

ENCRYPTION AND DECRYPTION OF DATA BETWEEN A COMMUNICATIONS DEVICE AND SMART CARD WITH NEAR FIELD COMMUNICATION FUNCTION

FIELD OF THE INVENTION

This invention relates to encryption and decryption of digital information based on Near Field Communication (NFC) technology, such as but is not limited to the encryption and decryption of mobile messages such as SMS and MMS, encryption and decryption of digital information in various internet environments for mobile devices such as mobile phones, encryption and decryption of computer data in various internet environments as well as the encryption and decryption technology of digital information for various digital devices with telecommunication functions (such as WIFI, Bluetooth, infrared sensor etc.) in various internet environments.

BACKGROUND ART

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

The encryption and decryption of digital information in an internet environment is extremely important - any device connected to the internet carrying out information transmission faces such issues. The SSL transmission is commonly adopted for information encryption and decryption where the security requirement is not high. The secret key of this encryption and decryption is stored locally on the communication or computing device and is prone to attack and security compromise. Where the security requirement is high or more customized, additional hardware encryption and decryption

methods are often adopted. Currently, some common hardware encryption and decryption methods include hardware encryption engine and hardware encryption terminal (such as USB Key), but these devices often require cable connection; or are expensive specialized devices and are non-portable; or they can only run on devices with general interface and device software such as computers (laptops) and may have compatibility issues between the hardware encryption terminal and the computer as well as poor portability. In a world where internet communication has become a critical part of social life, and where mobile payment, mobile business, mobile office, mobile social communication etc. all heavily demand data encryption and decryption, the core objective of this invention is to achieve portable, convenient and safe encryption and decryption of digital information, especially on the currently most prevalent device - mobile phones.

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”.

In accordance with a first aspect of the invention, there is a method for encrypting and decrypting data between a communications device and a smart card each configured with Near Field Communication (NFC) function comprising:-

reserving storage space on the communications device for storing the data to be encrypted or decrypted;

placing the smart card near or in contact with the communications device to achieve NFC communication;

verifying legitimacy of the communications device and /or the smart card;

sending data to be encrypted or decrypted from the communications device to the smart card in a prescribed format;

receiving data to be encrypted or decrypted by the smart card and submitting it to a specified algorithm together with a specified secret key to conduct the encryption or decryption, thereafter further sending the encrypted or decrypted data to the communications device in the prescribed format.

Preferably, the data may take the form of digital information.

Preferably, the legitimacy of the communications device and/or the smart card is achieved by verifying a binding relation between the communications device and the smart card.

Preferably, the binding relation is verified via a unique identifier preset in the communications device and the smart card.

Preferably, the unique identifier is a personal identification (PIN) code, a International Mobile Equipment Identity (IMEI) code, a International Mobile Subscriber Identity (IMSI) code, or a Media Access Control (MAC) address.

Preferably, markers are added to the head or tail of each batch of the data when NFC communication is interrupted.

Preferably, the prescribed format comprises a complete document manifested as several character fields of equal length or part thereof; the partial abstract of a complete document, numbers or diagrams in the document, image information of a video, text, drawings, graphs, photographs or combinations of one or more of the above.

Preferably, the communication device may be a mobile computing device

such as a mobile phone, tablet, laptop or personal digital assistant.

In accordance with a second aspect of the invention there is a communications device installed with software thereon, the software executable to perform the method according to the first aspect of the invention.

In accordance with a third aspect of the invention there is a smart card installed with software thereon, the software executable to perform the method according to the first aspect of the invention.

In accordance with a fourth aspect of the invention there is a system for encrypting and decrypting data between a communications device and a smart card each configured with Near Field Communication (NFC) function; where the communications device is operable to reserve storage space for storing the data to be encrypted or decrypted; NFC communication is enabled between the communications device and smart card when placed near or in contact with each other to verify the legitimacy of the communications device and/or the smart card; the communications device is further operable to send data to be encrypted or decrypted to the smart card in a prescribed format; and on receipt of the data, the smart card is operable to submit said data to a specified algorithm together with a specified secret key to conduct encryption or decryption, the smart card is further operable to send the encrypted or decrypted data to the communications device in the prescribed format.

Preferably the data may take the form of digital information.

Preferably the legitimacy of the communications device and/or the smart card is achieved by verifying a binding relation between the communications device and the smart card.

Preferably the binding relation is verified via a unique identifier preset in the

communications device and the smart card.

Preferably the unique identifier is a personal identification (PIN) code, a International Mobile Equipment Identity (IMEI) code, a International Mobile Subscriber Identity (IMSI) code, or a Media Access Control (MAC) address.

Preferably markers are added to the head or tail of each batch of the data when NFC communication is interrupted.

Preferably the prescribed format comprises a complete document manifested as several character fields of equal length or part thereof; the partial abstract of a complete document, numbers or diagrams in the document, image information of a video, text, drawings, graphs, photographs or combinations of one or more of the above.

Preferably, the communication device may be a mobile computing device such as a mobile phone, tablet, laptop or personal digital assistant.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood in the light of the following description, made with reference to the drawings, wherein:

Figure 1 is a flow diagram of an embodiment of the invention.

PREFERRED EMBODIMENT OF THE INVENTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawing. 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.

In accordance with a first embodiment of the invention, there is a method for encrypting and decrypting data between a communications device which has NFC capabilities and a smart card. The communications device may be a mobile computing device such as a mobile phone, tablet, laptop, personal digital assistant etc.. The smart card may be an IC card which has NFC capabilities and computing capability (CPU). The IC card chip provides symmetric or asymmetric algorithm; this algorithm can also be achieved by software in the chip storage space. With reference to Figure 1, the implementing process of this invention will now be described with reference to a mobile phone and IC card as follows:-

Mobile phone:

1. Set storage space in the phone for reserving the data to be encrypted or decrypted 110. The data to be encrypted or decrypted may be digital information such as short messaging system (SMS) messages, multi-media messages (MMS) or any digital information received or stored in the phone, including audio, video and images, text, drawings, graphs, photographs or combinations of one or more of the above.
2. Place the IC card near or in contact with the phone to enable NFC communication between the phone and IC card 120. A user could be prompted to do so according to prompts by the phone such as a message on the screen of the phone.
3. Verify legitimacy of the phone and/or IC card as the encryption and decryption devices 130. The legitimacy verification can be achieved by verifying the IC card PIN or the binding relation between the phone and IC card. The verification of IC card PIN means that a user presets a PIN code (personal identification code) in the IC card and inputs the corresponding PIN code in the phone before commencing encryption and decryption of the digital

information; when the IC card is placed near or in contact with the phone and communication between the phone and IC card is initiated (by the communication method between the NFC mobile phone and IC card), the PIN code of the phone is communicated to the IC card and compared with the PIN code preset in the IC card; if the two PIN codes are identical, the legitimacy of the phone and IC card is verified. The verification of the binding relation between the phone and the IC card can further involve the user presetting a unique identifier such as an International Mobile Equipment Identity (IMEI) of phone and/or an International Mobile Subscriber Identity (IMSI) of a phone card in the IC card and before commencing the encryption and decryption of the digital information); an application on the phone such as a mobile app then communicates the IMEI of the phone and/or the IMSI of the phone card to the IC card which is compared with the IMEI of the phone and/or IMSI of the phone card preset in the IC card; if the two sets of IMEIs and/or IMSIs are identical, the legitimacy of the phone and IC card is verified.

4. Send in batches to the IC card the digital information to be encrypted and decrypted 140 in the prescribed format. Meanwhile, receiving in batches the digital information to be encrypted and decrypted 170 from the IC card and store the information in the space set aside in the phone in the prescribed format. Markers can also be added by the mobile application to the head or tail of each batch of the digital information being transmitted to avoid restarting transmission of the digital information in case the NFC communication is interrupted by abnormal occurrences and ensure the remaining information transmission can resume later. This step is of great importance as communication anomalies are common in NFC communication.

5. The operation is completed when the phone sends and receives the end mark of digital information and the phone screen will prompt that the encryption and decryption process is finished. The IC card is then moved away from the phone.

IC card:

1. Place the IC card near or in contact with the phone to enable NFC communication between the phone and IC card 120. A user could be prompted to do so according to prompts by the phone such as a message on the screen of the phone.

2. Conduct the legitimacy verification 130 of the phone. The legitimacy verification 130 can be achieved by verifying the IC card PIN or the binding relation between the phone and IC card. The verification of IC card PIN means that the user presets a PIN code (personal identification code) in the IC card and inputs the corresponding PIN code in the phone before commencing the encryption and decryption of the digital information; when the IC card is placed near or in contact with the phone (by the communication method between the NFC mobile phone and IC card), the PIN code is communicated to the IC card and compared with the PIN code preset in the IC card; if the two PIN codes are identical, the legitimacy of the phone and IC card is verified. The verification of the binding relation between the phone and the IC card means that the user presets an IMEI of the phone and/or an IMSI of the phone card in the IC card before commencing the encryption and decryption of the digital information; the mobile App then communicates the IMEI of the phone and/or the IMSI of the phone card to the IC card which is compared with the IMEI of the phone and/or IMSI of the phone card preset in the IC card; if the two IMEIs and/or IMSIs are identical, the legitimacy of the phone and IC card is verified.

3. Receive in batches the digital information to be encrypted and decrypted by the IC card 150 from the phone and submit it to the specified algorithm together with specified secret key to conduct encryption or decryption operation; then sending the encrypted or decrypted digital information to the phone 160 in the prescribed format;

4. Stop sending the digital information when prompted by the phone such as when a completion prompt pops up on the phone screen.

In the above implementation illustration, the aforementioned “prescribed format” refers to the digital information encrypted and decrypted, which, depending on the various requirements of individual encryption and decryption content, can be the entire information of a complete document manifested as several character fields of equal length; the partial abstract of a complete document, such as: the beginning and/or the conclusion of the text, some numbers or diagrams in the document, and some image information of a video document, text, drawings, graphs, photographs or combinations of one or more of the above.

The beneficial effects of the invention are as follows:

1. The secret key and algorithm of encryption and decryption is stored in the IC card, which both ensures the security of the secret key storage and achieves the portability of information encryption and decryption.
2. The data interchange in the encryption and decryption between the mobile phone and the smart card is achieved through NFC communication without the need for drivers or any other support program or the risk of compatibility issues.
3. The mobile phone is now one of the primary device for data interchange due to its versatility; as such, the encryption and decryption of digital information based on mobile phone and smart card would be the most convenient method in solving the problem of hardware encryption and decryption of mobile data such as SMS and MMS employing the most prevalent digital encryption and decryption device.

It should be appreciated by the person skilled in the art that the above invention is not limited to the embodiment described. In particular, the following modifications and improvements may be made without departing from the scope of the present invention:

- The communications device may take the form of a desktop or laptop computer and the unique identifier is a Media Access Control (MAC) address of the said device.
- The digital information may take the form of may take the form of Short Messaging System (SMS) messages, Multimedia Messaging System (MMS) messages or other like messaging protocol.

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.

WE CLAIM

1. A method for encrypting and decrypting data between a communications device and a smart card each configured with Near Field Communication (NFC) function comprising:

reserving storage space on the communications device for storing the data to be encrypted or decrypted;

placing the smart card near or in contact with the communications device to enable NFC communication;

verifying legitimacy of the communications device and/or the smart card;

sending data to be encrypted or decrypted from the communications device to the smart card in a prescribed format;

receiving data to be encrypted or decrypted by the smart card and submitting said data to a specified algorithm together with a specified secret key to conduct encryption or decryption, thereafter further sending the encrypted or decrypted data to the communications device in the prescribed format.

2. The method according to claim 1 wherein the data may take the form of digital information.

3. The method according to claim 1 or 2 wherein the legitimacy of the communications device and/or the smart card is achieved by verifying a binding relation between the communications device and the smart card.

4. The method according to claim 3 wherein the binding relation is verified via a unique identifier preset in the communications device and the smart card.

5. The method according to claim 4 wherein the unique identifier is a personal identification (PIN) code, a International Mobile Equipment Identity (IMEI) code, a International Mobile Subscriber Identity (IMSI) code, or a Media Access Control (MAC) address.
6. The method according to any one of the preceding claims wherein markers are added to the head or tail of each batch of the data when NFC communication is interrupted.
7. The method according to any one of the preceding claims wherein the prescribed format comprises a complete document manifested as several character fields of equal length or part thereof; the partial abstract of a complete document, numbers or diagrams in the document, image information of a video, text, drawings, graphs, photographs or combinations of one or more of the above.
8. The method according to any one of the preceding claims wherein the communication device may be a mobile computing device such as a mobile phone, tablet, laptop or personal digital assistant.
9. A communications device installed with software thereon, the software executable to perform the method as claimed in any one of the preceding claims.
10. A smart card installed with software thereon, the software executable to perform the method as claimed in any one of claims 1 to 8.
11. A system for encrypting and decrypting data between a communications device and a smart card each configured with Near Field Communication (NFC) function;

where the communications device is operable to reserve storage space for storing the data to be encrypted or decrypted; NFC communication is enabled

between the communications device and smart card when placed near or in contact with each other to verify the legitimacy of the communications device and/or the smart card; the communications device is further operable to send data to be encrypted or decrypted to the smart card in a prescribed format; and on receipt of the data, the smart card is operable to submit said data to a specified algorithm together with a specified secret key to conduct encryption or decryption, the smart card is further operable to send the encrypted or decrypted data to the communications device in the prescribed format.

12. The system according to claim 11 wherein the data may take the form of digital information. .

13. The system according to claim 11 or 12 wherein the legitimacy of the communications device and/or the smart card is achieved by verifying a binding relation between the communications device and the smart card.

14. The system according to claim 13 wherein the binding relation is verified via a unique identifier preset in the communications device and the smart card.

15. The system according to claim 14 wherein the unique identifier is a personal identification (PIN) code, a International Mobile Equipment Identity (IMEI) code, a International Mobile Subscriber Identity (IMSI) code, or a Media Access Control (MAC) address.

16. The system according to any one of claims 11 to 15 wherein markers are added to the head or tail of each batch of the data when NFC communication is interrupted.

17. The system according to any one of claims 11 to 16 wherein the prescribed format comprises a complete document manifested as several character fields of equal length or part thereof; the partial abstract of a

complete document, numbers or diagrams in the document, image information of a video, text, drawings, graphs, photographs or combinations of one or more of the above.

18. The system according to any one of claims 11 to 17 wherein the communication device may be a mobile computing device such as a mobile phone, tablet, laptop or personal digital assistant.