formatted as a "0100" chip formatted authorization request message. The reformatted message is then passed (arrow 5) into the trusted back-end network 400, which routes the verification request (arrow 6) to the digital ID issuer 500.

The digital ID issuer 500 authenticates the digital ID verification transaction and stores the transaction for possible service provider fee collection at a level identified and requested on the verification request message. As previously discussed,

the response by the digital ID issuer may be a simple "yes" or "no" or it may include other digital ID holder-related data. The response also preferably includes an Authorization Response Cryptogram ("ARPC").

The digital ID issuer 500 responds to the switch via the trusted back-end network 400 with an authorization response message (arrow 7). If the back-end network is MasterCard's Banknet network, the message is a "0110" formatted authorization response message. It is formatted as a payment authorization request but carries digital ID response data. The back-end network 400 then passes the message (arrow 8) to the switch 300.

The switch formats the authorization response message as a SET/EMV response message (arrow 9) to the service provider 200. The response message confirms or denies the digital ID authentication at the requested service level. This response message is similar to an authorization for purchase response.

When the service provider 200 receives the SET/EMV response message, it decides whether to provide service to the cardholder. The service provider may optionally complete the EMV-like transaction by sending a SET message (arrow 10) back to the physical or virtual card.

The functions of the switch system are as follows:

1. Receive and translate SET/EMV messages on the Internet from service providers into 0100 payment formatted messages for Banknet.

2. Identify and translate 0110 formatted messages from Banknet into SET/EMV messages on the Internet to service providers.

3. Identify and log transactions for fee purposes.

4. Gather fees from service providers.

5. Distribute shares of fees to digital ID issuers.

6. Identify new contents of fields on 0100/0110 messages and SET/EMV messages to facilitate identification or non-payment transaction.

To ensure the freshness of a digital ID request and avoid replay of a digital ID request at a later date and time, it is preferred that digital ID devices will generate a random number challenge which is used, along with other data, by the digital ID holder to create the digital ID cryptogram sent to the digital ID issuer for validation. A preferred embodiment is to use SET technology and EMV chip card technology for this function.

A preferred embodiment of the present invention is built upon the EMV electronic commerce specification but includes the following modifications and additions. The digital ID number is preferably a fully "routable" credit or debit primary account number (PAN), but the number is not necessarily related to a payment account. In a preferred embodiment, the digital ID number is not the account number used for payment.

In addition, the present invention also adds the option to save the EMV final Transaction Certificate (TC) by the cardholder system. This final TC (arrow 11) is a cryptographic object that may be used to link a digital ID verification transaction to a payment transaction. The TC is based on the same shared secret as that used in generating the ARQC and on the ARPC received from the digital ID issuer. In those cases when the digital ID issuer is the same as the payment account issuer, the TC (along with the data needed to generate the TC) provides a strong linkage between the digital ID verification transaction and a payment authorization request. To achieve the linkage, the TC may be bundled into a payment transaction as the "random number" used in the initiate payment transaction stage. An advantage to using the TC in this manner is that a lower level of security is needed to transmit the payment transaction data over the Internet. This is because the transaction route has already been verified by the digital ID verification transaction and the receipt of an ARPC.

Although the present invention has been described in connection with particular embodiments thereof, it is to be understood that such embodiments are susceptible of modification and variation without departing from the scope of the inventive concept as defined by the appended claims.

RELATED REFERENCES

The following references are hereby incorporated by reference in their entireties:

SET References:

SET Secure Electronic Transaction Specification, Book 1: Business Description, Version 1.0, May 31, 1997 (available at http://www.setco.org/download.html).

SET Secure Electronic Transaction Specification Book 2: Programmer's Guide, Version 1.0, May 31, 1997 (available at http://www.setco.org/download.html).

SET Secure Electronic Transaction Specification Book 3: Formal Protocol Definition, Version 1.0, May 31, 1997 (available at http://www.setco.org/download.html).

SET Glossary of Terms, July 1999 (available at http://www.setco.org/download.html).

External Interface Guide to SET Secure Electronic Transaction, September 24, 1997 (available at http://www.setco.org/download.html).

SET Generic Cryptogram Extension, July 19, 1999 (available at http://www.setco.org/download.html).

SET Japanese Payment Option Extension, August 24, 1999 (available at http://www.setco.org/download.html).

SET Merchant Initiated Authorization Extension, July 19, 1999 (available at http://www.setco.org/download.html).

SET Online PIN Extensions, July 19, 1999 (available at http://www.setco.org/download.html).

SET CVV2/CVC2 Extension, September 29, 1999 (available at http://www.setco.org/download.html).

EMV References:

EMV '96 Chip Electronic Commerce Specification, Draft 1.0, 1999.

EMV '96 Integrated Circuit Card Specification for Payment Systems, Version 3.1.1, May 31, 1998 (available at http://www.emvco.com/specifications.cfm).

EMV '96 Integrated Circuit Card Terminal Specification for Payment Systems, Version 3.1.1, May 31, 1998 (available at http://www.emvco.com/specifications.cfm).

EMV '96 Integrated Circuit Card Application Specification for Payment Systems, Version 3.1.1, May 31, 1998 (available at http://www.emvco.com/specifications.cfm).

Business Functional Requirements for Debit and Credit on Chip, Version 1.0, October 20, 1997 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

Integrated Circuit Card Application Specifications for Debit and Credit on Chip, Version 2.0, November 1998 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

Minimum Card Requirements for Debit and Credit on Chip, Version 2.0, November 1998 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

Terminal Requirements for Debit and Credit on Chip, Version 2.0, November 1998 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

Integrated Circuit Card Terminal Application Services - Type Approval, Version 1.0, October 24, 1997 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

Personalization Data Specifications for Debit and Credit on Chip, Version 1.0, August 1998 (available at http://www.mastercard.com/emv/emvspecs02.html#emv2).

MULTOS References:

MAOSCO, *A Guide to the MULTOS Scheme* (2000).

MAOSCO, *Information Bulletin – Introduction to MULTOS & MAOSCO,* Jan. 4, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin 6 – MAOSCO Policy Position on ITSEC Matters,* Mar. 19, 1999 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No. 3 – Developing & Loading Applications,* Mar. 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No. 4 – Using MULTOS,* Apr. 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No 5 – Application Load/Delete Certificates & Application Load Units,* March 18, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No. 7 – Export Controls,* Sept. 29, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No. 8 – Obtaining an Implementation Licence,* May 14, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Information Bulletin No. 9 – Export Controls, End-User Undertaking Guidance,* Mar. 4, 1999 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Technical Bulletin No. 1 – Shell Applications,* Apr. 15, 1999 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Technical Bulletin No. 2 – MULTOS and ISO 7816 Files,* Jul. 7, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Technical Bulletin No. 4 – Enablement/MSM Controls Data Loading,*

Dec. 4, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Technical Bulletin No. 5 – Delegation,* Apr. 15, 1999 (available at http://dh007-00.web.dircon.net/present.ihtml).

MAOSCO, *Technical Bulletin No. 6 – What's New in MULTOS,* Sept. 1, 1998 (available at http://dh007-00.web.dircon.net/present.ihtml).

CLAIMS

1. A method for verifying an identity of an ID holder, comprising the steps of:

providing a central switch in communication with a first network and a second network;

receiving, into the central switch, identification data from the first network, wherein the identification data has been provided by the ID holder and transmitted into the first network;

controlling the central switch to use the identification data to generate an authorization request message having a format suitable for transmission through the second network;

controlling the central switch to transmit the authorization request message into the second network to an ID issuer;

receiving, into the central switch, an authorization response message from the second network, wherein the authorization response message has been generated by the ID issuer in response to the authorization request message;

controlling the central switch to use the authorization response message to generate an output response message having a format suitable for transmission through the first network; and

controlling the central switch to transmit the output response message into the first network.

2. A method as recited in claim 1, wherein the identification data includes a result of a cryptographic operation.

3. A method as recited in claim 2, wherein the result of the cryptographic operation includes an EMV-formatted cryptogram.

4. A method as recited in claim 2, wherein the cryptographic operation comprises:

generating an essentially random number; and

using the essentially random number to generate the result of the cryptographic operation.

5. A method as recited in claim 2, wherein the cryptographic operation comprises at least one of a secure electronic transaction cryptographic operation and an EMV chip card cryptographic operation.

6. A method as recited in claim 1, wherein the authorization response message includes a result of a cryptographic operation.

7. A method as recited in claim 6, wherein the result of the cryptographic operation includes an Authorization Response Cryptogram.

8. A method as recited in claim 1, further comprising issuing a digital ID to the ID holder, wherein the identification data is generated by the digital ID.

9. A method as recited in claim 1, wherein the first network comprises an international network.

10. A method as recited in claim 1, wherein the second network comprises a trusted network.

11. A method as recited in claim 1, wherein the central switch comprises a secure electronic transaction gateway.

12. A method as recited in claim 1, wherein the authorization response message includes at least one of an indication of authorization and an indication of denial of authorization.

13. A method as recited in claim 1, wherein the authorization response message includes information about the ID holder.

14. A method as recited in claim 13, wherein the information about the ID holder includes at least one of demographic data and payment history data.

15. A method as recited in claim 1, wherein the authorization response message includes a password suitable for enabling the ID holder to access a web site.

16. A method as recited in claim 1, further comprising issuing, to the ID holder, one of a physical chip card and a virtual chip card, wherein the identification data is generated by said one of a physical chip card and a virtual chip card.

17. A method as recited in claim 16, wherein the identification data has been transmitted into the first network by an ID requestor, said method further comprising sending a transaction-related message from the ID requestor to said one of a physical chip card and a virtual chip card.

18. A method as recited in claim 16, wherein said one of a physical chip card and a virtual chip card stores at least one application.

19. A method as recited in claim 16, further comprising assigning, to the ID holder, a digital ID account number, wherein the digital ID account number is stored within said one of a physical chip card and a virtual chip card.

20. A method as recited in claim 1, further comprising using the output response message to decide whether to provide a service to the ID holder.

21. A method as recited in claim 1, wherein the identification data includes a payment amount field.

22. A method as recited in claim 21, wherein the authorization response message is generated by performing an authentication operation upon the authorization request message, wherein the payment amount field is set to a selected amount, and wherein the authentication operation comprises deciding whether to authorize a payment transaction having a value corresponding to the selected amount.

23. A method as recited in claim 22, wherein the selected amount is zero.

24. A method as recited in claim 1, wherein the identification data includes a validation level amount field.

25. A method as recited in claim 24, wherein the authorization response message is generated by performing an authentication operation upon the authorization request

message, wherein the validation level amount field is set to a selected level, and wherein the authentication operation comprises deciding whether to validate the identity of the ID holder at a value corresponding to the selected level.

26. A method as recited in claim 1, wherein the authorization response message is generated by performing an authentication operation upon the authorization request message, said method further comprising storing transaction data related to at least one of the identification data, the authorization request message, the authentication operation, the authorization response message, and the output response message.

27. A method as recited in claim 26, wherein the transaction data comprises a cryptographic transaction certificate, said method further comprising:

storing secret data which is shared with the ID holder; and

using the secret data to generate the transaction certificate.

28. A method as recited in claim 27, further comprising:

incorporating the transaction certificate into payment transaction data; and

using the payment transaction data to initiate a payment.

29. A method as recited in claim 1, wherein the authorization request message has a 0100 chip format.

30. A method as recited in claim 1, wherein the authorization response message has a 0110 format.

31. A method as recited in claim 1, wherein the output response message has an EMV format.

32. A method as recited in claim 1, further comprising the steps of:

collecting a fee from an ID requestor which has transmitted the identification data into the first network; and

distributing at least one share of the fee to at least one ID issuer.

33. A method as recited in claim 1, wherein the identification data does not include a payment account number.

34. A method as recited in claim 1, further comprising:

storing secret data which is shared with the ID holder;

receiving, by the ID issuer, the authorization request message;

using, by the ID issuer, the secret data to perform an authentication operation upon the authorization request message, thereby generating the authorization response message; and

transmitting, by the ID issuer, the authorization response message through the second network to the central switch.

35. A method as recited in claim 34, wherein:

the identification data includes a result of a first cryptographic operation;

the authorization response message includes a result of a second cryptographic operation;

the first network comprises an international network;

the second network comprises a trusted network;

the central switch comprises a secure electronic transaction gateway;

the authorization response message includes at least one of an indication of authorization and an indication of denial of authorization;

the authorization response message includes information about the ID holder;

the authorization response message includes a password suitable for enabling the ID holder to access a web site;

the identification data includes at least one of a payment amount field and a validation level amount field;

the authorization request message has a 0100 chip format;

the authorization response message has a 0110 format;

the output response message has an EMV format; and

the identification data does not include a payment account number, said method further comprising the steps of:

issuing a digital ID to the ID holder, wherein the identification data is

generated by the digital ID;

using the output response message to decide whether to provide a service to the ID holder;

using the secret data to generate a cryptographic transaction certificate;

storing transaction data related to at least one of the identification data, the authorization request message, the authentication operation, the authorization response message, and the output response message, said transaction data including said transaction certificate;

incorporating the transaction certificate into payment transaction data;

using the payment transaction data to initiate a payment;

collecting a fee from an ID requestor which has transmitted the identification data into the first network; and

distributing at least one share of the fee to at least one ID issuer.

36. A method for verifying an identity of an ID holder, comprising the steps of:

receiving identification data from at least one of a first network and an ID requestor;

using the identification data to generate an authorization request message having a format suitable for transmission to at least one of a second network and an ID issuer;

transmitting the authorization request message to said at least one of a second network and an ID issuer;

receiving, from said at least one of a second network and an ID issuer, an authorization response message generated in response to the authorization request message;

using the authorization response message to generate an output message having a format suitable for transmission to said at least one of a first network and an ID requestor; and

transmitting the output message to said at least one of a first network and an ID requestor.

37. A method as recited in claim 36, wherein the identification data includes a result of a cryptographic operation.

38. A method as recited in claim 36, wherein the authorization response message includes a result of a cryptographic operation.

39. A method as recited in claim 36, further comprising issuing a digital ID to the ID holder, wherein the identification data is generated by the digital ID.

40. A method as recited in claim 36, wherein the first network comprises an international network.

41. A method as recited in claim 36, wherein the second network comprises a trusted network.

42. A method as recited in claim 36, wherein at least one of said steps of receiving identification data, using the identification data, transmitting the authorization request message, receiving an authorization response message, using the authorization response message, and transmitting the output message is performed using a secure electronic transaction gateway.

43. A method as recited in claim 36, wherein the authorization response message includes at least one of an indication of authorization and an indication of denial of authorization.

44. A method as recited in claim 36, wherein the authorization response message includes information about the ID holder.

45. A method as recited in claim 36, wherein the authorization response message includes a password suitable for enabling the ID holder to access a web site.

46. A method as recited in claim 36, further comprising issuing, to the ID holder, one of a physical chip card and a virtual chip card, wherein the identification data is generated by said one of a physical chip card and a virtual chip card.

47. A method as recited in claim 36, further comprising using the output message to decide whether to provide a service to the ID holder.

48. A method as recited in claim 36, wherein the identification data includes a payment amount field.

49. A method as recited in claim 36, wherein the identification data includes a validation level amount field.

50. A method as recited in claim 36, wherein the authorization response message is generated by performing an authentication operation upon the authorization request message, said method further comprising storing transaction data related to at least one of the identification data, the authorization request message, the authentication operation, the authorization response message, and the output message.

51. A method as recited in claim 50, wherein the transaction data comprises a cryptographic transaction certificate, said method further comprising :

storing secret data which is shared with the ID holder; and

using the secret data to generate the transaction certificate.

52. A method as recited in claim 51, further comprising:

incorporating the transaction certificate into payment transaction data; and

using the payment transaction data to initiate a payment.

53. A method as recited in claim 36, wherein the authorization request message has a 0100 chip format.

54. A method as recited in claim 36, wherein the authorization response message has a 0110 format.

55. A method as recited in claim 36, wherein the output message has an EMV format.

56. A method as recited in claim 36, further comprising the steps of:

collecting a fee from an ID requestor from which the identification data has been received; and

distributing at least one share of the fee to at least one ID issuer.

57. A method as recited in claim 36, wherein the identification data does not include a payment account number.

58. A method as recited in claim 36, further comprising:

storing secret data which is shared with the ID holder;

receiving, by said at least one of a second network and an ID issuer, the authorization request message;

using the secret data to perform an authentication operation upon the authorization request message, thereby generating the authorization response message; and

transmitting, from said at least one of a second network and an ID issuer, the authorization response message.

59. A system for verifying an identity of an ID holder, comprising a central switch in communication with a first network and a second network, said central switch being configured to perform the steps of:

receiving identification data from the first network;

using the identification data to generate an authorization request message having a format suitable for transmission through the second network;

transmitting the authorization request message through the second network;

receiving, from the second network, an authorization response message generated in response to the authorization request message;

using the authorization response message to generate an output message having a format suitable for transmission through the first network; and

transmitting the output message through the first network.

60. A system as recited in claim 59, wherein the identification data includes a result of a cryptographic operation.

61. A system as recited in claim 59, wherein the authorization response message includes a result of a cryptographic operation.

62. A system as recited in claim 59, further comprising an ID issuer configured to issue a digital ID to the ID holder, wherein the identification data is generated by the digital ID.

63. A system as recited in claim 59, wherein the first network comprises an international network.

64. A system as recited in claim 59, wherein the second network comprises a trusted network.

65. A system as recited in claim 59, wherein the central switch comprises a secure electronic transaction gateway.

66. A system as recited in claim 59, wherein the authorization response message includes at least one of an indication of authorization and an indication of denial of authorization.

67. A system as recited in claim 59, wherein the authorization response message includes information about the ID holder.

68. A system as recited in claim 59, wherein the authorization response message includes a password suitable for enabling the ID holder to access a web site.

69. A system as recited in claim 59, further comprising an ID issuer configured to issue, to the ID holder, one of a physical chip card and a virtual chip card, wherein the identification data is generated by said one of a physical chip card and a virtual chip card.

70. A system as recited in claim 59, further comprising an ID requestor configured to use the output message to decide whether to provide a service to the ID holder.

71. A system as recited in claim 59, wherein the identification data includes a payment amount field.

72. A system as recited in claim 59, wherein the identification data includes a validation level amount field.

73. A system as recited in claim 59, further comprising an ID issuer configured to generate the authentication response message by performing an authentication operation upon the authorization request message, wherein at least one of said central switch and said ID issuer is further configured to store transaction data related to at least one of the identification data, the authorization request message, the authentication operation, the authorization response message, and the output message.

74. A system as recited in claim 73, wherein the transaction data comprises a cryptographic transaction certificate.

75. A system as recited in claim 74, wherein said at least one of said central switch and said ID issuer is further configured to perform the steps of:

incorporating the transaction certificate into payment transaction data; and

using the payment transaction data to initiate a payment.

76. A system as recited in claim 59, wherein the authorization request message has a 0100 chip format.

77. A system as recited in claim 59, wherein the authorization response message has a 0110 format.

78. A system as recited in claim 59, wherein the output message has an EMV format.

79. A system as recited in claim 59, wherein the central switch is further configured to perform the steps of:

collecting a fee from an ID requestor which has transmitted the identification data into the first network; and

distributing at least one share of the fee to at least one ID issuer.

80. A system as recited in claim 59, wherein the identification data does not include a payment account number.

81. A system as recited in claim 59, further comprising an ID issuer configured to perform the steps of:

storing secret data which is shared with the ID holder;

receiving the authorization request message from the central switch, through the second network;

using the secret data to perform an authentication operation upon the authorization request message, thereby generating the authorization response message; and

transmitting the authorization response message to the central switch, through the second network.

82. A system as recited in claim 81, further comprising an ID requestor, wherein:

the identification data includes a result of a first cryptographic operation;

the authorization response message includes a result of a second cryptographic operation;

the first network comprises an international network;

the second network comprises a trusted network;

the central switch comprises a secure electronic transaction gateway;

the authorization response message includes at least one of an indication of authorization and an indication of denial of authorization;

the authorization response message includes information about the ID holder;

the authorization response message includes a password suitable for enabling the ID holder to access a web site;

the identification data includes at least one of a payment amount field and a validation level amount field;

the authorization request message has a 0100 chip format;

the authorization response message has a 0110 format;

the output message has an EMV format;

the identification data does not include a payment account number;

the ID issuer is configured to issue a digital ID to the ID holder, wherein the identification data is generated by the digital ID;

the ID requestor is configured to use the output message to decide whether to provide a service to the ID holder;

at least one of the central switch and the ID issuer is further configured to store transaction data related to at least one of the identification data, the authorization request message, the authentication operation, the authorization response message, and the output response message, said transaction data including a cryptographic transaction certificate;

at least one of the central switch and the ID issuer is further configured to perform the steps of:

incorporating the transaction certificate into payment transaction data; and

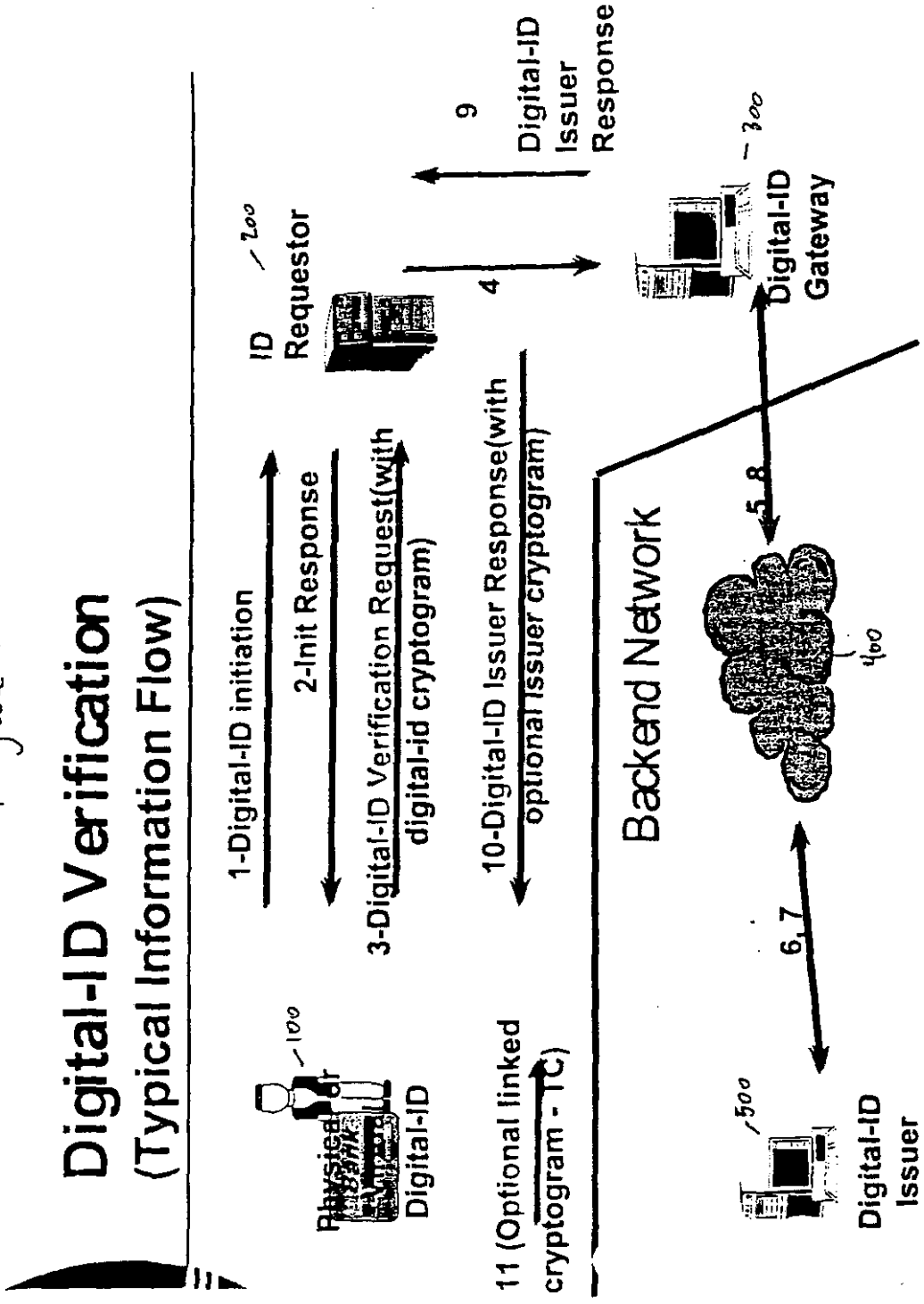
using the payment transaction data to initiate a payment; and

the central switch is further configured to perform the steps of:

collecting a fee from the ID requestor; and

distributing at least one share of the fee to at least one ID issuer.

Figure 1


Digital-ID Verification
(Typical Information Flow)
1-Digital-ID initiation
2-Init Response
3-Digital-ID Verification Request(with digital-id cryptogram)
4
9
Digital-ID Issuer Response
10-Digital-ID Issuer Response(with optional issuer cryptogram)
11 (Optional linked cryptogram - TC)
ID Requestor
200
Digital-ID
100
Digital-ID Gateway
300
Backend Network
400
5, 8
6, 7
Digital-ID Issuer
500

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 00/27458

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 826 245 A (SANDBERG-DIMENT ERIK) 20 October 1998 (1998-10-20) claim 1; figure 2	1-82
X	EP 0 921 487 A (M P TECHNOLOGY INC ;NIPPON TELEGRAPH & TELEPHONE (JP)) 9 June 1999 (1999-06-09) claim 1; figure 1	1-82
A	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK-DELIVERED SERVICES" IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 2, no. 4, 1 August 1995 (1995-08-01), pages 34-39, XP000517588 ISSN: 1070-9916 figure 2	1-82

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 February 2001	08/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 00/27458

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 557 518 A (ROSEN SHOLOM S) 17 September 1996 (1996-09-17) claim 1; figure 5	1-82
A	EP 0 590 861 A (AMERICAN TELEPHONE & TELEGRAPH) 6 April 1994 (1994-04-06) claim 1; figure 1	1-82
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) claim 1; figure 1	1-82
A	US 5 757 917 A (STEIN LEE H ET AL) 26 May 1998 (1998-05-26) claim 1; figure 1	1-82
A	US 5 903 882 A (ASAY ALAN ET AL) 11 May 1999 (1999-05-11) claim 1; figure 1	1-82

1

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter onal Application No
PCT/US 00/27458

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5826245 A	20-10-1998	AU 5366096 A	08-10-1996
		WO 9629667 A	26-09-1996
EP 0921487 A	09-06-1999	JP 11316729 A	16-11-1999
US 5557518 A	17-09-1996	AU 690662 B	30-04-1998
		AU 2105895 A	29-11-1995
		AU 701201 B	21-01-1999
		AU 5283598 A	02-04-1998
		AU 697007 B	24-09-1998
		AU 5283698 A	23-04-1998
		AU 696726 B	17-09-1998
		AU 5283798 A	23-04-1998
		AU 697013 B	24-09-1998
		AU 5283898 A	23-04-1998
		BR 9507107 A	09-09-1997
		CA 2184380 A	09-11-1995
		CN 1147875 A	16-04-1997
		CZ 9602513 A	15-10-1997
		EP 0758474 A	19-02-1997
		FI 964032 A	08-10-1996
		HU 76463 A,B	29-09-1997
		JP 9511350 T	11-11-1997
		NO 964538 A	05-12-1996
		NZ 283103 A	26-02-1998
		NZ 329065 A	25-03-1998
		NZ 329066 A	25-03-1998
		NZ 329067 A	25-03-1998
		NZ 329068 A	25-03-1998
		PL 317026 A	03-03-1997
		PL 179928 B	30-11-2000
		RU 2136042 C	27-08-1999
		SI 9520039 A	30-06-1997
		SK 117696 A	08-10-1997
		WO 9530211 A	09-11-1995
		US 6088797 A	11-07-2000
		US 5799087 A	25-08-1998
		US 5642419 A	24-06-1997
		US 5621797 A	15-04-1997
		US 5703949 A	30-12-1997
		US 5878139 A	02-03-1999
		US 6047067 A	04-04-2000
		US 5963648 A	05-10-1999
		US 5920629 A	06-07-1999
		US 5953423 A	14-09-1999
EP 0590861 A	06-04-1994	CA 2100134 A	30-03-1994
		JP 7129671 A	19-05-1995
		MX 9305830 A	30-06-1994
		US 5485510 A	16-01-1996
US 5883810 A	16-03-1999	NONE	
US 5757917 A	26-05-1998	AU 720433 B	01-06-2000
		AU 7551596 A	22-05-1997
		EP 0858697 A	19-08-1998
		JP 11514763 T	14-12-1999
		WO 9716897 A	09-05-1997

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter onal Application No
PCT/US 00/27458

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5903882 A	11-05-1999	AU 5515398 A	03-07-1998
		BR 9714400 A	18-04-2000
		CN 1244936 A	16-02-2000
		EP 0965111 A	22-12-1999
		WO 9826385 A	18-06-1998

Form PCT/ISA/210 (patent family annex) (July 1992)

事項編號 ： 9878937

參考編號 ： WO 01/27887 A1

名　　稱 ： 全球互聯網數碼身份辨認的系統和方法

摘　　要 ： 本發明關於一個可認證數碼身份的系統和方法，可以運用一個中央開關將數據在連接上服務供應者的網絡與連接上數碼身份發行人之間進行傳送。該系統可被配置以提供一個“是/否”的授權或者於已選擇的確認水平處提供確認。該系統可接收密碼式授權要求信息，並可發出密碼式授權回應信息。服務供應者可使用授權回應信息決定是否向數碼身份持有者提供服務。