Other mobile payment applications and associated services exist, typically having a similar functionality and potentially incorporating similar solutions. Examples are Apple Pay (operating on iOS devices) and Google Wallet (operating on Android devices).

Mobile payment applications require access to sensitive data for their operation. There are known mechanisms for holding secure data and performing secure operations on a mobile device. One approach is to use a secure element (SE) in the mobile device. A conventional SE is a tamper-resistant physical device, generally physically and logically protected to allow operations and data taking place in it to be trusted by other system elements. Another approach is to use a trusted execution environment (TEE) – this is an isolated execution environment provided by the main processor of the mobile device adapted so that code and data loaded within it is confidential and integrity protected. The TEE operates in parallel to the main operating system of the mobile device, and certain aspects of payment processing are carried out in the TEE for added security. For Android devices, a software architecture termed host card emulation (HCE) has been introduced (from Android 4.4 onwards) to provide representations of electronic identity using software alone without the use of a secure element – this has been used to achieve transactions using near field communication (NFC) protocols.

Often, those solutions that do not make use of a secure element within the mobile device require the periodic supply of session keys from a secure cloud-based server owned by the card issuer. This can be problematic when carrying out a large number of transactions, as there are a limited number of session keys available.

Against this background, the present disclosure aims to provide a method of carrying out payment transactions securely using a mobile phone (or other mobile device), without the need for either a chip-based SE or the periodic supply of session keys using a cloud-based solution.

SUMMARY

According to an aspect of the disclosure, there is provided a mobile computing device having at least one processor and at least one memory, together providing a first execution environment and a second execution environment logically isolated from the first execution environment. The mobile computing device comprises a mobile payment application executable within the first execution environment and configured to

perform payment processing with a point-of-interaction (POI) terminal. The mobile computing device

comprises a trusted application executable within the second execution environment and configured to store digitized card information. The mobile computing device comprises a secure communications channel between the mobile payment application and the trusted application. The trusted application is configured to generate one or more encrypted digitized card data items within the second execution environment and to provide the one or more encrypted digitized card data items for processing a mobile payment to the mobile payment application via the secure communications channel without exposing digitized card information to the mobile payment application in the first execution environment.

An advantage associated with the above-described configuration is that it provides for a highly flexible, simple and secure means for carrying out secure processing by utilizing the capabilities of a trusted execution environment (TEE) and a Rich execution environment (REE) within a user's mobile device. It is not necessary in the above configuration for any external system elements to be utilized in the main processing steps. The above configuration also has an advantage in that it allows the most sensitive information to be retained securely within the TEE (and never released to the REE), whilst enabling the majority (if not all) of the processing to be carried out within the mobile device.

Optionally, the trusted application is configured to receive configuration data from the mobile payment application via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

Advantageously, in the above-described configuration, the mobile payment application may comprise all of the software libraries and logic required to carry out the process, and is able to simply call the trusted application at the appropriate time to generate the encrypted digitized card data items securely. The present disclosure therefore effectively separates the processing steps between the REE and the TEE, and improves the flexibility and security of the system.

Optionally, a first one of the one or more encrypted digitized card data items comprises an authentication code for use in authenticating a process executed by the mobile payment application in the first execution environment.

Advantageously, the generation of an authentication code by the trusted application within the secure TEE, and its subsequent transmission to the mobile payment application to authenticate the process carried out by the mobile payment application (in the relatively less secure REE), increases the security of the system as sensitive data does not leave the TEE.

Optionally, the trusted application is configured to generate the authentication code by combining a plurality of data elements, and the plurality of data elements to be combined is dependent on the type of process to be executed.

The trusted application is able to tailor the properties of the authentication code generated to suit the needs of the particular process which is being carried out by the mobile payment application. This functionality of the present disclosure is advantageous as it provides for a highly flexible authentication system with all the benefits associated with using the secure environment of the TEE.

Optionally, at least one of the plurality of data elements is received by the trusted application from the mobile payment application via the secure communications channel.

The trusted application is able to receive additional data or information via a secure communications channel from the mobile payment application in order to generate an authentication code. This means that the trusted application does not require all of the requisite information to be provided to it initially or subsequently by an additional external source, and is able to flexibly incorporate information obtained by the mobile payment application from the user whilst the process is being carried out. This increases the flexibility and security of the system, and may be especially useful when carrying out transaction processes where information provided by a user during the transaction is used as part of the input when generating the authentication code.

Optionally, at least one of the plurality of data elements is stored by the trusted application within the second execution environment.

The present disclosure allows the trusted application to pre-store data within the TEE that is required for the generation of an authentication code. This advantageously increases the security of the system as it ensures that certain sensitive data elements required for generation of the authentication code can be provided to the trusted application to be retained securely within the TEE, and are not output directly to the relatively less-secure REE.

Optionally, the mobile payment application is configured to execute a payment transaction. The payment transaction may correspond to any one of:

a remote payment transaction, an NFC-enabled transaction, and a magnetic stripe transaction.

Advantageously, the present disclosure ensures that a high level of security is able to be maintained for the multiple different types of payment transactions which the mobile computing device is configured to carry out.

Optionally, the one or more encrypted digitized card data items comprise at least one of: a unique representation of the payment transaction, and an authentication code for use in authenticating the payment transaction.

Advantageously, the trusted application may generate an ATC (Application Transaction Counter), or other type of unique representation of the transaction, within the secure TEE, thereby increasing the security of the payment process as sensitive data is processed and retained only within the TEE. In addition, generating a transaction authentication code (e.g. a cryptogram or Message Authentication Code MAC) within the secure TEE, which code is used to verify that a particular transaction has been successfully carried out and that cardholder verification has been performed successfully, ensures that the security of transaction is maintained and that external (or additional) verification of the transaction is not required.

The trusted application may be configured to generate the authentication code by combining a plurality of data elements, where the plurality of data elements to be combined is dependent on the type of payment transaction to be executed.

Optionally, at least one of the plurality of data elements may be stored by the trusted application within the second execution environment.

The trusted application is able to generate different types of cryptograms, tailoring each cryptogram generated to the type required to authenticate a particular transaction type. For example, the cryptogram associated with an MST transaction is different from that associated with a remote or Internet transaction. This functionality of the present disclosure is advantageous as it provides for a highly flexible authentication system, largely contained within the secure environment of the TEE.

Optionally, the mobile computing device further comprises a biometric sensor for use in authenticating a user of the device.

Advantageously, this allows the device to securely verify the identity of a user using biometrics. Although the use of biometric verification does increase the security of the process, it should be noted that other methods of verifying a user's identity may also be applied in the present disclosure (e.g. user password entry).

Optionally, the mobile computing device further comprises a secure data connection to an external server of a provider of the mobile payment application.

Advantageously, this allows the mobile computing device (and therefore the mobile payment application) to communicate with an external server of the payment provider or card issuer, and thereby to receive data of information relating to the process executed by the mobile payment application. In the context of a payment transaction, this received data may be used in the generation of a MAC and the authentication of the transaction by the trusted application.

According to another aspect of the disclosure, there is provided a method of managing data items in a mobile computing device, the mobile computing device having at least one processor and at least one memory together providing a first execution environment and a second execution environment logically isolated from the first execution environment. The method comprises establishing a secure communications channel between a mobile payment application in the first execution environment and a trusted application in the second execution environment, the mobile payment application configured to perform payment processing with a point-of-interaction (POI) terminal and the trusted application configured to store digitized card information. The method comprises generating one or more encrypted digitized card data items within the second execution environment by the trusted application and providing the one or more encrypted digitized card data items for processing a mobile payment to the mobile payment application via the secure communications channel without exposing digitized card information to the mobile payment application in the first execution environment. The method comprises executing the mobile payment application in the first execution environment.

Optionally, the method further comprises receiving at the trusted application configuration data from the mobile payment application via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

Optionally, the method further comprises authenticating a process executed by the mobile payment application in the first execution environment, and wherein a first one of the one or more encrypted digitized card data items comprises an authentication code for use in authenticating the process.

Optionally, the method further comprises generating the authentication code by combining a plurality of data elements, where the plurality of data elements to be combined is dependent on the type of process to be executed.

It should be noted that advantages which have been described previously in relation to aspects of the disclosure, when expressed in terms of a system or device, apply equally as advantages of the disclosure when expressed in terms of a method.

Optionally, the method further comprises initializing the mobile payment application and trusted application by receiving setup data transmitted from a remote trusted party to the mobile payment application and the trusted application.

Advantageously, the present disclosure allows the functionality of the two applications to be set in an initialization or personalization step, where instructions for carrying out the process are provided to the applications, via a secure communications channel, from the application service provider prior to the process being executed. This increases the flexibility of the method when handling and executing different processes, as the applications are pre-programmed with all the data and instructions necessary to carry out all processes.

Optionally, the setup data is received by the trusted application without being processed by the mobile payment application.

Advantageously, this allows the sensitive data to be transmitted directly to the trusted application, and subsequently processed and stored within the TEE, bypassing the mobile payment application in the relatively less secure REE. This increases the security of the present method whilst still enabling all necessary provisioning data to be provided to the mobile computing device before execution of any processes.

Optionally, the setup data comprises at least one of the plurality of data elements, and initializing the trusted application further comprises storing the at least one of the plurality of data elements by the trusted application within the second execution environment.

Optionally, the method further comprises determining which ones of the plurality of data elements are to be combined to generate the authentication code based on a set of instructions forming at least a part of the setup data.

Advantageously, the above-described method ensures that, during initialization and setup, some or all of the data elements used by the trusted application to generate the authentication code for a particular process may be provided to and stored by the trusted application, via a secure communication channel. When the process is executed and the trusted application is called by the mobile payment application, the trusted application is able to access all the necessary data, and has also been provided with the necessary instructions to determine which data elements should be combined to generate an authentication code unique to the type of process executed. This increases the security of the method, as it does not require any additional transmission of data or instructions from an external server during execution of the process. This is particularly important when executing a payment transaction process, where the security of the data is paramount, and there may not be a secure communication channel readily available at the time when the authentication code is required to be generated.

Optionally, the method further comprises processing the setup data by the trusted application; and identifying (a) any sensitive data elements comprised within the setup data and (b) any data elements comprised within the setup data that relate only to the mobile payment application.

Optionally, the method further comprises retaining, by the trusted application, the sensitive data elements within the second execution environment; and transmitting, from the trusted application to the mobile payment application via the secure communications channel, the data elements relating only to the mobile payment application.

It may be advantageous for all of the setup data (even that intended for the first application) to be first transmitted to and processed by the trusted application, which is located within the secure TEE. In the above-described method, the trusted application is able to identify data elements that are particularly sensitive and should not leave the TEE, as well as any data elements that should be transmitted to the first application to complete its setup. The mobile payment application (in the relatively less secure REE) is therefore only provided with the data required to carry out its functions, and the

sensitive data never leaves the secure environment. This segregation of data provisioning and storage allows the majority (if not all) of the processing and authentication to be carried out in situ by the mobile computing device implementing the above method, without necessitating any external authentication or transmission of sensitive data during execution of the process. The flexibility and security of the system is therefore increased.

Optionally, executing the mobile payment application corresponds to executing a payment transaction. The method may further comprise generating the one or more encrypted digitized card data items by generating at least one of: a unique representation of the payment transaction, and an authentication code for use in authenticating the payment transaction.

The above described methods are particularly advantageous when applied to payment transaction processes, which necessarily require flexibility and a high degree of security when generating authentication codes (e.g. cryptograms).

Optionally, the method comprises generating the authentication code by combining a plurality of data elements, and the plurality of data elements to be combined is dependent on the type of payment transaction to be executed.

Optionally, the method comprises storing, by the trusted application, at least one of the plurality of data elements within the second execution environment.

Within the scope of this application, it is expressly intended that the various aspects, embodiments, examples and alternatives set out in the preceding paragraphs, in the claims and/or in the following description and drawings, and in particular the individual features thereof, may be taken independently or in any combination. That is, all embodiments and/or features of any embodiment or claim can be combined in any way and/or combination, unless such features are incompatible. The applicant reserves the right to change any originally filed claim or file any new claim accordingly, including the right to amend any originally filed claim to depend from and/or incorporate any feature of any other claim although not originally claimed in that manner.

BRIEF DESCRIPTION OF THE FIGURES

CLAIMS

1. A mobile computing device (1) having at least one processor (101) and at least one memory (102), together providing a first execution environment and a second execution environment logically isolated from the first execution environment, the mobile computing device comprising:

a mobile payment application (14) executable within the first execution environment and configured to perform payment processing with a point-of-interaction (POI) terminal;

a trusted application (16) executable within the second execution environment and configured to store digitized card information; and

a secure communications channel between the mobile payment application and the trusted application,

wherein the trusted application is configured to generate one or more encrypted digitized card data items within the second execution environment and to provide the one or more encrypted digitized card data items for processing a mobile payment to the mobile payment application (14) via the secure communications channel without exposing digitized card information to the mobile payment application in the first execution environment.

2. The mobile computing device of Claim 1, wherein the trusted application (16) is configured to receive configuration data from the mobile payment application (14) via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

3. The mobile computing device of Claim 1, wherein a first one of the one or more encrypted digitized card data items comprises an authentication code (400) for use in authenticating a process executed by the mobile payment application (14) in the first execution environment.

4. The mobile computing device of Claim 3, wherein the trusted application (16) is configured to generate the authentication code (400) by combining

a plurality of data elements (405, 415, 425), and the plurality of data elements to be combined is dependent on the type of process to be executed.

5. The mobile computing device of Claim 4, wherein at least one of the plurality of data elements (405, 415, 425) is received by the trusted application (16) from the mobile payment application (14) via the secure communications channel.

6. The mobile computing device of Claim 4, wherein at least one of the plurality of data elements (405, 415, 425) is stored by the trusted application (16) within the second execution environment.

7. The mobile computing device of Claim 1, wherein the mobile payment application (14) is configured to execute a payment transaction.

8. The mobile computing device of Claim 7, wherein the payment transaction corresponds to any one of: a remote payment transaction, an NFC-enabled transaction, and a magnetic stripe transaction.

9. The mobile computing device of Claim 8, wherein the one or more encrypted digitized card data items comprise at least one of: a unique representation (425, 540) of the payment transaction, and an authentication code (400, 500) for use in authenticating the payment transaction.

10. The mobile computing device of Claim 1, further comprising a biometric sensor (10) for use in authenticating a user of the device (1).

11. A method of managing data items in a mobile computing device (1), the mobile computing device having at least one processor (101) and at least one memory (102) together providing a first execution environment and a second execution environment logically isolated from the first execution environment, the method comprising:

establishing a secure communications channel between a mobile payment application (14) in the first execution environment and a trusted application (16) in the second execution environment, the mobile payment application (14) configured to perform payment processing with a point-of-interaction (POI) terminal and the trusted application (16) configured to store digitized card information;

generating one or more encrypted digitized card data items within the second execution environment by the trusted application (16) and providing the one or more encrypted digitized card data items for processing a mobile payment to the mobile payment application (14) via the secure communications channel without exposing digitized card information to the mobile payment application in the first execution environment; and

executing the mobile payment application (14) in the first execution environment.

12. The method of Claim 11, further comprising receiving at the trusted application (16) configuration data from the mobile payment application (14) via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

13. The method of Claim 11 , further comprising authenticating a process executed by the mobile payment application (14) in the first execution environment, and wherein a first one of the one or more encrypted digitized card data items comprises an authentication code (400) for use in authenticating the process.

14. The method of Claim 13, wherein generating the authentication code (400) comprises combining a plurality of data elements (405, 415, 425), and the plurality of data elements to be combined is dependent on the type of process to be executed.

15. The method of Claim 14, further comprising initializing the mobile payment application (14) and trusted application (16) by receiving setup data transmitted from a remote trusted party (44) to the mobile payment application (14) and the trusted application (16).

5

16. The method of Claim 15, wherein the setup data is received by the trusted application (16) without being processed by the mobile payment application (14).

17. The method of Claim 15, wherein the setup data comprises at least one of the plurality of data elements (405, 415, 425), and initializing the trusted application (16) further comprises storing the at least one of the plurality of data elements by the trusted application (16) within the second execution environment.

18. The method of Claim 15, further comprising determining which ones of the plurality of data elements are to be combined to generate the authentication code (400) based on a set of instructions forming at least a part of the setup data.

19. The method of Claim 15, further comprising:

processing the setup data by the trusted application (16); and

identifying (a) any sensitive data elements comprised within the setup data and (b) any data elements comprised within the setup data that relate only to the mobile payment application (14).

20. The method of Claim 19, further comprising:

retaining, by the trusted application (16), the sensitive data elements within the second execution environment; and

transmitting, from the trusted application (16) to the mobile payment application (14) via the secure communications channel, the data elements relating only to the mobile payment application.