

MOBILE COMMERCE PAYMENT SYSTEM**5 FIELD OF THE INVENTION**

This invention relates to a mobile commerce system that includes a payment system whereby goods or services can be located and selected using communications between a mobile communications device and the webpage
10 server of a supplier and wherein payment is required to be made for the selected goods or services.

More particularly, the invention relates to a mobile commerce system in which the mobile communications devices each include a unique electronic
15 identification and processing circuit capable of encrypting data utilizing an encryption key. A typical unique electronic identification and processing circuit is that of the well-known SIM card that can be used in cellular telephones or other wireless communications devices for identification and encryption purposes.

20

BACKGROUND TO THE INVENTION

Applicant believes that there is considerable potential in the mobile commerce field in spite of the ever increasing activity reported. One factor
25 that restrains additional growth of this market sector appears to be the security of electronic payments made for goods and services purchased on-line. In particular, credit card or debit card information inputted into the mobile communications device, typically a cellular telephone, is typically transmitted in an un-encrypted form simply because encryption keys that
30 would need to be shared between the communications device and payment engine in order to encrypt and to decrypt the relevant data cannot be provided in practice.

P1825PC00MobilePayment 2009/05/12

CONFIRMATION COPY

This being so, a typical mobile commerce transaction developed on a mobile device is illustrated in Figure 1. In such an application multiple mobile devices, in this instance cellular telephones (A), are provided wherein communication is enabled via a wireless network (B) with selected webpage servers (C) of multiple suppliers, such as online stores or booking applications. In order to complete a transaction it is often required to perform a payment and these applications need to connect to payment systems to facilitate the actual payment by transmitting the payment details to a backend server to perform the actual payment.

10

A mobile application would normally transmit the relevant data that typically includes credit or debit card or other financial account data to the webpage server or its associated payment engine using a secure TCP/IP protocol (e.g. HTTPS).

15

However, in most cases this level of security is not really sufficient. Each of the e-commerce stores needs to develop code to integrate to a payment engine or a financial switch (D) to perform the payment that is ultimately only finalised when the relevant banking institution (E) has cleared the transaction typically in accumulated batches of transactions.

20

Such applications are typically complicated pieces of development, but it is obviously necessary to ensure the integrity of the application. Every application on the mobile device that needs to capture payment will require the same functionality to capture the payment details, securely transmit the data to a backend system and then to integrate and pass these details to a payment engine or financial switch to perform the transaction. This is a substantial duplication of code both on the mobile device and the backend server. Of course, it is to be remembered that mobile devices have a limited amount of electronic capacity for processing and storing data.

30

Furthermore, payment details from online stores ultimately go through a financial switch (e.g. Visa or Mastercard etc). These transactions enter the switch in the country of the online store and not the country of the user making the payment. As a result these transactions are normally not
5 conducted in real time and are processed batchwise.

A typical mobile commerce system would thus gather the payment information from the user and then submit this data to a backend server that then connects to a payments engine. This requires that the mobile
10 commerce provider has online connectivity to the payment engine and has implemented the often tricky interface to the payment engine.

The general difficulties have led to the creation of various payment organisations often referred to as financial cyber mediaries, probably the
15 most well-known of which is the E-BAYTM owned organisation known as PAYPALTM, an e-mail based payment system in which payment is collected by the payment organisation and subsequently paid over to the recipient.

Various other efforts have been made to enhance the security of electronic
20 payments and in recent times a cellular telephone based payment system by the name of MOBILLCASHTM has been introduced that avoids the problem by adding payments to the actual cell phone account. However, this solution may well be unacceptable to cellular telephone service providers in that their responsibility of securing payments of their accounts is substantially
25 increased and the addition of service functions outside of the provision of a telephone service may not be acceptable.

Payment for goods or services purchased over the Internet therefore represents a serious technical problem that existing solutions have not been
30 able to overcome to a satisfactory extent and in a satisfactorily secure manner.

OBJECT OF THE INVENTION

It is an object of this invention to provide a mobile commerce payment system and components thereof that avoid at least some of the disadvantages of the existing payment systems that are outlined above.

SUMMARY OF THE INVENTION

In accordance with one aspect of this invention there is provided a mobile commerce system in which multiple wireless mobile communications devices (mobile devices) each has a unique electronic identification and processing circuit capable of encrypting data utilizing an encryption key and wherein each mobile device has a first application providing connectivity to commercial webpage servers for purposes that include the conduct of selected transactions involving a payment for goods or services and wherein the mobile device is independently enabled to conduct financial transactions in real time by communication with a financial institution, the mobile commerce system being characterized in that the mobile device further has a second application (herein termed mobile payment application) adapted to interact with the first application to receive data as to a payment required to conclude a transaction conducted by way of a commercial webpage server by way of the first application, to process such data to cause the creation of an instruction to the financial institution to make a payment to a payee designated by way of such data with the instruction being encrypted utilizing the unique electronic identification and processing circuit, wherein the encrypted instruction is transmitted to the financial institution, and a payment report is received from the financial institution.

Further features of the invention provide for the communications device to be a mobile telephone, in particular a cellular telephone; for the unique electronic identification and processing circuit to be that of a subscriber identity module (SIM) card that typically has at least one unique encryption

key embedded therein at factory level; for the webpage server to be associated with the World Wide Web; and for the mobile payment application to be adapted to transmit a successful payment report to the webpage server or associated payment engine to complete the transaction or, in the alternative, or in addition, for the system to be such that the financial institution transmits a successful payment report directly to the webpage server or associated payment engine.

The invention also provides a mobile communications device adapted to operate as a mobile device in a system as defined above.

The invention still further provides a method of performing a secure online commercial transaction using a mobile communications device that has a unique electronic identification and processing circuit capable of encrypting data utilizing an encryption key and wherein the mobile device has a first application providing connectivity to commercial webpage servers for purposes that include the conduct of selected transactions involving a payment for goods or services and wherein the mobile device is independently enabled to conduct financial transactions in real time by communication with a financial institution, the method comprising the steps of operating the wireless mobile communications device to connect to a commercial webpage server offering goods or services in exchange for payment therefor, selecting goods or services for which payment is required thereby initiating a transaction, and receiving information as to payment required, the method being characterized in that a second application (mobile payment application) resident on the communications device is adapted to interact with the first application to receive data containing information as to the payment required to conclude the transaction initiated by way of the commercial webpage server utilizing said first application, processing such data to cause the creation of an instruction to the financial institution to make a payment to a payee designated by way of such data wherein the instruction is encrypted utilizing the unique electronic identification and processing

circuit wherein the encrypted instruction is transmitted to the financial institution from the mobile communications device, and a payment report is received by the mobile communications device from the financial institution.

- 5 Further features of the method of the invention will be quite apparent from what is set out above.

In order that the invention may be more fully understood an expanded description thereof follows with reference to the accompanying drawings.

10

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:-

- 15 Figure 1 is a schematic illustration of a common prior art system for the payment of goods and services in a mobile commerce situation; and,

- Figure 2 is a similar illustration of a system according to the invention.
- 20

DETAILED DESCRIPTION WITH REFERENCE TO THE DRAWINGS

- In its most simple implementation, and as illustrated in Figure 2, a mobile commerce system according to the invention may include multiple wireless mobile communications devices, in this instance cellular telephones (1), each having a unique electronic identification and processing circuit capable of encrypting data utilizing an encryption key, in this instance in the form of a SIM card (2). As will be apparent to those skilled in the art the SIM card has at least one encryption key loaded onto it at factory level for the encryption of personal identification numbers (PINs) and, in this instance, payment details generated by the mobile payment application. The SIM card can thus be
- 25
- 30

used to sign the transaction using hardware algorithms in the SIM and security keys that reside thereon. Encryption of this nature renders a transaction significantly more secure than payments utilising existing expedients of online stores and booking applications according to the prior art.

Each mobile device has a browser in the form of a first software application providing connectivity by way of a wireless network (3) to commercial web page servers (4) for purposes that include the conduct of selected transactions involving a payment for goods or services in well known manner.

Each mobile device is independently enabled to conduct financial transactions in real time by communication with a financial institution, and whilst there are various possibilities, applicant prefers that their own cellular telephone-based banking system promoted under the trade mark FUNDAMO™ be employed.

As provided by this invention, each mobile device further has a second software application in the form of a mobile payment application adapted to interact with the first application to receive data as to a payment required by a commercial webpage server (4) for completion of a transaction implemented by way of the first application. Such interaction may take place by way of a plugin written for the browser that connects to the mobile device in any suitable or appropriate manner. The mobile payment application is adapted to process such data to create an instruction to the financial institution to make a payment to a payee designated by the webpage server and to encrypt the instruction utilizing the encryption key present in the SIM card so that an encrypted instruction is transmitted to a co-operant backend server (5) that operates in concert with a financial institution (6). This is done by using the 3DES algorithm and a key that was earlier provisioned onto the SIM by the mobile operator.

The mobile payment application is thus a software application that resides on the mobile device alongside other applications. It has an open application programming interface (API) that takes payment details and prompts the user to enter a personal identification number (PIN). The details can be sent to the application either from another application on the phone or via another connection method from an application that does not reside on the phone. Examples of this are from a retail till, point-of-sales device or from another mobile device. Where the application submitting the details does not reside on the mobile device the payment details could be sent using a number of different wireless communication methods such as SMS, Wi-Fi and Bluetooth.

The payment details would normally include the identifier of the application sending the request, payment amount and payment reference. The mobile payment application would then display to the user the payment details and ask the user to verify the payment by entering a PIN. This PIN may then be used to sign the payment using ISO PIN encryption algorithms and a secure key that resides on the SIM card. The payment details are then sent from the mobile payment application to the cooperant backend server.

The payment application associated with the backend server is adapted to send a payment report, either successful or unsuccessful, to the relevant mobile device and the mobile payment application on the mobile device, if the payment is successful, is adapted to transmit a payment report to the webpage server in order to conclude the transaction.

As an alternative, or in addition, the backend server could be adapted to transmit a successful payment report directly to the webpage server in order to enhance the confidence in the report.

It will be understood that by having a single mobile payment application that performs the payment portion of the transaction, for example, an on-line store

or booking application, the latter applications are not required to connect to a payment engine or financial switch. Any duplication of code is thus also eliminated.

- 5 Still further, the size of the online store or booking application is reduced by removing the payment portion from the application. A single payment application of this nature that all the online stores and booking systems can use will greatly reduce the space restrictions on the mobile device.
- 10 It is further to be noted that a system according to the invention will communicate with a backend application that resides in the user's country and there are significant advantages to this, particularly in terms of checking user balances and user PIN's. Also, transactions conducted using a system of this invention can be carried out in real time thereby obviating any
- 15 difficulties associated with subsequent clearing in batches of accumulated transactions.

It will be understood that numerous variations may be made to the system described above without departing from the scope hereof.

20

25

30

CLAIMS:

1. A mobile commerce system in which multiple wireless mobile communications devices (mobile devices) (1) each has a unique electronic identification and processing circuit (2) capable of encrypting data utilizing an encryption key and wherein each mobile device has a first application providing connectivity to commercial webpage servers (4) for purposes that include the conduct of selected transactions involving a payment for goods or services and wherein the mobile device is independently enabled to conduct financial transactions in real time by communication with a financial institution, the mobile commerce system being characterized in that the mobile device further has a second application (herein termed mobile payment application) adapted to interact with the first application to receive data as to a payment required to conclude a transaction conducted by way of a commercial webpage server by way of the first application, to process such data to cause the creation of an instruction to the financial institution to make a payment to a payee designated by way of such data with the instruction being encrypted utilizing the unique electronic identification and processing circuit, wherein the encrypted instruction is transmitted to the financial institution, and a payment report is received from the financial institution.
2. A mobile commerce system as claimed in claim 1 in which the communications device is a mobile telephone.
3. A mobile commerce system as claimed in either one of claims 1 or 2 in which the unique electronic identification and processing circuit is that of a subscriber identity module (SIM) card (2) that has at least one unique encryption key embedded therein.

4. A mobile commerce system as claimed in any one of the preceding claims in which the webpage server is associated with the World Wide Web.
- 5 5. A mobile commerce system as claimed in any one of the preceding claims in which the mobile payment application is adapted to transmit a successful payment report to the webpage server or associated payment engine to complete the transaction.
- 10 6. A mobile commerce system as claimed in any one of the preceding claims in which the system is such that the financial institution transmits a successful payment report directly to the webpage server or associated payment engine.
- 15 7. A mobile communications device adapted to operate as a mobile communications device in a system as claimed in any one of the preceding claims.
- 20 8. A method of performing a secure online commercial transaction using a mobile communications device that has a unique electronic identification and processing circuit capable of encrypting data utilizing an encryption key and wherein the mobile device has a first application providing connectivity to commercial webpage servers for purposes that include the conduct of selected transactions involving a payment for goods or services and wherein the mobile communications device is independently enabled to conduct financial transactions in real time by communication with a financial institution, the method comprising the steps of operating the wireless mobile communications device to connect to a commercial webpage server that offers goods or services in exchange for payment therefor, selecting goods or services for which payment is required thereby initiating a transaction, and receiving information as to payment
- 25
- 30

required, the method being characterized in that a second application (mobile payment application) resident on the mobile communications device is adapted to interact with the first application to receive data containing information as to the payment required to conclude the transaction initiated by way of the commercial webpage server utilizing said first application, processing such data to cause the creation of an instruction to the financial institution to make a payment to a payee designated by way of such data wherein the instruction is encrypted utilizing the unique electronic identification and processing circuit wherein the encrypted instruction is transmitted to the financial institution from the mobile communications device, and a payment report is received by the mobile communications device from the financial institution.

9. A method as claimed in claim 8 in which encryption of the data on the mobile communications device is effected utilizing the unique electronic identification and processing circuit (2) capable of encrypting data utilizing an encryption key.

10. A method as claimed in claim 9 in which the unique electronic identification and processing circuit is that of a subscriber identity module (SIM) card (2) that has at least one unique encryption key embedded therein.

25

30