



(22) Date de dépôt/Filing Date: 2006/09/28

(41) Mise à la disp. pub./Open to Public Insp.: 2008/03/21

(30) Priorité/Priority: 2006/09/21 (US60/846,446)

(51) Cl.Int./Int.Cl. *G06Q 20/00* (2006.01)

(71) Demandeurs/Applicants:
VON HEESEN, CLAUDIA, DE;
SPIEGEL, HARALD, DE

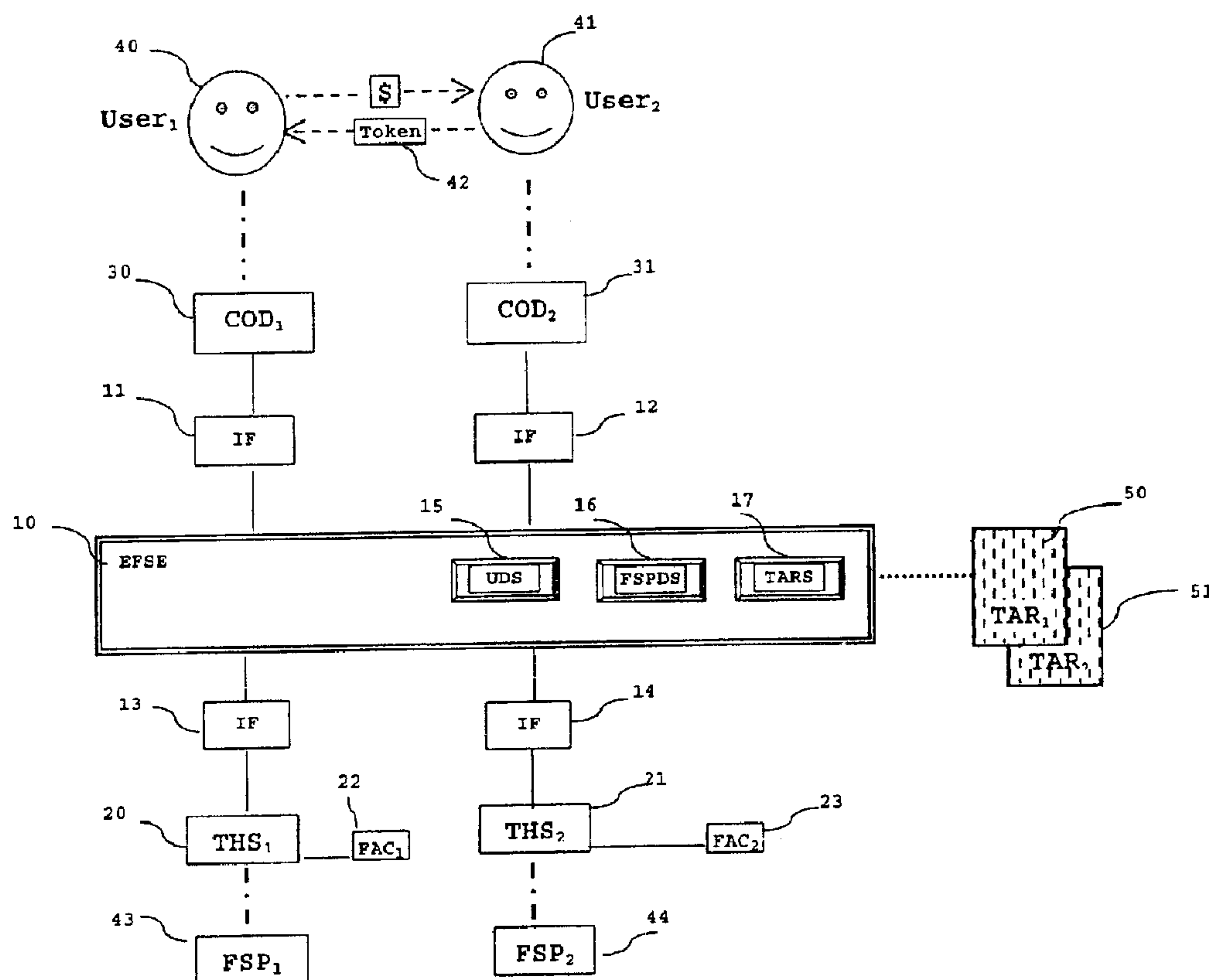
(72) Inventeurs/Inventors:
VON HEESEN, CLAUDIA, DE;
SPIEGEL, HARALD, DE

(74) Agent: SIM & MCBURNEY

(54) Titre : METHODE ET SYSTEME DE PAIEMENT

(54) Title: PAYMENT METHOD AND SYSTEM

System Architecture



(57) Abrégé/Abstract:

Method and system for secure handling of electronic financial services with the aid of an electronic financial services exchanger
Defined is a method of exchanging, handling and controlling electronic financial services, particularly mobile electronic financial



(57) **Abrégé(suite)/Abstract(continued):**

services from various financial service providers to authorized users with a wide variety of communication devices (both stationary and mobile). The system provides for the exchange of electronic financial services all services of the connected transaction handling systems 20, 21 from financial service providers 43, 44 in the form of a standardized platform by means of corresponding interfaces 13, 14 irrespective of the way in which the individual transaction handling systems 20, 21 are linked to the electronic financial services exchanger 10. The principle of the electronic financial services exchanger 10 now permits flexible linking of differing communication devices 30, 31 as well as various transaction handling systems 20, 21 from a variety of different financial service providers 43, 44. Confidential data requiring a secure exchange is now no longer done directly from communication device 30 to communication device 31 but - where possible at all - via standardized maximum security communication links and the electronic financial services exchanger 10 in the sense of a platform. The transaction partners, users 40 and 41 are established via a token loop (e.g. TAN loop). For each financial transaction the electronic financial services exchanger 10 generates a token (e.g. TAN) 42 which is communicated to the user 41 in the role of the transaction initiator, received by the other user 40 by an intentional transaction and returned as confirmation to the electronic financial services exchanger 10.

Abstract

Method and system for secure handling of electronic financial services with the aid of an electronic financial services exchanger

Defined is a method of exchanging, handling and controlling electronic financial services, particularly mobile electronic financial services from various financial service providers to authorized users with a wide variety of communication devices (both stationary and mobile).

The system provides for the exchange of electronic financial services all services of the connected transaction handling systems 20, 21 from financial service providers 43, 44 in the form of a standardized platform by means of corresponding interfaces 13, 14 irrespective of the way in which the individual transaction handling systems 20, 21 are linked to the electronic financial services exchanger 10.

The principle of the electronic financial services exchanger 10 now permits flexible linking of differing communication devices 30, 31 as well as various transaction handling systems 20, 21 from a variety of different financial service providers 43, 44.

Confidential data requiring a secure exchange is now no longer done directly from communication device 30 to communication device 31 but – where possible at all – via standardized maximum security communication links and the electronic financial services exchanger 10 in the sense of a platform.

The transaction partners, users 40 and 41 are established via a token loop (e.g. TAN loop). For each financial transaction the electronic financial services exchanger 10 generates a token (e.g. TAN) 42 which is communicated to the user 41 in the role of the transaction initiator, received by the other user 40 by an intentional transaction and returned as confirmation to the electronic financial services exchanger 10.

Payment Method and System

Prior art

In the field of electronic financial services, especially electronic payment services and more particularly mobile electronic payment services a plurality of different systems are currently in use which are hardly, or not at all, intercompatible, the greatly different stationary and mobile communication devices of which communicate via proprietary protocols with proprietary mainframe computers of the financial service providers.

Current mobile electronic payment systems greatly depend on the communication device used, the selected mobile wireless network operator as well as on the financial service provider.

This situation is a serious obstacle to making use of mobile payment systems in full scope and thus cost-effectively.

In addition, the systems in use in the marketplace to date are based on a direct connection between the terminals or mobile communication devices of the payment partners.

In this arrangement, for each payment transaction security-relevant or confidential information (for example bank account data of the payer and/or of the payee, the mobile communications number of the payer and/or of the payee etc.) is disclosed to the corresponding partner or communicated between the payment partners.

User authentication in established mobile payment systems is as a rule via the SIM card (subscriber ID module) of the mobile telephone and is thus dedicated to the device.

The established systems thus harbor the risk of being inherently open to misuse when the mobile telephone is stolen, with the risk of eavesdropping in the communication of user and invoice data from one mobile telephone to another with no possibility of anonymous payment.

Furthermore, established systems, especially on payment from one mobile communication device to another (peer-to-peer payment) necessitate a uniform access convention, i.e. it not being possible that the payee initializes the payment transaction via an online connection (e.g. with a WAP browser) whilst the payer concludes payment by SMS.

Laid-open document DE 100 28 238 A1 describes a securities trading system on the basis of portable devices in which trading the securities is possible from security trading locations connected to the system via a uniform trading communications protocol and the trading transactions are performed by the connected security trading subsystems. The system as described is not conceived as an open non-earmarked payment system.

Laid-open document US 2001/0037264 describes a method and a system which in making use of the existing infrastructure of mobile wireless network operators enables customers by mobile wireless telephone to select, order and pay for merchandize in an online shop from a catalog by

charging the amount to the mobile wireless account.

It is characteristic of the method that it is tied to a special mobile wireless operator or mobile wireless operator association, i.e. users not signed with this particular mobile wireless operator cannot use the system.

Described in laid-open document WO 98/47116 A1 is a method for performing payments from a customer to a merchant by telecommunication means as well as a corresponding device for performing the method. In this method the customer in the role as payer initiates payment by communicating by means of his mobile wireless telephone at least one merchant ID and the amount to be paid to a so-called telepay means which can connect to the bank of the customer, the bank of the merchant and to the merchant himself. The telepay means sends, among other things, the corresponding confirmation of receipt to the merchant. After having received the confirmation message from the merchant, the telepay means credits the merchant account and debits the customer account.

Characteristic of this method is that the payer initiates payment and is responsible for ensuring correct entry of the payment data with no error. Furthermore, use of this method is dedicated to one particular mobile telephone, since to authenticate payment use is made of data stored on the SIM card of the mobile telephone for ID and authentication.

Described in laid-open document WO 98/52151 is a method and a device for performing electronic transactions, particularly payments, using asymmetric encryption. In this method the transaction data is likewise entered solely by the customer and the transaction initiated. The customer has sole responsibility for forming the transaction message and communicating it by means of a digital signature generated by means of data stored on the SIM card of his mobile telephone. This transaction message is communicated to a banking means which checks the digital signature and prompts performance of the transaction. Using a digital signature permits communication of the transaction message over non-secure communication channels and verification that the transaction message has not been changed during communication.

With this method too, it is characteristic that solely the customer is responsible for entering the transaction data free of error and that the user is tied to one particular mobile telephone.

Described in German patent DE 199 03 822 C2 (of which an English language equivalent has been published as Canadian Patent Publication 2,361,489) is a method and a system for cashless payment. The merchant in the role of the payee starts the payment transaction by entering the payment data preferably at a stationary merchant station, particularly on his mobile telephone. From here the data together with the merchant ID is sent to a verification means. The verification means checks in making use of the data received by merchant station whether the merchant station is permitted to perform payment transactions and, if so, opens a payment transaction, the customer in the role of the payer confirms the opened payment transaction either by entering the ID of the merchant into his mobile telephone, receives it via an infrared connection from the merchant station and then communicates it together with the ID data to the verification means, or

by communicating it via a voice connection to the verification means. When the confirmation sent by the customer matches an open payment transaction, the payment data is communicated to the mobile wireless telephone of the customer so that payment can be ultimately confirmed by the customer.

Characteristic of this method is that the merchant is responsible for entering the invoice data and payment data and the payment transaction is simpler for the customer. What is a disadvantage is that only one open payment transaction is allowed per merchant station as is inherent to the method, i.e. subsequent customers are forced to wait until the person beforehand has completed his payment transaction.

Point of sale direct debit systems currently in use require a payer to provide identification about himself and the intended source of funds (e.g. an account with a financial institution such as a bank) through a terminal (for example by "swiping" a direct debit card) and entering a personal identification number (PIN) into a system in which such information is matched to information provided by the payee as to the value of the transaction and the amount is then debited against the payer's account with the financial institution associated with the information provided and credited to the payee's account.

However, current systems lack desirable flexibility both from the point of view of enabling the parties to choose the accounts that they wish to use for any transaction and having regard to the technical means used for participating in the transaction.

The present invention provides a financial exchange database or inter-connected databases (herein referred to as a financial services exchanger) in which the necessary data is stored to provide flexibility from either or both of these aspects. Such database or databases can be accessed in real time to permit a transaction to proceed.

Such database or databases will contain identifier information about subscribers to the system and from one aspect also contain information as to accounts with financial institutions that may be involved in transactions that may be carried out using information contained in the database or databases.

Alternatively or additionally they may contain information as to the technical interfaces that may be used to communicate with parties who are subscribers to the system and have their details entered into the database or databases.

Said financial services exchanger may store data in any convenient form in which it may be accessed automatically in real time including, for example, by electrical, magnetic or optical methods. For example, the financial services exchanger may comprise a server in a computerized system.

User access to a system comprising said financial services exchanger may be by any convenient means permitting real time communication. Suitable communication devices for this purpose

include personal computers, land-line based telephones, mobile telephones and other wireless communication devices and other fixed or mobile terminals. Such communication devices may be equipped with means for authenticating users employing the system which may be compared with user information stored in the financial services exchanger for the purposes of authenticating the identity of the user.

From another aspect, the present invention provides a mobile payment system for operation in full scope and thus cost-effectively must, among other things:

- offer as many means of combination as possible for the communication devices used,
- permit integrating as many electronic payment systems as possible already in successful operation to achieve cost-effective and speedy implementation,
- permit use of existing current, cash card and credit card accounts of users to attain high acceptance,
- permit as a platform as many different means of access (HTML, WAP, SMS, voice etc) as possible without requiring the basic financial service process to be adapted,
- be independent of the selected mobile wireless operator of the user
- permit user authentication irrespective of the hardware involved and be immune to interference.

The invention may be used to define a method for communicating electronic financial services of diverse financial service providers to authorized users with all sorts of communication devices (both stationary and mobile) and to control handling thereof.

In another aspect, the invention provides a method for secure handling of electronic financial services by means of:

- an electronic financial services exchanger,
- a communication device associated with a first user in the role of the transaction initiator, preferably the payee, connected by an interface to the electronic financial services exchanger,
- a communication device associated with a second user in the role of the transaction handler, preferably the payer, connected by an interface to the electronic financial services exchanger,
- at least one financial account associated with a first user serviced by at least one financial service provider,
- at least one financial account associated with a second user serviced by at least one financial service provider,
- at least one transaction handling system associated with at least one financial service provider for accessing the financial accounts and of each of the users respectively

comprising the steps

- assigning each user to the electronic financial services exchanger using communication devices by the users entering a dedicated ID code and a secret code or other characteristic information of that user into communication devices for communication to the electronic financial services exchanger,

- authenticating the said users using the secret or characteristic information of users saved in the electronic financial services exchanger by the electronic financial services exchanger comparing the communicated assignment data of the users to the secret information saved in the electronic financial services exchanger,
- initiating a financial service transaction by the transaction initiator,
- entering the transaction parameters in a communication device by either party (typically, but not necessarily the transaction initiator),
- secure communication of the transaction parameters to the electronic financial services exchanger by said communication device,
- allocating a token (for example a transaction number TAN) representing the initiated financial service transaction and the data thereof by the electronic financial services exchanger,
- communicating the token (e.g. a TAN) to the communication device of the transaction initiator by the electronic financial services exchanger,
- communicating the TAN from the transaction initiator to the other user,
- accepting the token (e.g. a TAN) in the communication device of the other user,
- communicating the token (e.g. a TAN) together with the user ID from the other user to the electronic financial services exchanger by a communication device,
- establishing the financial service providers associated with the transaction partners by the electronic financial services exchanger,
- requesting the transaction handling systems to handle the transaction by the electronic financial services exchanger,
- handling the transaction by the transaction handling systems using the financial accounts of the users,
- evaluating the response messages from the transaction handling systems of the users by the electronic financial services exchanger,
- sending messages acknowledging handling of the transaction to the communication devices employed by the users by the electronic financial services exchanger.

The financial services exchanger used in this method is desirably of the type noted above including a database or inter-active databases that contain identifier information about potential users of the method together with the necessary information about either or both of their financial account information that will be used in transactions to be carried out using the method and the electronic interface information as to how to contact users of the method electronically.

Useful ways of implementing the above described method include one wherein

- the electronic financial services exchanger comprises a data storage for records of the transaction in which the records associated with a transaction are stored for the users,
- after sending messages confirming handling of the transaction the following steps are additionally involved:
 - generating a duplicate record of the transaction for the transaction initiator by the electronic financial services exchanger,
 - storing the duplicate record of the transaction by the transaction data storage,

- generating a duplicate record of the transaction for the other user by the electronic financial services exchanger,
- storing the duplicate record of the transaction by the transaction data storage.

Useful ways for effecting data storage include inter alia hard drives, portable disks, semiconductor chips, holographic storages, magneto-optical memories, nanotubes, micro-electro-mechanical systems (MEMS), DNA storages.

In another useful method

- at least one of the communication devices used comprises means for sensing biometric or other characteristic data of one or more of the users and communicating same either untouched or compressed to the electronic financial services exchanger,
- at least one user entering a dedicated ID code in said communication devices and each communicating their biometric data to said communication device,
- authentication at least one of the users is done using secret information of the user saved in the electronic financial services exchanger by the electronic financial services exchanger comparing the communicated assignment data of at least one of the users to the biometric data saved in the electronic financial services exchanger.

The invention further comprises a system that may be of use for implementing one or more of said methods.

In one aspect such a system comprises

- an electronic financial services exchanger for central control of the complete method, comprising
- a user data storage for storing the data of all registered users, the financial account data to the accounts of the said users,
- a service provider data storage for storing the data of financial service providers including the access data to the transaction handling systems,
- at least one communication device for use by a user and connected via an interface to the electronic financial services exchanger,
- at least one financial account associated with a first user and serviced by the financial service provider,
- at least one transaction handling system assigned to a financial service provider for performing electronic transactions, preferably electronic crediting, on the financial account of the user and connected via an interface to the electronic financial services exchanger,
- at least one communication device for use by a second user and connected via an interface to the electronic financial services exchanger,
- at least one financial account associated with the first user and serviced by a financial service provider,

- at least one transaction handling system assigned to a financial service provider for performing electronic transactions, preferably electronic debiting on a financial account of the second user and connected via an interface to the electronic financial services exchanger.

Said system may additionally be of a type wherein at least one of the communication devices is a means of mobile telecommunication.

In a further aspect, the electronic financial services exchanger may comprise a data storage for records of the transaction in which the record of the transaction associated with a transaction are stored for the users.

The system as described above may usefully provide sensors for sensing data characteristic of the user, for example biometric, behavioral characteristic or physiological characteristic data of the users and communicating same either untouched or compressed to the electronic financial services exchanger.

Such sensors may "read" any pertinent data such as biometric data such as fingerprints or retina or iris patterns or physiological data such as voice profiles . Sensors for such data are commercially available.

Brief Description of the Drawings

Figure 1 shows the system architecture of a system according to the present invention

Figures 2, 3 and 4 show a flow sequence of events in a method according to the present invention.

Abbreviations

COD	=	communication device
EFSE	=	electronic financial services exchanger
FAC	=	financial account
FSP	=	financial service provider
FSPDS	=	financial service provider data storage
IF	=	interface
TAR	=	transaction record
TARS	=	transaction record storage
THS	=	transaction handling system
UDS	=	user data storage

Detailed Description of the Invention

For communicating electronic financial services the system provides all services of the linked transaction handling systems 20, 21 from financial service providers 43, 44 in the form of a standardized platform. This is achieved by corresponding interface 13, 14 irrespective of the way in which the individual transaction handling systems 20, 21 are connected to the financial services exchanger 10.

Each service user 40, 41 makes connection via a communication device 30, 31, preferably a mobile wireless telephone, to the financial services exchanger 10, signs on and is able to prompt the wanted financial service. The financial services exchanger 10 identifies and authenticates the necessary financial service providers 43, 44, polls the needed data and coordinates the financial transactions associated with the financial service which are handled by the transaction handling systems 20, 21 of the financial service providers 43, 44 in making use of the financial accounts 22, 23.

The principle of the electronic financial services exchanger 10 now makes it possible to flexibly link the various communication devices 30, 31 as well as the diverse transaction handling systems 20, 21 from the various financial service providers 43, 44.

The exchange of confidential data as is critical to security is now no longer peer-to-peer, i.e. direct from communication device 30 to communication device 31 but, where at all possible, via standardized maximum security communication links and the electronic financial services exchanger 10 in the sense of a platform.

The consequential use of tokens (e.g. transaction numbers) 42 as is novel in accordance with the invention now makes it possible to handle financial transactions, preferably payment transactions, without communicating or disclosing confidential data of the transaction partners.

The token principle is easy to display in mobile payment as the preferred means of transaction.

The user 41 in the role of the payee starts the payment transaction by communicating the record of the transaction data to the electronic financial services exchanger 10 via a secure standard communication link for example via HTML, WAP or SMS.

The electronic financial services exchanger 10 generates a token, e.g. a transaction number (TAN) 42 and returns it to the user 41.

The generated token (e.g. TAN) 42 represents the commenced payment transaction and the record of the transaction data contained therein, data as to the user 41 and as to his financial account 23, the financial service provider 44 as well as the transaction handling system 21 thereof.

The token (e.g. TAN) 42 is totally uncritical for the user 41 and can thus be communicated as often as is required, preferably by it being displayed to the user 40 in the role of the payer.

Since the token (e.g. TAN) 42 comprises no large data volume, it can be communicated very simply and reliably.

No matter how the user 40 receives the token (e.g. TAN) 42, it is not passed on to the electronic financial services exchanger 10 until as signaled by the user 40 in context with the user 41 as the payee and declares the commenced transaction by the user 40 as the active payer as legally binding by he entering the token (e.g. TAN) 42 on his communication device 30.

The basic use of tokens (e.g. transaction numbers) in conjunction with a change in the communication medium now achieves maximum possible security in assuring that only the transaction partners actually involved, preferably payment partners, can take part in the transaction.

In addition to this, making use of transaction numbers now makes it possible that, for example, a payee can initiate several payment transactions in parallel, since the individual transactions now remain separate by the dedicated tokens (e.g. transaction numbers).

Example Embodiment

With reference to the drawing as shown in FIGS. 1 to 4 a preferred example embodiment of the invention will now be detailed relating to mobile payment from a communication device 30 of a user 40 to a second communication device 31 of the user 41.

This example embodiment was selected because it is achievable directly with mobile wireless telephones as preferably currently available and thus the operator of such a system can count on relatively low starting costs.

Referring now to FIG. 1 there is illustrated the basic architecture of the system as set forth in claims 4 to 7, whereas FIGs. 2, 3 and 4 illustrate the sequence of the method as it reads from claims 1 to 3.

The requirement for making use of the financial service in accordance with the method or system in accordance with the invention is that both the users 40, 41 as well as the financial service providers 43, 44 are memorized in the user data storage 15 and service provider data storage 16 respectively and are registered with the electronic financial services exchanger 10.

When a user 40, 41 wishes to accept e.g. electronic credit cards he additionally requires the corresponding acceptance agreements with the corresponding credit or cash card institute.

The user 41 in the role of the payee selects in step 1 on his communication device 31 the function „payment received“ and then enters in step 2 the necessary data (preferably amount of payment, currency, VAT included /not included).

In step 3 the electronic financial services exchanger 10 receives the order for payment handling and in the preferred version of the method in step 5 generates for current mobile wireless telephones (status 08. 2004) a token (e.g. transaction number TAN) 42 which is displayed on the communication device 31 of the payee (user 41).

So that the financial services exchanger 10 can identify the payer (user 40) the payee (user 41) informs the payer (user 40) in step 6 the token (e.g. TAN) 42 typically by voice, telephone in particularly also in writing. The payer (user 40) enters this token (e.g. TAN) 42 into his communication device 30 (step 7). After communication of the token (e.g. TAN) 42 to the electronic financial services exchanger 10 in step 8 the payment partners (users 40 and 41) are fully known for the financial services exchanger 10.

On the basis of the known payment partners (users 40 and 41) the financial services exchanger 10 in using the data stored in the user data storage 15 and service provider data storage 16 as well as the data entered by the payer (user 40) establishes in step 9 and step 10 both the financial service provider 43 of the payer (user 40) and the associated transaction handling system 20 as well as the financial service provider 44 of the payee (user 41) and the associated transaction handling system 21.

In step 11 the financial services exchanger 10 sends an request to check the account to each of the transaction handling systems 20, 21 of the payment partners (users 40 and 41).

The transaction handling system 20 responsible for the payer (user 40) checks in steps 12 and 14 whether a financial account 22 exists with the account ID (typically the account No.) stored in the user data storage 15 and whether the wanted payment transaction can be handled (typically by questioning coverage).

The transaction handling system 21 responsible for the payee (user 41) checks in step 13 whether a financial account 23 with the account ID (typically the account No.) stored in the user data storage 15 exists and whether the wanted payment transaction can be handled.

As soon as the positive confirmations in checking the corresponding financial accounts 22, 23 have been received by the financial services exchanger 10 from the transaction handling systems 20, 21 (steps 15 and 16) the cash transfer transactions involved in the payment transaction are requested by the financial services exchanger 10 with the transaction handling systems 20, 21 (step 17).

Once all necessary cash transfer transactions have been successfully concluded and the corresponding concluding confirmations of the cash transfer having been received by the financial services exchanger 10 (steps 19 and 21) the financial services exchanger 10 sends confirmation of payment respectively to the communication device 30 of the payer (user 40) and to the communication device 31 of the payee (user 41) (steps 22 to 24).

If desired by the users 40, 41 the financial services exchanger 10 can generate a duplicate record of the transaction 51 for the payee (user 41) in step 26 and a duplicate record of the transaction 50 for the payer (user 40) in step 25 for storing in the record of the transaction in data storage 17. Both records of the transaction can be viewed at any time on a communication device via the financial services exchanger 10 by the respectively record of the transaction owner (users 40 and 41).

CLAIMS

1. A method for secure handling of electronic financial services by means of:
 - an electronic financial services exchanger,
 - 5 - a communication device associated with a first user in the role of the transaction initiator, preferably the payee, connected by an interface to the electronic financial services exchanger,
 - a communication device associated with a second user in the role of the transaction handler, preferably the payer, connected by an interface to the electronic financial services exchanger,
 - 10 - at least one financial account associated with a first user serviced by at least one financial service provider,
 - at least one financial account associated with a second user serviced by at least one financial service provider,
 - 15 - at least one transaction handling system associated with at least one financial service provider for accessing the financial accounts and of each of the users, respectively,
 - comprising the steps
 - assigning each user to the electronic financial services exchanger using communication devices by the users entering a dedicated ID code and a secret code or other characteristic information of that user into communication devices for communication to the electronic financial services exchanger
 - 20 - authenticating the said users using the secret or characteristic information of users saved in the electronic financial services exchanger by the electronic financial services exchanger comparing the communicated assignment data of the users to the secret information saved in the electronic financial services exchanger,
 - 25 - initiating a financial service transaction by the transaction initiator,
 - entering the transaction parameters in a communication device by either party,
 - 30

- secure communication of the transaction parameters to the electronic financial services exchanger by said communication device,
 - allocating a token representing the initiated financial service transaction and the data thereof by the electronic financial services exchanger,
 - 5 - communicating the token to the communication device of the transaction initiator by the electronic financial services exchanger,
 - communicating the token from the transaction initiator to the other user,
 - accepting the token in the communication device of the other user,
 - 10 - communicating the token together with the user ID from the other user to the electronic financial services exchanger by a communication device,
 - establishing the financial service providers associated with the transaction partners by the electronic financial services exchanger,
 - requesting the transaction handling systems to handle the transaction
 - 15 by the electronic financial services exchanger,
 - handling the transaction by the transaction handling systems using the financial accounts of the users,
 - evaluating the response messages from the transaction handling systems of the users by the electronic financial services exchanger,
 - 20 - sending messages acknowledging handling of the transaction to the communication devices employed by the users by the electronic financial services exchanger.
2. A method according to claim 1, wherein
- 25 - the electronic financial services exchanger comprises a data storage for records of the transaction in which the records associated with a transaction are stored for the users,
 - after sending messages confirming handling of the transaction the following steps are additionally involved:
 - 30 - generating a duplicate record of the transaction for the transaction initiator by the electronic financial services exchanger,

- storing the duplicate record of the transaction by the transaction data storage,
 - generating a duplicate record of the transaction for the other user by the electronic financial services exchanger,
 - 5 - storing the duplicate record of the transaction by the transaction data storage.
3. A method according to claim 1 or claim 2, wherein said data storage may comprise hard drives, portable disks, semiconductor chips, holographic storages, magneto-optical memories, nanotubes, micro-electro-mechanical
- 10 systems (MEMS), DNA storages.
4. A method according to any one of claims 1 to 3, wherein
- at least one of the communication devices used comprises means for
 - 15 sensing biometric or other characteristic data of one or more of the users and communicating same either untouched or compressed to the electronic financial services exchanger,
 - at least one user entering a dedicated ID code in said communication devices and each communicating their biometric data to said communication
 - 20 device,
 - authentication of at least one of the users is done using secret information of the user saved in the electronic financial services exchanger by the electronic financial services exchanger comparing the communicated assignment data of at least one of the users to the biometric data saved in the
 - 25 electronic financial services exchanger.
5. A system for implementing one or more methods according to any one of claims 1 to 4, which comprises
- an electronic financial services exchanger for central control of the
 - 30 complete method, comprising
 - a user data storage for storing the data of all registered users, the financial account data to the accounts of the said users,

- a service provider data storage for storing the data of financial service providers including the access data to the transaction handling systems,
 - at least one communication device for use by a user and connected via an interface to the electronic financial services exchanger,
 - at least one financial account associated with a first user and serviced by the financial service provider,
 - at least one transaction handling system assigned to a financial service provider for performing electronic transactions, preferably electronic crediting, on the financial account of the user and connected via an interface to the electronic financial services exchanger,
 - at least one communication device for use by a second user and connected via an interface to the electronic financial services exchanger,
 - at least one financial account associated with the second user and serviced by a financial service provider,
 - at least one transaction handling system assigned to a financial service provider for performing electronic transactions, preferably electronic debiting on a financial account of the second user and connected via an interface to the electronic financial services exchanger.
6. A system according to claim 5, wherein at least one of the communication devices is a means of mobile telecommunication.
7. A system according to claim 5 or claim 6, wherein the electronic financial services exchanger comprises a data storage for records of the transaction in which records associated with a transaction are stored for the users.
8. A system according to any one of claims 5 to 7, wherein sensors are provided for sensing data characteristic of the user, for example biometric, behavioral

characteristic or physiological characteristic data of the users and communicating same either untouched or compressed to the electronic financial services exchanger.

- 5 9. A system according to claim 8, wherein sensors read any pertinent data such as biometric data such as fingerprints or retina or iris patterns or physiological data such as voice profiles.

1 Drawings

1.1 System Architecture

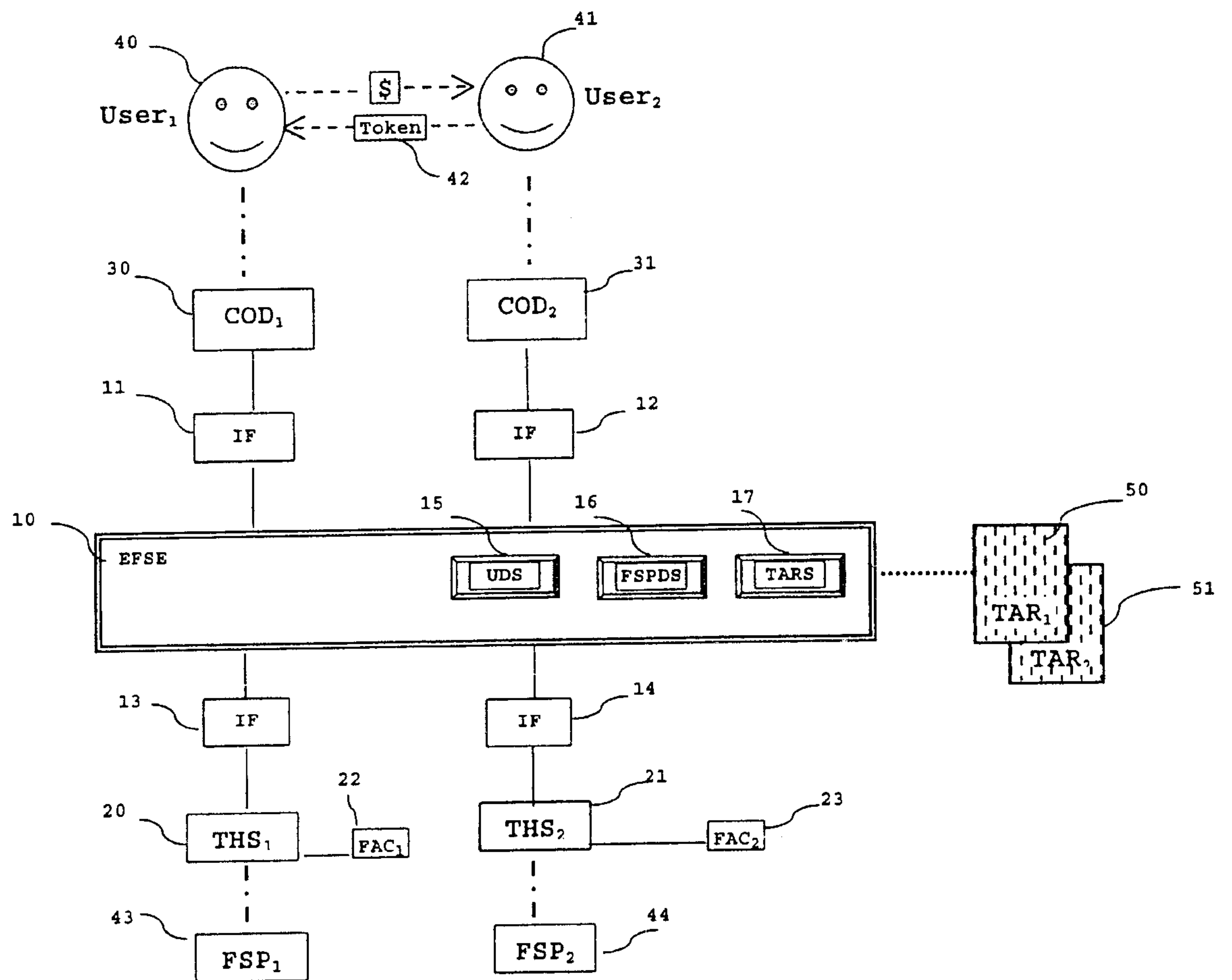


Fig. 1

1.3 Flow chart of a method according to the present invention

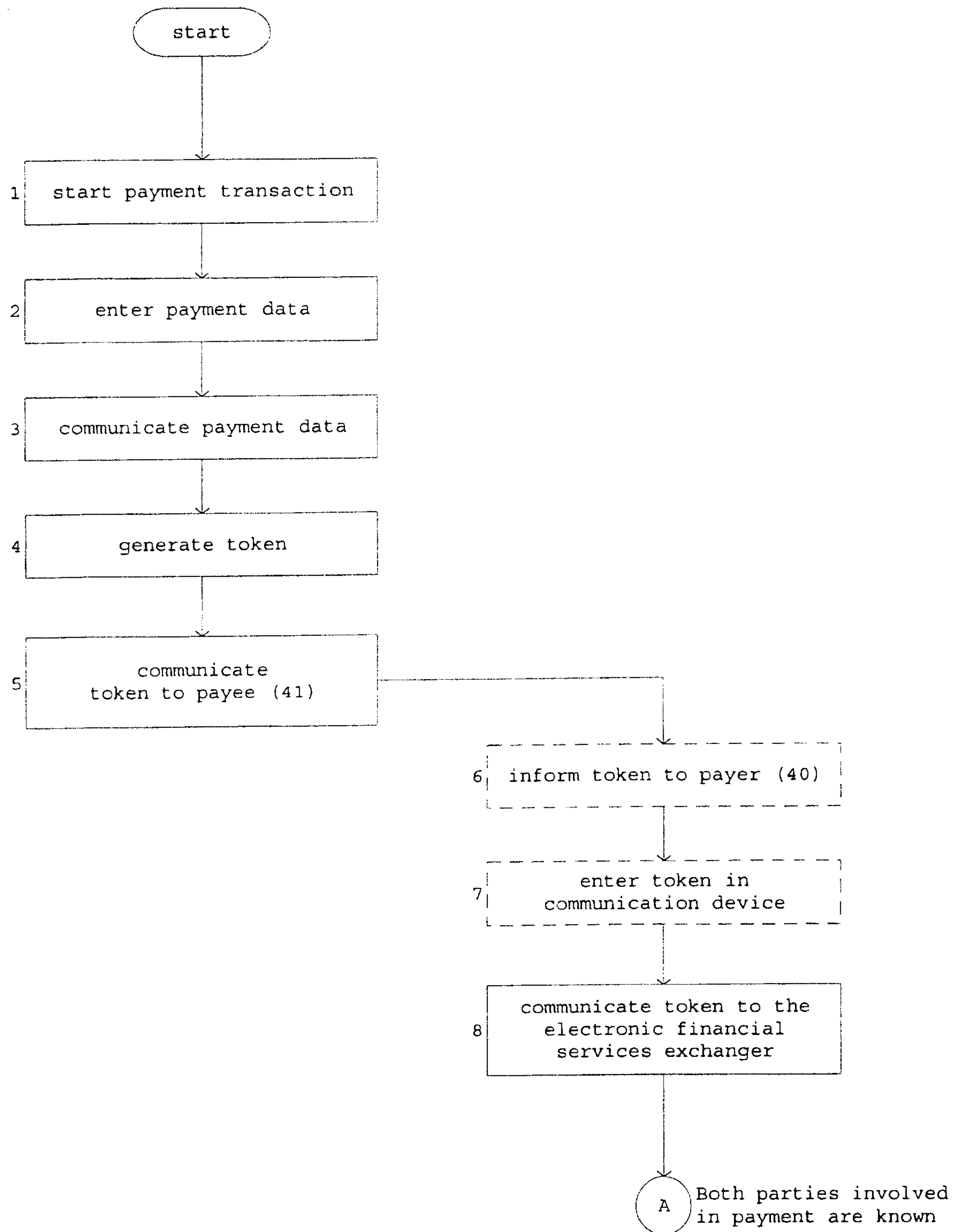
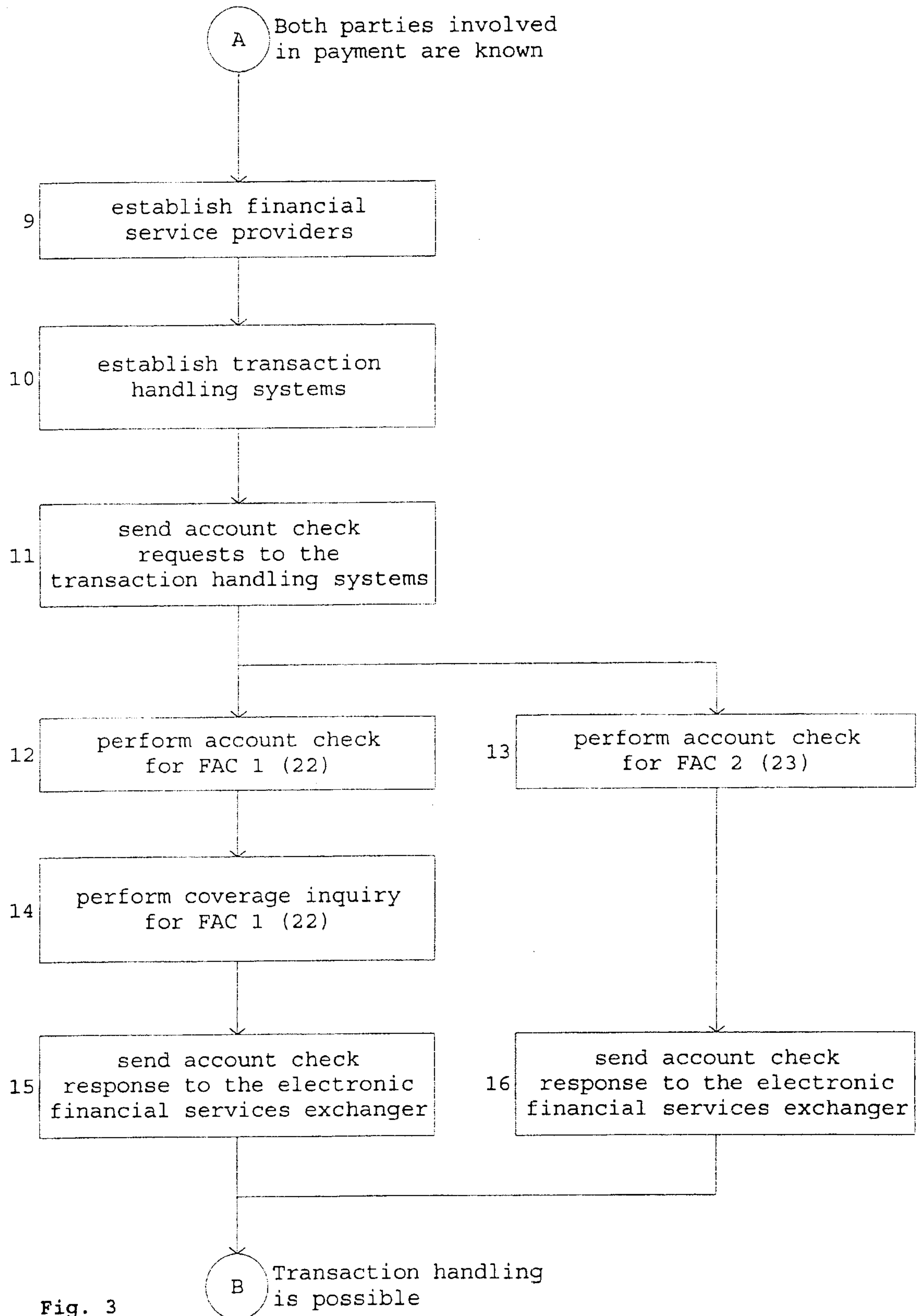


Fig. 2



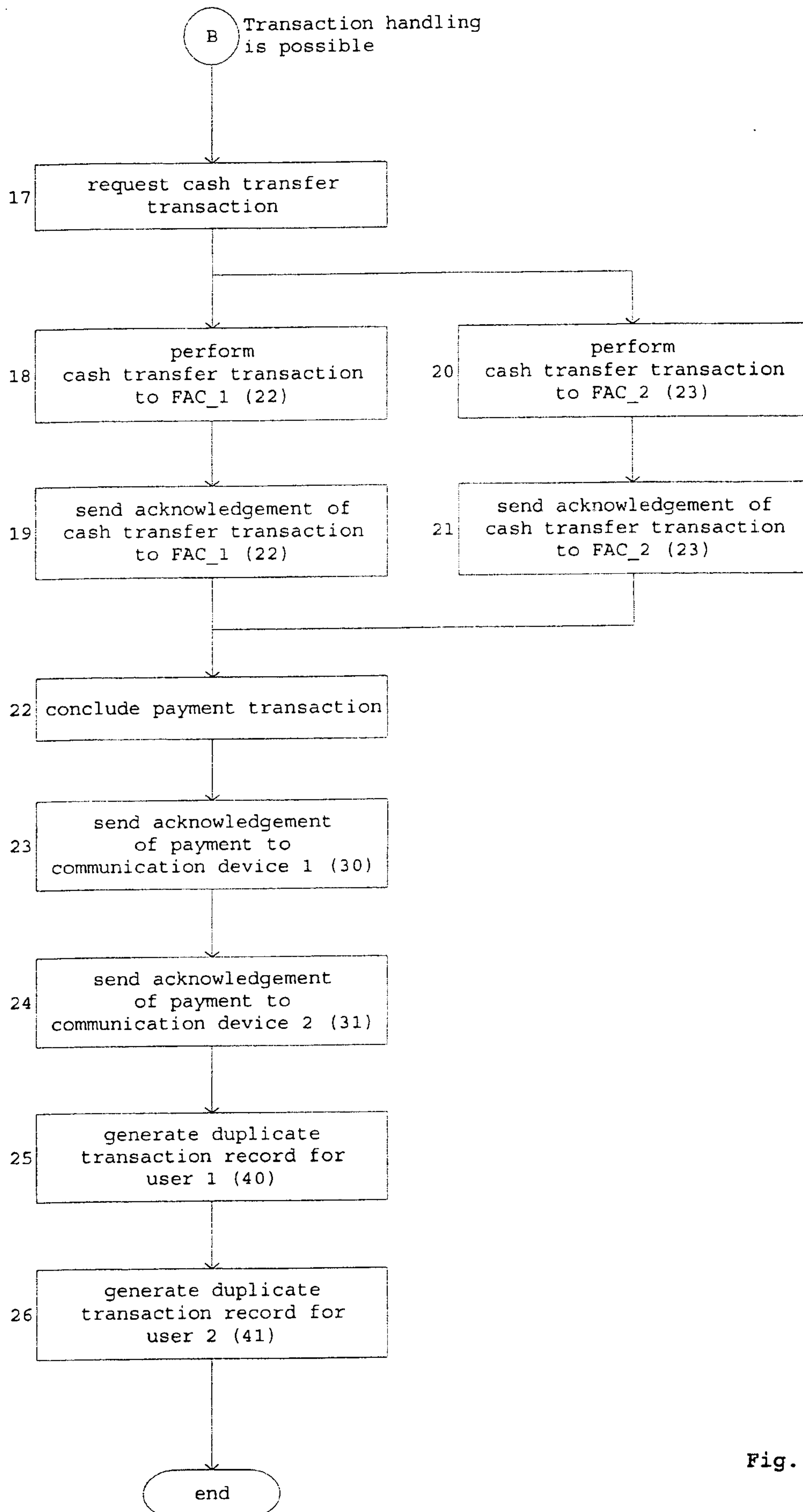


Fig. 4

System Architecture

