

DESCRIPTION

Electronic payment method

5 TECHNICAL FIELD

The invention relates to the field of electronic payment and particularly relates to an electronic payment method not requiring a bank card.

10 PRIOR ART

Payment by bank card, in which a customer presents his bank card to an electronic payment terminal (EPT) of a merchant, is known.

15 Payment by bank card does however have a certain number of drawbacks for both merchants and consumers alike.

- For merchants:

- it involves high transaction costs,
- it requires a large number of intermediate parties,
- it leads to a transaction that is relatively lengthy (approximately 15s)
- 20 - it is subject to bank card fraud which is considerable,
- it requires a payment terminal (leased or purchased) to receive payments by bank card,
- it complicates payments over the Internet due to the 3DSecure™ system and the requirement for strong authentication to validate payments,
- 25 - the complexity gives rise to friction, which has the consequence of a loss of turnover for e-commerce merchants or merchants due to a high cart abandonment rate at the time of payment.

- For consumers:

- 30 - it requires an annual payment according to the type of bank card,
- it is subject to a possible billing of charges on cash withdrawals,
- the bank card is sometimes accepted to a limited extent by some merchants (requirement for a minimum amount),
- the bank card has upper limits on payments and withdrawals,

- it is impossible to make payments between private individuals,
- it is not possible to manage a deferred or immediate debit on one and the same card,
- upper payment limits exist for contactless payments.

5 To avoid use of the bank card, solutions involving a smartphone have begun to appear. These solutions make it possible to dematerialize the bank card but still have the drawbacks of payment by bank card.

 There is a need to simplify payments by dispensing with the system of payment by bank card.

10

SUMMARY OF THE INVENTION

 The aim of the invention is to make provision for a payment and receipt solution that is simple, fast, secure, and that does not use a bank card, both for
15 payments made physically and for online payments.

 For this purpose, the invention makes provision according to a first aspect for an electronic payment method, comprising the following steps, implemented by a payment server:

- receiving a transaction message from a merchant terminal, the transaction
20 message comprising an amount of a sale to a customer, the amount of the sale having been entered by means of a merchant terminal;
- generating a transaction fingerprint from the received transaction message, the fingerprint comprising the amount of the sale and an identity of the merchant known to the payment server in the form of a format which can be acquired by
25 acquiring means of a customer terminal;
- sending the generated fingerprint to the merchant terminal, the merchant terminal being configured to present the fingerprint to a customer terminal;
- receiving a sale message from a customer terminal, the sale message comprising an item of information relating to an amount of a transaction and an item
30 of information relating to an identity of a merchant, the sale message having been generated by the customer terminal following the acquiring of the transaction fingerprint by the customer terminal, the authenticating of the customer and the validating of the transaction by the customer at the customer terminal.

Complementarily, the method comprises the following steps, implemented by a payment server:

- comparing the amount of the transaction with a payment capacity contained in a customer account stored in the payment server and if the amount of the transaction is less than or equal to the payment capacity;
- sending to a central server a message to transfer the amount of the transaction in such a way that the central server credits an operating account of the merchant with the amount of the transaction minus a commission, debits an operating account of the customer and credits a central operating account with the commission;
- sending to the central server an order to debit the debit balance of the customer operating account from the customer bank account (11) to the central operating account of the central bank
- sending an order to transfer the balance from the operating account of the merchant to the merchant bank account;
- receiving from the central server a notification that the debit balance of the customer operating account has been debited.

According to an embodiment, the fingerprint is a QR code, a near-field communication tag, a 6-figure numerical code, a Bluetooth Low Energy communication tag.

- According to an embodiment, if the amount of the transaction is greater than a payment capacity contained in the customer account, sending to the merchant terminal a notification of abandonment of the transaction and sending to the customer terminal a notification of refusal of the transaction.

According to an embodiment, the debit order is sent with every transaction or else periodically on a given schedule, once a day or once a month at the end of the day or at the end of the month.

According to an embodiment, the method comprises the following steps implemented by a customer terminal:

- acquiring the fingerprint sent by the payment server and presented to the customer by means of a merchant terminal;
- authenticating a customer;
- validating the transaction of the customer by way of the customer terminal;
- generating the sale message;
- sending the sale message to the payment server.

According to an embodiment, the acquiring of the fingerprint triggers the opening of an application stored on the customer terminal, the application making it possible to authenticate the customer and validate the transaction.

According to an embodiment, the method comprises the following steps
5 implemented by a merchant terminal:

- generating the transaction message comprising the amount of the sale
- sending the transaction message to the payment server
- presenting the fingerprint, received from the payment server, to the customer.

According to a second aspect, the invention relates to a payment server
10 comprising a processing unit configured to implement a method according to the first aspect of the invention.

According to a third aspect, the invention relates to a payment method implemented by a customer terminal comprising the following steps:

- acquiring the fingerprint sent by the payment server;
- 15 - authenticating a customer;
- validating of the transaction by the customer;
- generating the sale message;
- sending the sale message to a payment server according to the second aspect of the invention.

20 According to a fourth aspect, the invention relates to a payment method comprising the following steps implemented by a merchant terminal:

- entering of a sale by the merchant, the entry comprising the amount of the sale;
- generating the transaction message comprising the amount of the sale
- 25 - sending the transaction message to a payment server according to the second aspect of the invention;
- presenting the fingerprint, received from the payment server according to the second aspect of the invention, to the customer.

According to a fifth aspect, the invention relates to a computer program
30 product comprising instructions, which when the program is executed by a computer, lead it to implement the steps of the method according to one of the aspects of the invention.

According to a sixth aspect, the invention relates to an electronic payment method, comprising the following steps:

- entering a sale by means of a merchant terminal,
- generating, by the merchant terminal, the transaction message comprising the amount of the sale,
- sending, by the merchant terminal, the transaction message to a payment server,
- receiving, by a payment server, a transaction message from a merchant terminal, the transaction message comprising an amount of a sale to a customer;
- generating, by a payment server, a transaction fingerprint from the received transaction message, the fingerprint comprising the amount of the sale and an identity of the merchant known to the payment server;
- sending, by a payment server, the generated fingerprint to the merchant terminal configured to present the fingerprint to a customer;
- presenting, by means of the merchant terminal, the fingerprint received from the payment server to the customer;
- receiving a sale message from a customer terminal, the sale message comprising an item of information relating to an amount of a transaction and an item of information relating to an identity of a merchant, the sale message having been generated by the customer terminal following the acquiring of the transaction fingerprint by the customer terminal, the authenticating of the customer and the validating of the transaction by the customer at the customer terminal.

The invention according to one of the aspects set out above has the following advantages.

The invention makes it possible to finally dispense with the use of a bank card, even a remote one, presented to an electronic payment terminal.

The invention does not require any prior recharging of the account, due to its operation by debits (unlike solutions based on the bank card).

The invention identifies all the parties to the transaction, which secures transactions.

The invention allows for very fast payment since by dispensing with the bank card, the solution dispenses with all the usual intermediate parties to payment by bank card.

The invention allows for more secure payment than payment by bank card:

- Use of the security elements of the terminal of the bearer (pin code or biometric identification elements),

- Use of the security elements of the application of the bearer (pin code or biometric identification elements) for payments over a determined amount, for example €50,
- The amount of the payment without PIN code can be parameterized between €0 and a determined amount, for example €50 in the application according to the security requirements desired by each bearer,
- It is no longer necessary to enter or record one's bank codes to make online payments.
- No need to record one's bank card in an online wallet (of Apple Pay™, Google Pay™ type etc.),
- No transmission to the merchant of sensitive items of information relating to the bearer (account number for example). Specifically, the bank card is a payment means that takes information from the interbank system using the identification number of the card (PAN for Primary Account Number code) whereas with the invention it is the merchant who gives the item of payment information to the customer who validates the transaction. The PAN code is used by perpetrators of fraud to link the bank account of the customer to his card. The invention therefore limits fraud.

The invention allows the customer bearing the payment application according to the invention to be able to manage the debiting of his payments by choosing whether he wishes to switch from a deferred-debit payment to an immediate-debit payment.

The invention makes it possible to obtain a spending capacity according to one's resources, determined automatically during the onboarding process.

The invention does not require the precharging of one's account from the application to make purchases.

The invention does not require any entering of the amount of the transaction by the customer. Only the merchant makes this entry.

OVERVIEW OF THE FIGURES

Other features, aims and advantages of the invention will become apparent from the following description, which is purely illustrative and non-limiting, and which must be read with reference to the appended drawings on which:

- figure 1 illustrates an architecture for implementing an electronic payment method in accordance with the invention;

- figure 2 illustrates steps of an electronic payment method in accordance with the invention;

5 - figure 3 illustrates a customer terminal comprising a screen and an area of acquisition of a QR code.

On all the figures similar elements bear identical reference numbers.

DETAILED DESCRIPTION

10

Architecture

Figure 1 illustrates an architecture for implementing an electronic payment method in accordance with the invention.

15 A customer C1 accesses a sales point PdV of a merchant C2 to make a purchase. The customer C1 possesses an electronic terminal T1. The electronic terminal T1 is preferably a smartphone but can also be any item of equipment suitable for connecting to a payment server SP: touch-sensitive tablet, laptop computer, games console, smartwatch, etc.

20 The sales point PdV can be an Internet site, a physical location, etc. The sales point PdV is in particular materialized as an electronic terminal T2 also suitable for connecting to the payment server SP.

25 The terminals T1, T2 may connect to the payment server SP by means of a wireless connection, for example by Internet R. This connection may be implemented by a wired link (for example a link via optical fiber, ADSL, network etc.), a wireless link of Wi-Fi type or via a mobile communication network (3G, 4G, 5G, etc.).

30 The payment server SP is typically configured to implement processing and in this capacity comprises one or more electronic control units. Preferably, the payment server SP and the terminals T1, T2 are configured to exchange data securely via the Internet connection. Advantageously, the payment server SP and the terminals T1, T2 are configured to exchange data in a highly secure manner according to communication standards well-known to those skilled in the art. Furthermore, the payment server SP comprises one or more memories to allow the storage of various data.

To access the payment server SP, a payment application is installed on the terminal T1 of the customer C1 and the customer C1 has created a customer account 10 allowing him to use the application.

Similarly, the merchant C2 uses a dedicated application to allow him to interact
 5 with the terminal T1 of the customer C1, the merchant C2 possessing a merchant account 20 to access the payment server SP. The customer and merchant accounts, respectively 10 and 20, are stored by the payment server SP and comprise all the items of information relating to the customer and to the merchant and make it possible to trace all the transactions.

10 The customer and merchant applications use deep links which ensure increased security for the transaction. This makes it possible to limit the risks related to man-in-the-middle attacks (MITM) or interception attacks which have the aim of intercepting and modifying communications between two parties. This is because the customer and the merchant never directly communicate with one another but always
 15 go through the payment server SP.

The payment server SP is associated and connected with a central server SC of a central bank EC which makes it possible to handle banking flows such as interbank transfers of funds, particularly by bank transfer. The connection between the central server SC and the payment server SP is implemented similarly to the
 20 connection between the payment server SP and the terminals T1, T2. The payment server SP is associated with the central server SC of a central bank EC which will handle all banking flows.

Since this concerns an application allowing electronic payment, the customer C1 possesses a customer bank account 11 managed by a server S1 of a bank E1
 25 and the merchant holds a merchant bank account 21 managed by a server S2 of a merchant bank E2.

On figure 1 three separate banks are shown but one or more banks may be contiguous according to the preferences of the customer and of the merchant.

As will be understood, communications between the different servers and the
 30 terminal of the merchant and that of the customer are transported over the Internet network R and are secured according to standards well-known to those skilled in the art. The connections implemented will not be further detailed.

The terminal T1 of the customer C1 and terminal T2 of the merchant C2 may moreover be configured to communicate with one another using Near Field

Communication (NFC) or else by the Bluetooth Low Energy (BLE) communication technology.

5 Onboarding

As shown above, an electronic payment method described in relation to figure 2, requires the installation on the customer side C1 of an application on the customer terminal T1 to access the payment service. Once the application has been installed on his customer terminal T1, to be able to access the payment service, the customer C1 is onboarded onto the service (step Insc C1) via the application by creating his customer account 10.

Advantageously, the onboarding (step Insc C1) of the customer comprises the following steps:

- 15 - recording the mobile number of the customer;
- recording the postal address of the customer, complying where applicable with the legislation in effect in the country of use of the service (in France to access such a payment server, the customer must enter his tax address); to streamline such an input, provision is made for an automated address search;
- 20 - recording the place of birth of the customer;
- checking the identity of the customer: such a check may comprise the transmission of an identity document of the customer (identity card, passport, residence permit, driving license.) The copy of the document can be made using the camera of the customer terminal. Following the transmission of the identity document,
- 25 the face of the customer is then captured to check that the face of the customer matches that appearing on the identity document;
- optionally, recording the employment situation and an amount of income. As regards the employment situation a closed list is proposed to the customer so that he can choose the one that best matches him;
- 30 - recording the bank details of the customer either by entering his bank details (entering the IBAN) or by direct collection of the details from the bank of the customer (with a connection of DSP2 type). The bank details thus recorded constitute a banking authorization to debit the bank account 11 of the customer held at the bank E1 which

can be of any kind. Specifically, the payment server operates by implementing bank debits.

- accepting of the conditions of access to the service by the customer and signifying to this latter a withdrawal period;

5 - configuring a confidential PIN code to secure transactions during the use of the service and in particular to access the application implementing the service.

It can be seen that the customer C1 does not need to possess a bank card to register to finalize his onboarding and the opening of his customer account.

10 All the recorded data are attached to the customer account 10 which is stored in the payment server SP and further includes the recorded data (in particular the identity and bank details), and a payment capacity. Such a payment capacity limits the amount that the customer can use per month (in one or more transactions) to use the service and implement the electronic payment method described here. This
15 payment capacity is preferably initially set to a ceiling of low value and raised once the customer bank account 11 has been confirmed.

The onboarding of the customer is optimized in terms of the number of manual entries and validation. Specifically, the customer has only a small number of elements to input manually which reduces the risk of error and speeds up onboarding.

20 Moreover, once the registration is finished, the customer can use the service (even if he has not automatically associated his bank account via DSP2) even if his external customer bank account has not been confirmed. There is therefore no wait, and the service can be used immediately to make a payment.

25 Similarly, the merchant C2 is onboarded onto the service (step Insc C2) and possesses a merchant account 20 stored in the payment server SP. This merchant account 20 includes the identity of the merchant but also his banking details associated with its merchant bank account 21.

Advantageously, the onboarding (step Insc C2) of the merchant comprises the
30 following steps:

- recording of items of identity and contact information of the merchant: surname, first name, telephone number, postal address, e-mail address, password to access the merchant account;

- optionally, an electronic message is issued and contains a code that the merchant must enter in order to verify his e-mail address; this makes it possible to check that the e-mail address is correct;

- recording the name of the business (in France by means of the SIREN number);

- displaying the information recorded for validation by the merchant;
- recording the bank details of the merchant by entering the IBAN
- checking the identity of the merchant: such a check may comprise the transmission of an identity document of the merchant (identity card, passport, residence permit.) The copy of the document can be made using the camera of the merchant terminal. Following the transmission of the identity document, the face of the merchant is then captured to check that the face of the customer matches that appearing on the identity document;

- recording the place of birth of the merchant;
- accepting of the conditions of access to the service by the merchant.

The onboarding of the customer and of the merchant makes it possible to unambiguously identify the two parties participating in a transaction. This makes it possible to secure the transaction. This is particularly useful to combat money laundering and financing of terrorism.

The bank details will allow the initiation of banking operations required by the payment server SP to the central server SC which is authorized to implement this type of operation.

To do this, on creation of the customer and merchant accounts 10, 20, a customer operating account 12 (payment account type) and a merchant operating account 22 (payment account type) are created in the central server SC of the central bank EC with which the payment server SP is associated. These operating accounts will make it possible to manage the bank flows in a transparent manner for the customer and the merchant when the time comes.

Initiating a payment

A description will now follow of a use of the payment service by the implementation of the electronic payment method, a preferred embodiment of which is illustrated on figure 2.

A customer C1 goes to a sales point PDV to buy one or more items of goods (step 100). The customer C1 presents himself at the sales point PDV so that the merchant C2 can enter the sale (step 101). Here this is for example a conventional checkout. The sale is entered by the merchant C2 on his merchant terminal T2 and
 5 leads to the generation of a transaction message M1 comprising the amount of the sale (step 102). The transaction message M1 also comprises the identity of the merchant so that the payment server SP can identify it.

The merchant C2, via his terminal T2, validates the sale which triggers the sending (step 103) of the transaction message M1 to the payment server SP. Only
 10 the merchant C2 enters the amount of the transaction, so the customer does not have to enter such an amount.

On receiving (step 104) this transaction message M1, the payment server SP generates (step 105) a transaction fingerprint EP1 intended to be acquired/received by the customer terminal T1.

15 The transaction fingerprint EP can take several forms.

According to an embodiment the transaction fingerprint EP1 is a QR code.

According to an embodiment the transaction fingerprint EP1 is a near-field communication (NFC) tag.

According to an embodiment, the transaction fingerprint EP1 is a 6-figure
 20 numerical code.

According to an embodiment, the fingerprint EP1 is a BLE (Bluetooth Low Energy) communication tag.

This fingerprint EP1 contains the amount of the sale as well as the identity of the merchant C2 known to the payment server SP.

25 This fingerprint EP1 is stored (step 106) in the payment server SP to allow traceability of the transactions and is returned (step 107) to the terminal T2 of the merchant C2 to carry out the transaction with the customer C1.

In practice, since the fingerprint EP1 comes directly from the merchant this latter is clearly identified by the customer.

30 Alternatively, in the case of a remote payment, the fingerprint EP1 is shown to the customer via the site of the merchant. In this way, the merchant is capable of creating a transaction in different receipt situations.

By offering the fingerprint EP1, the merchant dispenses with the use of an electronic payment terminal (TPE) which reduces the costs for the merchant in terms

of equipment and computer resources and therefore energy. Moreover, since the fingerprint EP1 can take several forms, the merchant is not technologically limited. Thus, it is very easy for a merchant to offer such a payment service.

5

Transaction session

The fingerprint EP1 is presented/sent to the customer C1 (step 108) particularly by way of the merchant terminal T2; the transaction can be done physically or remotely.

10

Next, the customer C1 confirms the transaction as follows, according to the type of fingerprint EP1.

Payment by QR code

15

The customer C1 then reads the QR code by means of the terminal T1. He can either read the QR code directly with his camera or with the payment application installed on his terminal T1. Figure 3 illustrates a customer terminal T1 with the application during use. On this figure the screen S showing the area Z of acquisition of the QR code can be seen.

20

Using the camera, the reading of the QR code will trigger the opening of the payment application installed on his terminal T1.

Once the application is open, a prior authentication of the customer C1 is implemented by the terminal T1 of the customer before being able to validate a transaction. This authentication can be done for example by a recognition of a human fingerprint or facial recognition or else by entering a code.

25

Next, the customer C1 brings his customer terminal T1 close to the terminal T2 to proceed to the acquisition (step 109) of the fingerprint EP1. The terminal T1 then reads the QR code by acquiring an image of the QR code. The acquiring of the transaction fingerprint triggers a request for validation of the transaction by the customer C1 which takes the form of an authentication of the customer C1 (step 110). Note that if the customer does not have the application, the acquiring of the fingerprint will return a link to download the application to access the service.

30

Moreover, the QR code bears a deep link which makes it possible to directly access the application.

Moreover, the use of a QR code ensures security for the customer since the fingerprint systematically returns secure and certified addresses, otherwise an error
5 is returned to the customer.

Contactless payment by NFC or BLE

The customer C1 brings his customer terminal T1 close to the terminal T2 to then acquire (step 109) the fingerprint EP1. The terminal T1 proceeds to reading the
10 fingerprint by NFC link. In the case of NFC, the acquiring of the fingerprint triggers the opening of a payment application on the customer terminal T1 which requests an authentication of the customer C1. This authentication is implemented by the terminal T1 of the customer, for example by a recognition of a human fingerprint or a facial recognition or else by entry of a code. The acquiring of the transaction fingerprint
15 triggers a request for validation of the transaction by the customer C1 which takes the form of an authentication of the customer C1 (step 110). The receipt by NFC of the fingerprint EP1 if the application is not already open triggers the opening of the application.

Thus:

20 - in the context of NFC contactless payment: the customer must bring his terminal close to an NFC chip (which can be located on the counter of the merchant or on a table or on a wall). Thus, the customer is brought directly to the interface used to validate the transaction; he will automatically be brought to this interface when the telephone detects an NFC chip;

25 - in the context of BLE contactless payment: the terminal of the customer will detect the transaction via the terminals of the merchant which send BLE (radio frequency) waves. The receipt of these waves triggers the sending of a notification in the application and by clicking on the notification the application will open so that the customer can be brought to the interface making it possible to validate the transaction.

Payment by entering a transaction code

30 By way of the application and prior authentication of the customer C1, the customer enters the 6-figure code associated with the fingerprint presented by the merchant on his terminal T1. The amount requested by the merchant is then displayed and the customer C1 has the option to validate or cancel the transaction.

Once the customer C1 has been authenticated, this latter validates the transaction (step 111).

At this stage, the customer has proceeded to making the payment. The transaction is immediate and has lasted two seconds at the most. This streamlines payments and facilitates the checkout process.

Note that the number of steps to validate the transaction is three at the most (including the opening of the application) which improves the customer experience and simplifies the handling of the payment but also makes payment faster. Time is clearly saved when finalizing a sale.

The following steps are then transparent for the merchant and the customer since they are exchanges between the servers involved in the payment method. Note that at this stage no communication with a bank is required and that in particular no bank flow with the aim of crediting or debiting a bank account is used.

The validated transaction (step 111) triggers the generation (step 112) by the terminal T1 of the customer of a sale message M2 followed by its sending (step 113) to the payment server SP. The sale message M2 particularly includes an item of information relating to the amount of the transaction, an item of information relating to an identity of the customer and an item of information relating to an identity of a merchant. Such a sale message M2 will allow the payment server SP to process the transaction by clearly identifying all the parties involved in the transaction

The received sale message M2 (step 114) is then decoded (step 115) by the payment server SP to extract the items of information relating to the transaction. Advantageously, the payment server SP then makes a comparison (step 116) of the amount of the transaction with a payment capacity set for his customer account 10. Such a capacity is defined on creation of the customer account 10 and varies according to the items of information communicated by the customer, and according to the financial data collected. The payment capacity may be between 0 and 200 euros as default, and above after a solvency assessment of the customer. This assessment can be carried out, for example, by the sending of the last three bank statements of the customer or via a connection with his bank, allowing the payment server to recover the banking data of the past three months.

Whatever the scenario, the external account of the customer must be confirmed for the amount of his payment ability to change from €50 to €200 (this is

particularly valuable in the context of an onboarding done without any DSP2 connection).

If the amount of the transaction is greater than the payment capacity of the customer, the transaction is abandoned, and the payment server SP sends a message to the merchant terminal T2 as well as to the customer terminal T1. The customer C1 and the merchant C2 are thus notified simultaneously of the refusal of the transaction (step 117, step 118).

If the amount of the transaction is less than or equal to the payment capacity of the customer C1 then the payment server SP sends (step 121) the central server SC a transfer message M3 which allows the central server SC to execute the following operations (step 122): crediting the operating account of the merchant 22 with the amount of the transaction minus a commission which is transferred from a central operating account 30 also stored in the central server SC, and debiting the operating account of the customer 12 with the amount of the transaction.

Once the transfer has been made to the operating account of the merchant 22, the transaction is finished and the merchant C2 is notified (step 123) by the payment server SP.

Between the validation of the transaction by the customer 11 and the notification of the merchant 22 a time period of 2 seconds at the most has elapsed. This also improves the customer experience and simplifies the handling of the payment but also speeds up the payment. Time is thus clearly saved when finalizing a sale.

After the transaction, the operating account of the customer is therefore debited with the amount of the transaction while that of the operating account of the merchant is positive by this amount minus the amount of the commission.

It will be understood that several transactions may be credited to or debited from the merchant and customer operating accounts.

Bank transfer session

The bank transfer session is initiated on a variable schedule or with each transaction. The session is for example initiated every day (at the end of the day), every month (at the end of the month), every week (at the end of the week), etc. The idea is that it does not interfere with the validation of the payment by the customer and does not slow down the transaction as such.

At the desired moment, the payment server SP sends a first debit order (step 124) to the central server SC of the central bank EC. This first order has the aim of covering the debit(s) of the customer operating account 12.

The central server SC then debits the total debits of the customer operating
 5 account according to the known standards in effect. The execution of this first debit order involves the central server SC sending the first order to the customer bank E1 and in particular to the server S1 of the customer bank. The server of the customer bank S1 therefore transfers (step 126) from the bank account of the customer 11 to the central operating account 30 the total debits of the customer operating account
 10 12. The payment server SP is then notified of the covering of the debits of the customer (step 127, step 128).

Meanwhile, the sums credited to the operating account 22 of the merchant at each transaction are then transferred to the merchant bank account 21 (step 125). This operation is sent by the payment server SP (step 129) to the central server SC
 15 of the central bank EC. This second order has the aim of crediting the merchant bank account 21 with the amount to the credit of its operating account 22.

The central server then SC executes (step 131) a transfer from the operating account of the merchant 22 of the amount to be credited, to the merchant bank account 21 (step 132).

20 The merchant is sure of receiving the funds of his sales since the clearing of the funds is dissociated from the payment of the merchants and is covered by the bank associated with the central server (SC).

Other aspects:

25 According to a first exemplary embodiment, an electronic payment method in accordance with this summary comprises the following steps, implemented by a payment server:

a) receiving a sale message from a customer terminal, the sale message comprising an item of information relating to an amount of a transaction and an item
 30 of information relating to an identity of a merchant;

b) comparing the amount of the transaction with a payment capacity contained in a customer account stored in the payment server and if the amount of the transaction is less than or equal to the payment capacity;

b) sending to a central server a message to transfer the amount of the transaction in such a way that the central server credits an operating account of the merchant with the amount of the transaction minus a commission, debits an operating account of the customer and credits a central operating account with the commission;

5 c) sending to the central server an order to debit the debit balance of the customer operating account from the customer bank account to the central operating account of the central bank;

d) sending an order to transfer the balance from the operating account of the merchant to the merchant bank account;

10 e) receiving from the central server a notification that the debit balance of the customer operating account has been debited.

The method according to the first example is advantageously completed by the following features, taken alone or in any of their technical possible combinations:

- prior to the step a):

15 a0) receiving a transaction message from a merchant terminal, the transaction message comprising an amount of a sale;

a1) generating a transaction fingerprint from the transaction message received, the fingerprint comprising the amount of the sale and an identity of the merchant known to the payment server;

20 a2) sending the generated fingerprint to the merchant terminal.

- the fingerprint is a QR code, a near-field communication tag, a 6-figure numerical code or a communication tag (NFC) or by Bluetooth Low Energy (BLE).

- the receiving of the sale message follows the validation of the transaction by the customer by way of the customer terminal following the reading by the customer terminal of the fingerprint and the authentication of the customer at the customer terminal.

- if the amount of the transaction is greater than a payment capacity contained in the customer account, sending to the merchant terminal a notification to abandon the transaction and sending to the customer terminal a notification of refusal of the transaction.

30 - the debit order is sent at each transaction or else periodically on a given schedule.

CLAIMS

1. An electronic payment method, comprising the following steps, implemented by a payment server (SP):

- 5 - receiving (104) a transaction message (M1) from a merchant terminal (T2), the transaction message (M1) comprising an amount of a sale to a customer (C1), the amount of the sale having been entered by means of a merchant terminal (T2);
- generating (105) a transaction fingerprint (EP1) from the received transaction message (M1), the fingerprint (EP1) comprising the amount of the sale and an identity
- 10 of the merchant (C2) known to the payment server (SP) in the form of a format which can be acquired by acquiring means of a customer terminal (T1);
- sending (107) the generated fingerprint (EP1) to the merchant terminal (T2), the merchant terminal (T2) being configured to present the fingerprint (EP1) to a customer terminal;
- 15 - receiving (114) a sale message (M2) from a customer terminal (T1), the sale message (M2) comprising an item of information relating to an amount of a transaction and an item of information relating to an identity of a merchant, the sale message (M2) having been generated by the customer terminal (T1) following the acquiring
- (109) of the transaction fingerprint (EP1) by the customer terminal (T1), the
- 20 authenticating (110) of the customer (C1) and the validating (111) of the transaction by the customer (C1) at the customer terminal (T1).

2. The method as claimed in claim 1, comprising the following steps, implemented by a payment server (SP):

- 25 - comparing (116) the amount of the transaction with a payment capacity contained in a customer account stored in the payment server (SP) and if the amount of the transaction is less than or equal to the payment capacity;
- sending (121) to a central server (SC) a message (M3) to transfer the amount of the transaction in such a way that the central server (SC) credits an operating
- 30 account of the merchant with the amount of the transaction minus a commission, debits an operating account of the customer and credits a central operating account with the commission;

- sending (124) to the central server (SC) an order to debit the debit balance of the customer operating account from the customer bank account (11) to the central operating account (30) of the central bank;

- sending an order to transfer the balance from the operating account of the merchant (22) to the merchant bank account (21);

- receiving (127) from the central server a notification that the debit balance of the customer operating account has been debited.

3. The method as claimed in one of claims 1 to 2, wherein the fingerprint (EP1) is a QR code, a near-field communication tag (NFC), a 6-figure numerical code, a Bluetooth Low Energy communication tag.

4. The method as claimed in one of claims 1 to 3, wherein if the amount of the transaction is greater than a payment capacity contained in the customer account, sending (117) to the merchant terminal (T2) a notification of abandonment of the transaction and sending (118) to the customer terminal (T1) a notification of refusal of the transaction.

5. The method as claimed in one of claims 2 to 4, wherein the debit order is sent with every transaction or else periodically on a given schedule, once a day or once a month at the end of the day or at the end of the month.

6. The method as claimed in one of the preceding claims, comprising the following steps implemented by a terminal customer (T1):

- acquiring (109) the fingerprint (EP1) sent by the payment server (SP) and presented to the customer by means of a merchant terminal;

- authenticating (110) a customer (C1);

- validating the transaction (111) of the customer (C1) by way of the customer terminal;

- generating the sale message (M2);

- sending (113) the sale message (M2) to the payment server (SP).

7. The method as claimed in the preceding claim, wherein the acquiring (109) of the fingerprint (EP1) triggers the opening of an application stored on the customer

terminal (T1), the application making it possible to authenticate the customer and validate the transaction.

8. The method as claimed in one of the preceding claims, the following steps
5 implemented by a merchant terminal (C2):

- generating (102) the transaction message comprising the amount of the sale
- sending (103) the transaction message (M1) to the payment server
- presenting (108) the fingerprint (EP1), received from the payment server, to the customer (C1).

10

9. A payment server (SP) comprising a processing unit configured to implement a method as claimed in one of claims 1 to 5.

10. A payment method implemented by a customer terminal comprising the steps of:

- 15
- acquiring (109) the fingerprint (EP1) sent by the payment server (SP);
 - authenticating (110) a customer (C1);
 - validating of the transaction (111) by the customer (C1);
 - generating the sale message (M2);
 - sending (113) the sale message (M2) to a payment server (SP) as claimed

20 in claim 9.

11. The payment method comprising the following steps implemented by a merchant terminal:

25

- entering (101) a sale by the merchant, the entry comprising the amount of the sale;

- generating (102) the transaction message comprising the amount of the sale
- sending (103) the transaction message (M1) to a payment server as claimed in claim 9;

30

- presenting (108) the fingerprint (EP1), received from the payment server as claimed in claim 9, to the customer (C1)

12. A computer program product comprising instructions, which when the program is executed by a computer, lead it to implement the steps of the method as claimed in one of claims 1 to 11.

- 5 13. An electronic payment method, comprising the following steps:
- entering (101) a sale by means of a merchant terminal;
 - generating (102), by the merchant terminal, the transaction message comprising the amount of the sale;
 - sending (103), by the merchant terminal, the transaction message (M1) to a
10 payment server;
 - receiving (104), by a payment server (SP), a transaction message (M1) from a merchant terminal (T2), the transaction message (M1) comprising an amount of a sale to a customer (C1);
 - generating (105), by a payment server (SP), a transaction fingerprint (EP1)
15 from the received transaction message (M1), the fingerprint (EP1) comprising the amount of the sale and an identity of the merchant (C2) known to the payment server (SP);
 - sending (107), by a payment server (SP), the generated fingerprint (EP1) to the merchant terminal (T2) configured to present the fingerprint (EP1) to a customer;
 - 20 - presenting (108), by means of the merchant terminal, the fingerprint (EP1) received from the payment server to the customer (C1);
 - receiving (114) a sale message (M2) from a customer terminal (T1), the sale message (M2) comprising an item of information relating to an amount of a transaction and an item of information relating to an identity of a merchant, the sale message
25 (M2) having been generated by the customer terminal (T1) following the acquiring (109) of the transaction fingerprint (EP1) by the customer terminal (T1), the authenticating (110) of the customer (C1) and the validating (111) of the transaction by the customer (C1) at the customer terminal (T1).