METHOD AND SYSTEM FOR SECURE ONLINE TRANSACTION USING INTEGRATED CIRCUIT CARD

A method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising, in the integrated circuit card, generating a dynamic encryption key for transaction data, and transmitting the dynamic encryption key to the communications device via near field communication; in the communications device, encrypting the transaction data using the dynamic encryption key; in the integrated circuit card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication; and transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server, wherein a tag is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data.
METHOD AND SYSTEM FOR SECURE ONLINE TRANSACTION USING INTEGRATED CIRCUIT CARD

FIELD OF THE INVENTION

The present invention relates to a method and a system for secure online transaction using an integrated circuit (IC) card, in particular but not exclusively, to a method and a system for performing transaction signing and encryption transmission by means of an IC card.

BACKGROUND TO THE INVENTION

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention. However, it should be appreciated that the discussion is not an acknowledgment or admission that any of the material referred to was published, known or part of the common general knowledge in any jurisdiction as at the priority date of the application.

With advancement in technology in the area of integrated circuit (IC) cards, financial cards that are issued by banks have progressed from financial cards in the form of magnetic stripe cards to IC cards. In comparison with magnetic stripe cards, the advantages of having financial cards in the form of an IC card include the card being copy-proof and tamper-proof, and the card having a built-it key which helps to achieve the encryption of data, etc. As such, financial IC cards advantageously resolve the many problems related to security of offline transactions. At the same time, the switch from financial magnetic stripe cards to financial IC cards do not require users such as service providers to add additional devices or change the way or process of how they would handle a payment to accommodate the switch in the type of card.

However, for online transactions at present, in order to ensure the security thereof, the transactions are performed via online banking and with a hardware device, such as a U key or a token. Mobile banking or mobile payment similarly relies on a hardware device, such as an audio key or mPOS, so as to ensure the security of transactions made online via a mobile device. Whilst it may be inconvenient for a user having to carry around a hardware device, a certain degree of security is compromised if such a device is not used
while mobile banking or mobile payment is performed by a user. As such, performing online transactions at present are either secure but inconvenient, or convenient but insecure.

Generally in most countries, there are certain requirements imposed on banks or financial institutions in relation to the issuance of financial cards so as to ensure that these cards issued meet a certain level of security, for example, the EMVCo global standard for credit and debit payment cards; and the People's Bank of China (PBOC) standard for financial cards issued in China. Such a financial IC card is able to securely store a cardholder's key inside the card, and a built-in CPU in the card can realize multiple symmetric and asymmetric encryption and decryption algorithms which typically complies with both international and national standards. Data may be encrypted in the card and decrypted by background or back-end servers, and hence has the potential to perform a function similar to that of existing hardware security devices such as U key, token or any other hardware security devices or modules that are currently used in conjunction with performing online transactions. However, there is no such application at present.

Typically, to enable a secure offline transaction, a financial IC card provided by a user for a transaction is used in conjunction with a dedicated card reading device provided by a merchant or service provider which has been authenticated and is compatible with the financial IC card. In particular, signing of the transaction data is performed in the IC card itself and the card reading device encrypts the transaction data, where both the IC card and the card reading device each having its own built-in key. However, for online transactions, a user conducts such a transaction with a merchant or a bank via the Internet without a card reading device as it is difficult and impractical for the user to have on hand a dedicated card reading device to be used with the financial IC card so as to perform an online transaction that is secure. It is also inconvenient for a user having to carry around additional hardware devices such as an audio key to ensure the security of transactions made online.

Therefore, the present invention attempts to overcome at least in part some of the aforementioned disadvantages.
SUMMARY OF THE INVENTION

Throughout this document, unless otherwise indicated to the contrary, the terms "comprising", "consisting of, and the like, are to be construed as non-exhaustive, or in other words, as meaning "including, but not limited to".

The problem to be resolved by the present invention is to provide a method and a system for secure online transaction, which includes performing transaction signing, encryption of transaction data and encryption transmission by means of an integrated circuit (IC) card, such as a financial IC card, and using the IC card and a communications device, such as a general-purpose card reading device, to realize secure transaction signing and transaction encryption.

In accordance with a first aspect of the present invention, there is provided a method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:

(a) in the integrated circuit card, generating a dynamic encryption key for transaction data, and transmitting the dynamic encryption key to the communications device via near field communication;

(b) in the communications device, encrypting the transaction data using the dynamic encryption key;

(c) in the integrated circuit card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication; and

(d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,

wherein a tag is assigned to the dynamic encryption key in step (a) for identification during decryption of the encrypted transaction data.

In accordance with a second aspect of the present invention, there is provided a method
for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:

(a) in the integrated circuit card, signing transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication;

(b) in the integrated circuit card, generating a dynamic encryption key for the transaction data, and transmitting the dynamic encryption key to a communications device via near field communication;

(c) in the communications device, encrypting the transaction data using the dynamic encryption key; and

(d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,

wherein a tag is assigned to the dynamic encryption key in step (b) for identification during decryption of the encrypted transaction data.

Preferably, the step of generating a dynamic encryption key comprises:

(a) executing an application for the online transaction by the communications device;

(b) requesting the integrated circuit card to generate an application cryptogram (AC_i) and setting all fields of the transaction data to a prescribed value by the communications device; and

(c) generating the application cryptogram (AC_i), an integrated circuit card verification result (CVR_i) and an application transaction counter (ATC) by the integrated circuit card and transmitting the generated AC_i, CVR_i and ATC to the communications device, wherein the generated AC_i is the encryption key used for encrypting the transaction data.
Preferably, the step of signing of the transaction data comprises:

(a) processing the transaction data by dividing at least one field of the transaction data into \( n \) groups by the communications device if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the server to the remaining data length that is not divided into one or more groups, to make up the prescribed size to form a group;

(b) populating the one or more fields of the transaction data according to the grouping of the step (a) by the communications device and requesting the integrated circuit card to generate an application cryptogram \((AC_2)\); and

(c) repeating the step (b) until all the transaction data is communicated to the integrated circuit card, and the integrated circuit card generates the application cryptogram \( AC_2 \) to \( AC_{n+1} \), verification result \( CVR_2 \) to \( CVR_{n+1} \) and corresponding application transaction counters and transmits the same to the communications device to complete the signing of the transaction data.

Preferably, the step of transmitting the encrypted transaction data and signature comprising transmitting the encrypted transaction data, the transaction signature \((AC_2 \text{ to } AC_{n+1})\), the application transaction counter \((ATC)\) and all the verification results \((CVR_i \text{ to } CVR_{n+1})\) from the communications device to the server via the communications means.

Preferably, the step of decrypting the encrypted transaction data by the server comprising:

(a) deriving a key and an application interchange profile \((AIP)\) corresponding to the integrated circuit card from a database having information relating to the integrated circuit card holder;

(b) calculating the \( AC_i \) according to the received \( ATC \) and \( CVR_i \), the key and the \( AIP \) derived from the step (a) above, and the prescribed value of
(c) decrypting the encrypted transaction data by using the calculated $AC_1$ and a prescribed algorithm;

(d) dividing the at least one field of the transaction data into $n$ groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed data length that is not divided into one or more groups;

(e) adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and $CVR_n$, and comparing the calculated application cryptogram data with $AC_n$; and

(f) repeating the step (e) until all the calculated application cryptogram is compared with all $AC_{n+1}$,

wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

Preferably, the application cryptogram is an eight-byte application cryptogram.

Preferably, the one or more fields of the transaction data comprise(s) a transaction type, an authorized amount, an unpredictable number and an account number.

Preferably, the communications device is a mobile computing device.

Preferably, the mobile computing device is one of a mobile phone, tablet, laptop and personal digital assistant.

Preferably, the communications means is one of the Internet, an intranet, a dedicated network and any network suitable for connecting the communications device and the server.

Preferably, the prescribed size is four bytes.
Preferably, the integer multiple is an integer multiple of four.

Preferably, the tag is in the form an ordinal.

Preferably, the tag is in the form of a timestamp.

Preferably, the method for performing secure online transaction between an integrated circuit card, a communications device and a server is substantially as hereinbefore described with reference to any one of the accompanying drawings as appropriate.

In accordance with a third aspect of the present invention, there is provided a system for performing secure online transaction comprising:

(a) an integrated circuit card;

(b) a communications device; and

(c) a server,

wherein the integrated circuit card and the communications device communicate via near field communication; and the communications device and the server communicate via a communications means; and

wherein the integrated circuit card is operable to generate a dynamic encryption key for transaction data; the communications device is operable to encrypt the transaction data using the encryption key; the integrated circuit card is further operable to sign the transaction data to obtain transaction signature and send the transaction signature to the communications device; and transmit the encrypted transaction data and transaction signature from the communications device to the server via the communications means; the server further operates to decrypt the encrypted transaction data and authenticate the transaction signature in which a tag is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data.

Preferably, the system for performing secure online transaction is substantially as hereinbefore described with reference to any one of the accompanying drawings as appropriate.
In accordance with a fourth aspect of the present invention, there is provided a server for use in a system for performing secure online transaction wherein the server is operable to receive an encrypted transaction data and transaction signature from a communications device; and is further operable to decrypt the encrypted transaction data and authenticate the transaction signature; the server further comprises:

(a) means for deriving a key and an application interchange profile (AIP) corresponding to an integrated circuit card from a database having information relating to the integrated circuit card holder;

(b) means for calculating an application ciphertext (ACi) according to an application transaction counter (ATC) and an integrated circuit card verification result (CVR), the key and the AIP derived from the step (a) above, and a prescribed value of the transaction data;

(c) means for decrypting the encrypted transaction data by using the calculated ACi and a prescribed algorithm;

(d) means for dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;

(e) means for adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR, and comparing the calculated application cryptogram data with AC; and

(f) means for repeating the step (e) until all the calculated application cryptogram is compared with all ACn+i,

wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

Preferably, the server for use in a system for performing secure online transaction is
substantially as hereinbefore described with reference to any one of the accompanying
drawings as appropriate.

The technical effect of the present invention comprises the following:

In accordance with EMV specifications, which define a set requirements to ensure
worldwide interoperability and acceptance of secure payment transactions, by way of
rationally utilizing the transaction methods and flows stipulated by EMV, in an online
transaction, the signing for transaction data by an integrated circuit (IC) card, such as a
financial IC card, and encryption transmission for the transaction data by the card
cooperating with a communications device, such as a general-purpose card reading
device, are realized. Using an IC card, such as a financial IC card, held by a cardholder
ensures the transmission security of online transaction data, and realizes both
convenience (consistent with use habits of an offline transaction) and security (using this
hardware device of the IC card to ensure security). The EMV specifications is fully met,
the method of the present invention is efficient and effective, and the signing for
transaction data and encryption transmission for the transaction data performed by an IC
card are completed without increasing hardware cost, thereby reducing the cost and
challenges faced in promoting online transactions.

Other aspects and advantages of the invention will become apparent to those skilled in
the art from a review of the ensuing description, which proceeds with reference to the
following illustrative drawings of various embodiments of the invention.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 shows a system for performing secure online transaction in accordance with an
embodiment of the present invention. The system comprises an integrated circuit (IC)
card in the form of a financial IC card which is in line with the EMV specifications, a
communications device in the form of a mobile or cell phone with near field
communication function (NFC), and a server.

Fig. 2 shows the financial IC card and cell phone of the system of Fig. 1, in which a
default data element and financial IC card response data used when the cell phone sends
an instruction of "generate application cryptogram" to a financial IC card for the first
time.
Fig. 3 shows the financial IC card and cell phone of the system of Fig. 1, in which a first part of transaction data element and financial IC card response data used when the cell phone sends an instruction of "generate application cryptogram" to a financial IC card for the second time.

Fig. 4 shows the financial IC card and cell phone of the system of Fig. 1, in which a second part of transaction data element and financial IC card response data used when the cell phone sends an instruction of "generate application cryptogram" to a financial IC card for the third time.

Fig. 5 shows the process of encrypting plaintext of transaction data by the cell phone of the system of Fig. 1.

Fig. 6 shows the process of decrypting the encrypted transaction data by the server of the system of Fig. 1.

Fig. 7 shows a system for performing secure online transaction in accordance with another embodiment of the present invention.

**DETAILED DESCRIPTION OF THE INVENTION**

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

With reference to Figs. 1 to 7, there is described hereinafter a system and a method for performing secure online transaction using an integrated circuit (IC) card.

In accordance with an embodiment of an aspect of the present invention, there is a system for performing secure online transactions comprising an integrated circuit (IC) card, a communications device and a server (or background server). The IC card and the communications device communicate via near field communication, and the communications device and the server communicate via a communications means.
The IC card is operable to generate a dynamic encryption key for transaction data. The communications device is operable to encrypt the transaction data using the encryption key. The integrated circuit card is further operable to sign the transaction data to obtain transaction signature and send the transaction signature to the communications device.

The encrypted transaction data and transaction signature is transmitted from the communications device to the server via the communications means. The server further operates to decrypt the encrypted transaction data and authenticate the transaction signature in which a tag is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data (see Fig. 7).

The IC card is typically in the form of a financial IC card issued by a bank or financial institution, and the card meets the requirements of the EMV specifications. The server may be hosted by an IC card-issuing entity such as a bank or financial institution. The communications device is typically in the form of a general-purpose card reader or a mobile computing device which includes a mobile or cell phone, a tablet, a laptop, a personal digital assistant and the like. The communications means can be one of the Internet, an intranet, a dedicated network or any network that is suitable for connecting the communications device and the server.

In accordance with an embodiment of another aspect of the present invention, there is a method for performing secure online transaction by means of an integrated circuit (IC) card generally comprising the following steps:

A first step: generating a dynamic encryption key for transaction data, and using the key to encrypt the transaction data;

A second step: signing of the transaction data;

A third step: transmitting the encrypted transaction data and signature; and

A fourth step: decrypting the encrypted transaction data.

In particular, the method is for performing secure online transaction between an integrated circuit card, a communications device and a server and the method comprises the following steps:

Step (a): In the IC card, generating a dynamic encryption key for transaction data, and
transmitting the dynamic encryption key from the IC card to the communications device via near field communication;

Step (b): In the communications device, encrypting the transaction data using the dynamic encryption key;

Step (c): In the IC card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication; and

Step (d): Transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server, wherein a tag is assigned to the dynamic encryption key in the step (a) for identification during decryption of the encrypted transaction data.

In the step of generating a dynamic encryption key, the method comprises the following steps:

Step (a): Executing an application for the online transaction by the communications device;

Step (b): Requesting the IC card to generate an application cryptogram (ACi) and setting all fields of the transaction data to a prescribed value by the communications device; and

Step (c): Generating the application cryptogram (ACi), an integrated circuit card verification result (CVRi) and an application transaction counter (ATC) by the integrated circuit card and transmitting the generated ACi, CVRi and ATC to the communications device, wherein the generated ACi is the encryption key used for encrypting the transaction data.

In the step of signing of the transaction data, the method comprises the following steps:

Step (a): Processing the transaction data by dividing at least one field of the transaction data into n groups by the communications device if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the server to the
remaining data length that is not divided into one or more groups, to make up the prescribed size to form a group;

Step (b): Populating the one or more fields of the transaction data according to the grouping of the step (a) by the communications device and requesting the integrated circuit card to generate an application cryptogram \((AC_2)\); and

Step (c): Repeating the step (b) until all the transaction data is communicated to the integrated circuit card, and the integrated circuit card generates the application cryptogram \(AC_2\) to \(AC_{n_i}\), verification result \(CVR_2\) to \(CVR_{n+i}\) and corresponding application transaction counters and transmits the same to the communications device to complete the signing of the transaction data.

In the step of transmitting the encrypted transaction data and signature, the method comprises transmitting the encrypted transaction data, the transaction signature \((AC_2\) to \(AC_{n_i}\)), the application transaction counter \((ATC)\) and all the verification results \((CVR_i\) to \(CVR_{n+i}\)) from the communications device to the server via the communications means.

In the step of decrypting the encrypted transaction data by the server, the method comprises the following steps:

Step (a): Deriving a key and an application interchange profile \((AIP)\) corresponding to the integrated circuit card from a database having information relating to the integrated circuit card holder;

Step (b): Calculating the \(AC_i\) according to the received \(ATC\) and \(CVR_1\), the key and the \(AIP\) derived from the step (a) above, and the prescribed value of the transaction data;

Step (c): Decrypting the encrypted transaction data by using the calculated \(AC_i\) and a prescribed algorithm;

Step (d): Dividing the at least one field of the transaction data into \(n\) groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;
Step (e): Adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and $CVR_n$, and comparing the calculated application cryptogram data with $AC_n$; and

Step (f): Repeating the step (e) until all the calculated application cryptogram is compared with all $AC_{n+1}$, wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

Following from the above, the application cryptogram is typically in the form of an eight-byte application cryptogram.

The one or more fields of the transaction data described above comprise(s) one or more a transaction type, an authorized amount, an unpredictable number and an account number.

The IC card is typically in the form of a financial IC card issued by a bank or financial institution, and the card meets the requirements of the EMV specifications. The server may be hosted by an IC card-issuing entity such as a bank or financial institution. The communications device is typically in the form of a general-purpose card reader or a mobile computing device which includes a mobile or cell phone, a tablet, a laptop, a personal digital assistant and the like. The communications means can be one of the Internet, an intranet, a dedicated network or any network that is suitable for connecting the communications device and the server.

The prescribed size of the data length described is four bytes. The integer multiple of the data length is an integer multiple of four.

The tag that is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data is unique and can be in the form of an ordinal, a timestamp of the like.

In accordance with another embodiment, the step of signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication takes place before the steps of generating a dynamic encryption key for transaction data in the IC card, and transmitting the dynamic encryption key from the IC card to the communications device via near field communication, and encrypting the transaction data using the dynamic encryption key in
the communications device. In other words, the method for performing secure online transaction by means of an integrated circuit (IC) card generally comprises the following steps:

A first step: signing of the transaction data;

A second step: generating a dynamic encryption key for transaction data, and using the key to encrypt the transaction data;

A third step: transmitting the encrypted transaction data and signature; and

A fourth step: decrypting the encrypted transaction data.

In particular, the method is for performing secure online transaction between an integrated circuit card, a communications device and a server and the method comprises the following steps:

Step (a): In the IC card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication;

Step (b): In the IC card, generating a dynamic encryption key for transaction data, and transmitting the dynamic encryption key from the IC card to the communications device via near field communication;

Step (c): In the communications device, encrypting the transaction data using the dynamic encryption key; and

Step (d): Transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server, wherein a tag is assigned to the dynamic encryption key in the step (b) for identification during decryption of the encrypted transaction data.

In accordance with an embodiment of another aspect of the present invention, there is a server for use in a system for performing secure online transaction wherein the server is operable to receive an encrypted transaction data and transaction signature from a
communications device, and is further operable to decrypt the encrypted transaction data and authenticate the transaction signature. The server further comprises the following features:

(a) means for deriving a key and an application interchange profile (AIP) corresponding to an integrated circuit card from a database having information relating to the integrated circuit card holder;

(b) means for calculating an application ciphertext (AC) according to an application transaction counter (ATC) and an integrated circuit card verification result (CVR), the key and the AIP derived from the step (a) above, and a prescribed value of the transaction data;

(c) means for decrypting the encrypted transaction data by using the calculated AC and a prescribed algorithm;

(d) means for dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;

(e) means for adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR, and comparing the calculated application cryptogram data with AC; and

(f) means for repeating the step (e) until all the calculated application cryptogram is compared with all AC,

wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

The server may be hosted by an IC card-issuing entity such as a bank or financial institution.
The implementing process of the present invention will now be described as follows:

When performing transaction signing, a communications device such as a general-purpose card reading device or a mobile computing device which includes a mobile or cell phone, a tablet, a laptop, a personal digital assistant and the like, sends transaction data (the one or more fields of the transaction data includes a "transaction type", an "authorized amount" and an "unpredictable number", etc.) to a financial IC card, and requests a "generate application cryptogram" operation in accordance with the EMV specifications, so as to realize signing of the transaction data by an IC card, such as a financial IC card issued by a bank or financial institution, and the card meets the requirements of the EMV specifications, by obtaining a transaction ciphertext or an application cryptogram (AC).

The operation relating to "generate application cryptogram" can be in the form of three types: (i) approving transaction or transaction certificate (TC); (ii) requesting online authorisation or authorisation request cryptogram (ARQC); and (iii) request application authentication or application authentication cryptogram (AAC). Any one of the above-mentioned types can be used. However, the IC card will perform risk management according to relevant parameters when receiving a ciphertext request, and the IC card may change a request for approving transaction to requesting online authorisation or application authentication, and may also change requesting online authorisation to the application authentication; and only when receiving the application authentication request, the IC card will return the cryptogram for application authentication. Therefore, during implementation, applying for "application authentication ciphertext" or "application authentication cryptogram" (AAC) enables the logic to be simpler without having to influence the normal offline transaction of the IC card.

In an online transaction, except for the field "authorized amount", there is also typically a need for the transaction data to comprise other information, such as "transferred in account number". Whilst an instruction of requesting "transaction ciphertext" or "application cryptogram" does not contain fields, such as "transferred in account number", an "unpredictable number" field with four bytes can be set arbitrarily. Transaction fields of "transferred in account number", etc. which are not contained in an instruction of applying for "transaction ciphertext" or "application cryptogram" are
segmented into groups with every four bytes being one group, the above-mentioned data comprising the transaction fields, with four bytes being one group, of "transferred in account number", etc. are successively placed into an "unpredictable number" field of the instruction by requesting a "transaction ciphertext" or "application cryptogram" operation for an IC card several times, and all the data are successively sent into the IC card, thereby realizing signing of the entire transaction data by the IC card.

Plaintext of the transaction data will be transmitted via a communications means such as a network after being encrypted, and the solution adopted in the present invention as to how to negotiate an encryption key with a server is described as follows:

When transaction encryption is performed, a communications device such as a general-purpose card reading device or a mobile computing device which includes a mobile or cell phone, a tablet, a laptop, a personal digital assistant and the like, uses fields of a "transaction type", an "authorized amount" and an "unpredictable number", etc. with a group of default data elements (for example, all is "zero") to request a "transaction ciphertext" or an "application cryptogram" operation for an IC card, such as a financial IC card issued by a bank or financial institution, and the card meets the requirements of the EMV specifications, uses the transaction ciphertext or application cryptogram (AC) returned by the IC card as an encryption key, and then encrypts plaintext of the transaction data on the communications device; and a server can restore this encryption key according to a transaction counter or application transaction counter (ATC) and an integrated circuit card verification result (CVR) of the IC card, a key and an application interchange profile (AIP) of the IC card, and a default value of the transaction data. In this way, the problem of encryption of transmission of transaction data is resolved. Since a communications device such as a general-purpose card reading device (like a cell phone with a near field communication (NFC) function) does not have the security module on a dedicated card reading machine tool, performing encryption on such a device is not secure enough. However, the present invention uses an IC card which generates a one-time AC as an encryption key, and the encryption key is different every time, i.e. "one key one time", and therefore, the security thereof is also guaranteed.

During implementation under certain circumstances, the communications device and the server are faced with the problems in which the encryption and decryption keys change
dynamically and the length of the transaction data is uncertain, etc. when performing
transaction encryption and decryption operations. In this regard, the preferable method
during implementation is first determining a dynamic key of such a transaction when
transaction signing and data encryption transmission are performed by means of an IC
card, followed by signing up transaction data, then using the dynamic key of this
transaction by the communications device to encrypt the transaction data, and finally
sending the encrypted transaction data together with the transaction signature, etc. by the
communications device to a server, and decryption is then performed by the server. A
"transaction ciphertext" or an "application cryptogram" operation is applied, and a
"refuse transaction" type is selected.

With reference to the figures, the following particular embodiments of the present
invention are described based on the preferred method described above:

In the process of an entire online transaction, a communications device will apply several
times of "refuse transaction" ciphertext or cryptogram for an IC card. The entire
transaction process is described as follows by using a transfer transaction in which a cell
phone is used as a communications device to perform non-contact or contactless
communication with a financial IC card through a cell phone NFC signal:

1. Signing and Encryption of Transaction Data by a Cell Phone:

In a first step, a cell phone executes a command of "application selection" based on the
EMV specifications and selecting a debit or credit application in a financial IC card.

In a second step, the cell phone executes commands of "application initialization" and
reading application data based on the EMV specifications.

In a third step, as shown in Fig. 2, the cell phone uses a default data element to request
"refusing transaction ciphertext" or "application authentication cryptogram" (AAC) for
the financial IC card. (AC is a collective term of ciphertext or cryptogram, comprising
approving transaction ciphertext or transaction certificate (TC), requesting online
authorization ciphertext or authorisation request cryptogram (ARQC) and refusing
transaction ciphertext or application authentication cryptogram (AAC)). The financial IC
card response data comprises ATC₁|AAC₁|CVR₁.
In a fourth step, the cell phone converts a 19-bit payee account number or receivables account number of this transaction into eight-byte hexadecimal data.

In a fifth step, the steps one and two described above are repeated, and the financial IC card is allowed to consider restarting a transaction.

In a sixth step, as shown in Fig. 3, the cell phone sends the transfer amount, transaction type and first four bytes of the payee account number or receivables account number into the financial IC card to apply for a second "offline transaction refuse" operation. The financial IC card response data comprises $ATC_2|AAC_2|CVR_2$.

In a seventh step, the steps one and two described above are repeated, and the financial IC card is allowed to consider restarting a transaction.

In an eighth step, as shown in Fig. 4, the cell phone sends the transfer amount, transaction type and last four bytes of the payee account number or receivables account number into the financial IC card to apply for a third "offline transaction refuse" operation. The financial IC card response data comprises $ATC_3|AAC_3|CVR_3$.

In a ninth step, as shown in Fig. 5, the cell phone uses the $AAC_i$ as an encryption key to encrypt sensitive transaction information in relation to a transferred in/transferred out account number, and transfer amount and type, etc. of this transaction, so as to obtain an encrypted transaction data.

In a tenth step, the cell phone sends the $ATC_i|CVR_i|encrypted
data|AAC_2|CVR_2|AAC_3|CVR_3$ to a server (or background server) via a communications means such as an open network. The communications means can be one of the Internet, an intranet, a dedicated network or any network that is suitable for connecting the communications device and the server.

2. Decrypting the Transaction Data by the Server for Background Server):

In a first step, the server derives a key and an application interchange profile (AIP) corresponding to the financial IC card from a database according to cardholder information.

In a second step, the server calculates $AAC_i$ according to the $ATC_i|CVR_i|AIP$ and
financial IC card key as well as a transaction data default value.

In a third step, as shown in Fig. 6, the AACi is used to decrypt the transaction information in relation to the account number, amount and type, etc. of this transaction.

In a fourth step, one is added to the ATCi, and application ciphertext or application cryptogram data is calculated according to the first four bytes of the account number, amount, transaction type, and data of CVR₂, etc. and the application ciphertext or application cryptogram data is compared with the AAC₂. The values compared must be identical in order that the authenticity is verified and the integrity of the online transaction is preserved.

In a fifth step, another one is added to the ATCi, and application ciphertext or application cryptogram data is calculated according to the last four bytes of the account number, amount, transaction type, and data of CVR₃, etc. and the application ciphertext or application cryptogram data is compared with the AAC₃. The values compared must be identical in order that the authenticity is verified and the integrity of the online transaction is preserved.

In a sixth step, if the AAC₂ and the AAC₃ are compared successfully (in other words, the values compared are identical), it shows that the signing for the transaction data by the financial IC card of the cardholder is genuine and believable, the authenticity is verified and the integrity of the online transaction is preserved.

The advantages of the present invention include the following:

1. Both the transaction signing and the generation of a dynamic encryption key are performed by the IC card, whilst the encryption of transaction data using the dynamic encryption key generated by the IC card is performed by a separate communications device, hence enabling or realising secure transaction signing and transaction encryption for an online transaction.

2. Each dynamic encryption key generated is assigned a tag that is unique, meaning to say that each dynamic encryption key generated is unique; hence the encrypted transaction data which is communicated to the server can only be decrypted if the assigned tag matches a corresponding tag which the server has on its system. This
provides for identification during decryption of the encrypted transaction data at the server and hence prevents the processing of online transactions that are being intercepted or hacked into by third parties at the server which facilitates the overall online transaction to be secure.

3. The communications device being in the form of a general-purpose card reader or a mobile computing device eliminates the need for a dedicated card reading device provided by a merchant or service provider which has been authenticated and is compatible with the IC card, hence providing the convenience when performing online transactions that are secure. It also eliminates the need for a user to have on hand a dedicated card reading device such as an audio key to be used with the IC card so as to perform an online transaction that is secured, adding to the convenience.

It is to be understood that the above embodiments have been provided only by way of exemplification of this invention, and that further modifications and improvements thereto, as would be apparent to persons skilled in the relevant art, are deemed to fall within the broad scope and ambit of the present invention described herein. It is further to be understood that features from one or more of the described embodiments may be combined to form further embodiments.
CLAIMS

1. A method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:
   (a) in the integrated circuit card, generating a dynamic encryption key for transaction data, and transmitting the dynamic encryption key to the communications device via near field communication;
   (b) in the communications device, encrypting the transaction data using the dynamic encryption key;
   (c) in the integrated circuit card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication; and
   (d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,
wherein a tag is assigned to the dynamic encryption key in step (a) for identification during decryption of the encrypted transaction data.

2. A method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:
   (a) in the integrated circuit card, signing transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication;
   (b) in the integrated circuit card, generating a dynamic encryption key for the transaction data, and transmitting the dynamic encryption key to a communications device via near field communication;
   (c) in the communications device, encrypting the transaction data using the dynamic encryption key; and
   (d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,
wherein a tag is assigned to the dynamic encryption key in step (b) for identification
during decryption of the encrypted transaction data.

3. The method according to claim 1 or 2, wherein the step of generating a dynamic encryption key comprises:
   (a) executing an application for the online transaction by the communications device;
   (b) requesting the integrated circuit card to generate an application cryptogram \((AC_1)\) and setting all fields of the transaction data to a prescribed value by the communications device; and
   (c) generating the application cryptogram \((AC_i)\), an integrated circuit card verification result \((CVR_i)\) and an application transaction counter \((ATC)\) by the integrated circuit card and transmitting the generated \(AC_1\), CVR\(_i\) and ATC to the communications device, wherein the generated \(AC_i\) is the encryption key used for encrypting the transaction data.

4. The method according to claim 3, wherein the step of signing of the transaction data comprises:
   (a) processing the transaction data by dividing at least one field of the transaction data into \(n\) groups by the communications device if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the server to the remaining data length that is not divided into one or more groups, to make up the prescribed size to form a group;
   (b) populating the one or more fields of the transaction data according to the grouping of the step (a) by the communications device and requesting the integrated circuit card to generate an application cryptogram \((AC_2)\); and
   (c) repeating the step (b) until all the transaction data is communicated to the integrated circuit card, and the integrated circuit card generates the application cryptogram \(AC_2\) to \(AC_{n+1}\), verification result \(CVR_2\) to \(CVR_{n+1}\) and corresponding application transaction counters and transmits the same to the communications device to complete the signing of the transaction data.
5. The method according to claim 4, wherein the step of transmitting the encrypted transaction data and signature comprising transmitting the encrypted transaction data, the transaction signature (AC_2 to AC_{n+1}), the application transaction counter (ATC) and all the verification results (CVR_i to CVR_{n+1}) from the communications device to the server via the communications means.

6. The method according to claim 5, wherein the step of decrypting the encrypted transaction data by the server comprising:
   (a) deriving a key and an application interchange profile (AIP) corresponding to the integrated circuit card from a database having information relating to the integrated circuit card holder;
   (b) calculating the AC_i according to the received ATC and CVR_i, the key and the AIP derived from the step (a) above, and the prescribed value of the transaction data;
   (c) decrypting the encrypted transaction data by using the calculated AC_i and a prescribed algorithm;
   (d) dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;
   (e) adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR_{n}, and comparing the calculated application cryptogram data with AC_{n}; and
   (f) repeating the step (e) until all the calculated application cryptogram is compared with all AC_{n+i}, wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

7. The method according to any of claims 3 to 6, wherein the application cryptogram is an eight-byte application cryptogram.
8. The method according to any preceding claim, wherein the one or more fields of the transaction data comprises a transaction type, an authorized amount, an unpredictable number and an account number.

9. The method according to any preceding claim, wherein the communications device is a mobile computing device.

10. The method according to claim 8, wherein the mobile computing device is one of a mobile phone, tablet, laptop and personal digital assistant.

11. The method according to any preceding claim, wherein the communications means is one of the Internet, an intranet, a dedicated network and any network suitable for connecting the communications device and the server.

12. The method according to any preceding claim, wherein the prescribed size is four bytes.

13. The method according to any preceding claim, wherein the integer multiple is an integer multiple of four.

14. The method according to any preceding claim, wherein the tag is in the form an ordinal.

15. The method according to any of claims 1 to 13, wherein the tag is in the form of a timestamp.

16. A system for performing secure online transaction comprising:
   (a) an integrated circuit card;
   (b) a communications device; and
   (c) a server,

   wherein the integrated circuit card and the communications device communicate via near field communication; and the communications device and the server
communicate via a communications means; and
wherein the integrated circuit card is operable to generate a dynamic encryption key for transaction data; the communications device is operable to encrypt the transaction data using the encryption key; the integrated circuit card is further operable to sign the transaction data to obtain transaction signature and send the transaction signature to the communications device; and transmit the encrypted transaction data and transaction signature from the communications device to the server via the communications means; the server further operates to decrypt the encrypted transaction data and authenticate the transaction signature in which a tag is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data.

17. A server for use in a system for performing secure online transaction wherein the server is operable to receive an encrypted transaction data and transaction signature from a communications device; and is further operable to decrypt the encrypted transaction data and authenticate the transaction signature; the server further comprises:

(a) means for deriving a key and an application interchange profile (AIP) corresponding to an integrated circuit card from a database having information relating to the integrated circuit card holder;
(b) means for calculating an application ciphertext (ACi) according to an application transaction counter (ATC) and an integrated circuit card verification result (CVRi), the key and the AIP derived from the step (a) above, and a prescribed value of the transaction data;
(c) means for decrypting the encrypted transaction data by using the calculated $AC_1$ and a prescribed algorithm;
(d) means for dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;
(e) means for adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR<sub>n</sub>, and comparing the calculated application cryptogram data with AC<sub>n</sub>; and

(f) means for repeating the step (e) until all the calculated application cryptogram is compared with all AC<sub>n+i</sub>, wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

18. A method for performing secure online transaction between an integrated circuit card, a communications device and a server substantially as hereinbefore described with reference to any one of the accompanying drawings as appropriate.

19. A system for performing secure online transaction substantially as hereinbefore described with reference to any one of the accompanying drawings as appropriate.

20. A server for use in a system for performing secure online transaction substantially as hereinbefore described with reference to any one of the accompanying drawings as appropriate.
Figure 1

Default data element:
Authorized amount: 000000000000
Other amount: 000000000000
Terminal country code: 0156
Terminal verification result: 0000000000
Currency code of transaction: 0156
Transaction date: 000000
Transaction type: 00
Unpredictable number: 00000000

Figure 2

CID1: XX
ATC1: XXXX
AAC1: XXXXXXXXXXX
CVR1: XXXXXXX

Generate application ciphertext 1
Response 1
Transaction data element 1:
- Authorized amount: XXXXXXXXXXX
- Other amount: 000000000000
- Terminal country code: 0156
- Terminal verification result: 0000000000
- Currency code of transaction: 0156
- Transaction date: XXXXXX
- Transaction type: XX
- Unpredictable number: First four bytes of account number

Figure 3
Transaction data element 3:
Authorized amount: XXXXXXXXXXXX
Other amount: 000000000000
Terminal country code: 0156
Terminal verification result: 0000000000
Currency code of transaction: 0156
Transaction date: XXXXX
Transaction type: XX
Unpredictable number: Last four bytes of account number

Figure 4
Figure 5

Figure 6
Figure 7
A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/30 (2012.01)  G06Q 20/32 (2012.01)  G06Q 20/34 (2012.01)  G06Q 20/38 (2012.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPIAP, TXTE, INSPEC, Google Patent, Google Web, Google Scholar, ESPACENET, THE LENS with keywords: EMV, integrated circuit, transaction, data, point of sale, generate, derive, encryption, key, sign, signature, NFC, tag, timestamp, ordinal, transaction counter, verification result, account number, divide and similar terms; and classification symbols such as G06Q20/00, H04L9/00, H04W12/06, G06Q20/34, G06Q20/343, G06Q20/352, G06Q20/38, G06Q20/40, G06Q20/401, G06Q20/40975, H04L9/328 I, H04L9/3294, H04L9/3297, H04W12/06, G06Q20/322, G06Q20/327, G06Q20/382 in EPODOC only.

Applicant/Inventors name searches were conducted in ESPACENET, AUSPAT and internal databases provided by IP Australia.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Documents are listed in the continuation of Box C</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Further documents are listed in the continuation of Box C</th>
<th>See patent family annex</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>&quot;A&quot;</td>
<td>document defining the general state of the art which is not considered to be of particular relevance</td>
<td></td>
</tr>
<tr>
<td>&quot;E&quot;</td>
<td>earlier application or patent but published on or after the international filing date</td>
<td></td>
</tr>
<tr>
<td>&quot;L&quot;</td>
<td>document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td>
<td></td>
</tr>
<tr>
<td>&quot;O&quot;</td>
<td>document referring to an oral disclosure, use, exhibition or other means</td>
<td></td>
</tr>
<tr>
<td>&quot;P&quot;</td>
<td>document published prior to the international filing date but later than the priority date claimed</td>
<td></td>
</tr>
<tr>
<td>&quot;T&quot;</td>
<td>later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td>
<td></td>
</tr>
<tr>
<td>&quot;X&quot;</td>
<td>document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td>
<td></td>
</tr>
<tr>
<td>&quot;Y&quot;</td>
<td>document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td>
<td></td>
</tr>
<tr>
<td>&quot;&amp;&quot;</td>
<td>document member of the same patent family</td>
<td></td>
</tr>
</tbody>
</table>

Date of the actual completion of the international search
6 February 2017

Date of mailing of the international search report
06 February 2017

Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
Email address: pct@ipaaustralia.gov.au

Authorised officer
Mu-en Tien
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. 0262832598
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2015/0006407 A1 (EBAY INC.) 01 January 2015 See whole document particularly Abstract; FIG. 1-3, 7, 11; para. [0001], [0007]-[0008], [0019]-[0049], [0057].</td>
<td>1-2, 9, 11, 14-16</td>
</tr>
<tr>
<td>Y</td>
<td>US 2014/0324698 A1 (MOBEEWAVE, INC.) 30 October 2014 See whole document particularly Abstract; FIG. 1-3, 9a-11; para. [0033], [0037]-[0047], [0051]-[0052], [0056], [0063]-[0070], [0102]-[0104].</td>
<td>1-2, 9, 11, 14-16</td>
</tr>
<tr>
<td>A</td>
<td>US 2014/0236842 A1 (ONSUN OY) 21 August 2014 See whole document.</td>
<td>6, 17</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (fifth sheet) (July 2009)
**Continuation of Box II**
The claims do not comply with Rule 6.2(a) because they rely on references to the description and/or drawings.

**Continuation of Box III**
This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

This Authority has found that there are different inventions based on the following features that separate the claims into distinct groups:

- **Group I**: Claims 1-5, 16 and claims 6-15 (in part) are directed to a method for performing secure online transaction between an integrated circuit card, a communications device and a server or a system for performing secure online transaction. The features of the integrated circuit card generating a dynamic encryption key for transaction data; transmitting the generated dynamic encryption key to the communications device via next field communication; encrypting the transaction data using the generated dynamic encryption key, signing the transaction data to obtain transaction signature; transmitting the encrypted transaction data and the transaction signature to the server for authentication and assigning a tag to the generated dynamic encryption key for identification of the encryption key during decryption at the server are specific to this group of claims. In particular, the features in this group of claims are directed to signing the transaction data, generating dynamic encryption key, encrypting the transaction data by the dynamic encryption key, generating transaction data and assigning a tag to the dynamic encryption key.

- **Group II**: Claim 17 and claims 6-15 (in part) are directed to a method for performing secure online transaction between an integrated circuit card, a communications device or a server for use in a system for performing secure online transaction. The features of deriving a key and an application interchange profile (AIP) corresponding to an integrated circuit card from a database; calculating application ciphertext according to application transaction counter (ATC) and integrated circuit card verification results (CVR), the derived key, the derived AIP and the prescribed value of the transaction data; dividing the at least one field of the transaction data into several groups if the data length thereof is greater than a prescribed size are specific to this group of claims. In particular, the features in this group of claims are directed to performing secure online transaction by using the derived key, the derived AIP, the received ATC, the received CVR and the prescribed value of the transaction data to generate the application ciphertext/application cryptogram/transaction signature.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

When there is no special technical feature common to all the claimed inventions there is no unity of invention.

In the above groups of claims, the identified features may have the potential to make a contribution over the prior art but are not common to all the claimed inventions and therefore cannot provide the required technical relationship. Therefore there is no special technical feature common to all the claimed inventions and the requirements for unity of invention are consequently not satisfied a priori.
**Box No. II  Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. **I** Claims Nos.:
   - because they relate to subject matter not required to be searched by this Authority, namely:
     - the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. **X** Claims Nos. **18-20**
   - because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
     - *See Supplemental Box*

3. **I** Claims Nos:
   - because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

**Box No. III  Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

- *See Supplemental Box for Details*

1. **I** As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. **I** As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. **I** As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. **I** No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

- **I** The additional search fees were accompanied by the applicant’s protest and, where applicable, the payment of a protest fee.
- **I** The additional search fees were accompanied by the applicant’s protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- **I** No protest accompanied the payment of additional search fees.
This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication Number</td>
<td>Publication Date</td>
<td>Publication Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2013207817 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2013207817 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2016204947 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2860586 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 104054098 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2803022 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2015510168 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2016189198 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20140113722 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20170001745 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2013106723 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2013225577 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2860987 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2881429 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 104145285 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2820601 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2015513738 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20140137400 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RU 2014138935 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2016132861 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2013126996 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2761553 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FI 20116274 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FI 125071 B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FI 20155310 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2013045743 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2013288898 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 104603810 A</td>
</tr>
</tbody>
</table>

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

Form PCT/ISA/210 (Family Annex)(July 2009)
This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication Number</td>
<td>Publication Date</td>
</tr>
<tr>
<td></td>
<td>Publication Number</td>
</tr>
<tr>
<td>JP 201553 1108 A</td>
<td>29 Oct 2015</td>
</tr>
<tr>
<td>KR 201500365 12 A</td>
<td>07 Apr 2015</td>
</tr>
<tr>
<td>TW 20140937 1 A</td>
<td>01 Mar 2014</td>
</tr>
<tr>
<td>TW 153629 1 B</td>
<td>01 Jun 2016</td>
</tr>
<tr>
<td>WO 201401 157 1 A1</td>
<td>16 Jan 2014</td>
</tr>
</tbody>
</table>

End of Annex