

IMPROVED COMPUTER-IMPLEMENTED SYSTEMS AND METHODS FOR SECURE ELECTRONIC
TRANSFERS

TECHNICAL FIELD

5 The present disclosure relates to improvements in secure transfer or exchange of data across electronic networks. In particular, embodiments disclosed herein provide solutions for processing sensitive data on electronic devices. Advantageously, these devices can comprise consumer off-the-shelf devices such as mobile phones, laptops, tablets etc. which typically lack the integral security mechanisms required for storing and/or processing highly sensitive data.

10

Additionally, or alternatively, embodiments of the disclosure can be described as providing technical solutions for the secure performance of operation(s) and/or communication(s) across an electronic network between two or more participants. Such operations and communications may require the transfer, exchange, storage and/or processing of sensitive data in order to perform the operation(s).

15

Additionally, or alternatively, embodiments of the disclosure can be described as providing technical solutions for securing, permitting and/or denying access to at least one controlled resource. Such solutions may comprise systems and methods for authenticating the identity of at least one entity that wishes to gain access to the controlled resource(s).

20

BACKGROUND

There are many situations, for example within the payments industries and other application areas, in which sensitive data needs to be exchanged between sending and receiving parties. In some instances, the sender and receiver might belong to the same organisation, but in others they may not. As a result, there may be a lack of trust between the parties involved. Moreover, given the ubiquitous nature of mobile or portable technologies in today's world, the performance of such transfers often needs to involve such commercially available end-user devices. However, mobile/portable devices such as smart phones are not deemed secure enough for the transfer of highly sensitive data such as, for example, cryptographic keys, passcodes etc.. The sensitive data could, for example, be used to control access to a controlled resource such as a bank account, a computing network, a building or vehicle, a patient's medical or personal records in a database or other storage facility, military data and so on.

25

30

Although the present disclosure is not limited with regard to this application area, in the context of financial transactions such technical challenges are met using a 'fixed purpose' device (such as a softpos, Pos or other type of payment terminal) that is provided to a merchant by a supplier. The supplier sets up i.e. configures the device for the specific merchant so that the merchant can perform transactions securely. This includes providing cryptographic keys and other merchant-specific configuration data on the device. Thereafter, the configuration of the merchant's device does not change. Moreover, such payment devices are typically hardware specific, in that a device provided by one supplier will not work with other supplier's systems. As a result, the merchant's device will only allow users (customers) to transact with the merchant's contracted acquirer. Clearly, though, challenges arise in situations where the merchant and the user are not co-located, or where the user wishes to use the same CoTS device to perform secure transactions with a plurality of different merchants who are not all associated with the same acquirer.

Therefore, technical challenges arise such as to how to establish identity, ensure secure communication, storage and processing of sensitive data even on an insecure end-user device, how to enhance the versatility of such user devices for use in a wider range of transaction environments, and how to perform data exchanges across distinct, different electronic networks in a way that ensures that only authorised parties are able to access that sensitive data and other controlled resources. Embodiments of the present disclosure provide systems and methods that address at least these challenges.

SUMMARY

Preferred embodiments of the disclosure provide solutions which enable or facilitate configuration of an electronic device such that it becomes temporarily operative to use, emulate, duplicate or extend the state of a further (remote) electronic device.

The electronic device may also be configured for secure communication with one or more remote computing resources to facilitate sharing or transmissions of (potentially sensitive) data between them. Preferably, the configuration of the electronic device is performed dynamically. In a preferred example, this may mean that the configuration is performed on the electronic device upon demand, as and when said communication or data sharing is required for the purposes of performing a specific, pre-defined (transfer) operation. Installation of the configuration on the electronic device may be triggered, requested or initiated by an event performed by an

operator/user of the electronic device. Thus, in some embodiments, the configuration of the electronic device lasts only while required for performance of the predefined operation and is removed from the electronic device thereafter.

5 Preferably, one or more of the following may apply:

- the electronic device comprises hardware, firmware and/or software that enables it to perform processing functionalities; in some examples, it may comprise a commercial, off-the-shelf (COTS) device; in some examples it may comprise a mobile, handheld or portable device such as a cellular (mobile) phone, a laptop, a tablet etc., although the disclosure is not
10 limited in this regard; hereafter, for convenience only, the user's electronic device may be referred to as a mobile phone; the phone may be operated by a first entity which we may call a user, end user, first user, customer, first operator, consumer, cardholder etc. In some examples, the electronic device comprises a touchscreen, camera, speaker, microphone, biometric reader, smart card reader, face recognition functionalities, wireless
15 communications capabilities such as Bluetooth, NFC, telecommunications and internet connectivity. In some embodiments, the install/uninstall of the configuration of the user's electronic device may be controlled, performed or influenced by a software component or application installed on the electronic device. The software component/application may be referred to hereafter for ease of reference as a "Software Development Kit (SDK)"; in other
20 embodiments, the install/uninstall of the configuration may be performed on demand. For example, it may be triggered by an action, signal detection or electronic communication/transfer event such as, for example, an action comprising the scanning of a QR code, receipt of an electronically transmitted message such as email, sms or communication via a messaging app, or receipt of some other signal/communication at or by
25 the user's electronic device;
- the further resource may comprise processing and communication capabilities such that it is operative to initiate, facilitate and/or complete the pre-defined operation. The further resource may be remote relative to the electronic device. The term 'remote' should not be
30 construed as implying a geographical distance or relative physical proximity, but rather that it is distinct and separate from the electronic device.
In some examples, the further device may comprise a terminal, a Point-of-Sale (PoS) or ePOS device/system, an on-line commerce resource or other arrangement operative to initiate and/or perform a financial transaction; in such examples, the further resource may be

referred to herein as a “merchant device” for convenience. The further resource may be operated by a second entity which we may call a middle/second/further user or operator, merchant etc.

In some examples, the further device may be a virtual device rather than a physical one e.g. an eCommerce or payment gateway. In some other cases the further device may be a physical device e.g. a payment terminal provided by an acquiring bank or payment solutions provider to a particular merchant and configured for use by that particular merchant when performing secure transactions with customers.

In some embodiments, the configuration of the further device may be static, in that once the further device has been configured, that initial configuration does not change. In some examples, the configuration may comprise at least one configuration file and/or secret key associated with the further device.

- the operation may comprise, for example, a financial transaction, a calculation, verification of the user’s identity prior to permitting access to one or more controlled resources, a secure communication etc. For convenience only, the operation may be referred to hereafter as a ‘transaction’ but this is intended to be construed in a generic sense and the disclosure is not limited to use solely in respect of financial transactions. The phrase ‘authentication session’ may be used interchangeably with ‘transaction’ or ‘operation’.

In a preferred embodiment, the transaction may comprise a process for authorisation of access to a controlled resource. Such a process may comprise the verification of a user’s identity and/or authorisation prior to allowing access to the controlled resource(s). For example, the controlled resource may comprise a vehicle, device, building, an electronic account, a file storage resource, a web site, etc. The operation may be performed in association with a transaction entity such as a financial organisation or institution e.g. an acquiring bank, or a locking/unlocking device arranged to permit or deny access to a building or vehicle etc. The transaction entity (which we will refer to hereafter for ease of reference as “the acquirer”) may own, control, operate or be otherwise associated with the remote resource.

In summary, then, the disclosure may provide embodiments which create, dynamically and on-demand, a temporary replica of a second entity’s statically configured further device on a first entity’s electronic device to enable or facilitate a transfer between the further device and the electronic device. In some examples, the embodiment comprises creating the replica by generating

a new, unused instance of the further device on the electronic device, and then (on a per transfer/on-demand basis) configuring the instance by providing it with one or more configuration files and or keys, thus cloning the state of the further device on the electronic device.

- 5 In one or more embodiments may comprise the step of using a software component (SDK) that has been provided/installed on the user's electronic device (e.g. phone) to temporarily extend, project, duplicate, replicate or emulate the state of the further device (e.g. merchant terminal) on the user's electronic device e.g. phone. Thus, the SDK may be arranged to configure the phone (or a portion thereof, e.g. a virtual machine, enclave, TEE, HSM or other secure portion of the user's device) to
- 10 emulate the further device. In other embodiments, the dynamic, temporary and on-demand configuration may be performed in response to a trigger, such as the receipt of a signal or one or more instructions received by a processor of the phone.

- The state of the further resource may comprise one or more cryptographic keys. Additionally, or
- 15 alternatively, it may comprise one or more portions of configuration data (which may be referred to for convenience as configuration files). The cryptographic key(s) and/or configuration file(s) may have been provided to the further resource from a third entity or resource that has ownership or control of the controlled resource. This third entity may be, for example, an acquiring bank, payment aggregator or payment solutions provider. Additionally, or alternatively, the cryptographic
- 20 key(s) and/or configuration file(s) may uniquely identify the further resource to the third entity.

- The phone may use at least part of the state of the further device (e.g. the cryptographic key(s)) to identify itself to the third entity and/or communicate with the third entity as if it is the further resource. For example, the phone may use the emulated state to present itself to an acquiring bank
- 25 as if it is a particular merchant for the purpose of conducting a specific financial transaction. In another example, the phone may emulate the secure configuration of an electric car to enable a driver to authorise a software download, or enable a user to authorise security updates on a laptop etc.

- 30 Upon completion of the operation, the software component may uninstall the configuration from the user's device so that it returns to its prior state. In other words, the configuration of the user's device may be returned to how it was prior to installation of the state of the further device.

These and other aspects of the present invention will be apparent from and elucidated with reference to, the illustrative embodiment(s) disclosed herein. An illustrative embodiment of the present disclosure will now be described, by way of example only, and with reference to the accompanying Figures.

5

LIST OF FIGURES

Figure 1 provides a flowchart illustrating an example embodiment of the disclosure in use.

Figure 2 provides an overview of resources, device and actors involved during an example embodiment of the disclosure in use.

- 10 Figure 3 provides an illustration of a possible computing environment which may be used for implementation of one or more embodiment of the disclosure.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

We now provide some example embodiments, for the purpose of illustration and without limitation.

15

As explained above, embodiments of the present disclosure provide improved solutions that enable users to perform electronic exchanges with other parties in a secure way, even if the user is making that transaction from a commercially available CoTS (commercial off-the-shelf) device such as a mobile phone. In an example scenario, where the user wishes to transact with a merchant, the traditional scenario is that the merchant presents the user with a secure PoS terminal that the user can tap their payment card on or insert into. Clearly, though, this is not possible in situations where the user is not physically present in the merchant's store.

20

Advantageously, embodiments of the present disclosure address such challenges by providing a blank terminal on the user's device, such that the blank terminal can be configured as a clone of the merchant's device, almost instantaneously such that the transaction can be performed on the user's device as if the user was physically present at the location of the merchant's device. Preferably, this means that an embodiment of the disclosure is arranged to replicate the merchant device, remotely, onto the user's device in almost real time for a single transaction, before removing/destroying the replica merchant device from the user's device. This not only ensures that the transaction is secure, but that the user is able to transact with different merchants using the same device but simply replicating a different merchant device on it each time.

25

30

Thus, in a preferred example, an embodiment provides, emulates, extends or projects the estate of a (particular) merchant's system (further device) onto a user's (consumer) electronic device.

Traditionally, the estate of the merchant's payment system would comprise one or more payment devices (which may also be called 'terminals') located in venues such as shops or other facilities where the transaction is to take place; the payment terminal would typically comprise hardware, firmware and/or software. Each payment terminal comprises acquirer's (cryptographic) keys and configuration. A Terminal Management System (TMS) is typically used to provision new payment devices, update configurations, update keys, and remove payment terminals from the merchant's payment system. With MPOS, however, the mobile device plus the payment app becomes the terminal. In recent times this has been performed using a hardware dongle that is inserted into the merchant's device. Advantageously, embodiments of the present disclosure remove the need for the merchant's hardware dongle and, instead, are able to utilise the NFC reader and other capabilities that are now commonly provided within mobile devices.

Embodiments of the disclosure enable the user to install an emulation, or virtual copy, of the secure terminal software on their COTS device. In some examples, this is performed using a software installation (that we will call the SDK) provided on the user's device. This enables verification and assurance that the runtime environment on the user's device meets the same security requirements as the merchant's traditional payment device. Embodiments thus create a copy of the merchant's device on the user's device. The copy may be identical to, or so closely resemble, the merchant's device that another device that is arranged to interact with the merchant device is unable to distinguish the two from one another. In other words, the copy provides the functionality and data expected of the merchant device by a further device. This is achieved by temporarily providing cryptographic keys and other necessary configuration data onto the user's device, thus extending the merchant's terminal estate and configuration onto the user/cardholder's device. For completion of the transaction, therefore, the user's device appears to the issuing bank as if it is the merchant's original (traditional) payment terminal.

In essence, embodiments of the disclosure provide the ability to:

- provide, to an end user, a software application or component thereof (which we may call an SDK) that is operative to replicate one or more configuration elements e.g. security data or settings of a further device on the user's device; in an alternative wording, embodiments may provide, to a user's device via a software application or component thereof, the

security and other functionality of a further device; in yet another form of wording, embodiments may provide, on a user's device, a virtual device which emulates the further device (at least in part);

- This may comprise temporarily providing security data such as one or more keys and /or one or more parameters to the virtual device that is generated on the user's device, wherein the key(s) and/or parameter(s) match those provided on or in association with the further device; this ensures that the technical environment that is created on the user's device meets the same security requirements that are required and provided by the further device.

Thus, in the prior art, each merchant terminal comprises its own public/private key pair which can be used to identify and authenticate transactions that it performs. The key pair does not change, because the merchant always uses the same acquirer. Therefore, the traditional terminal never changes, and always contains the same key(s) and configuration that were supplied by the TMS when it was set up.

However, in accordance with the disclosure, the acquirer is able to be changed on the user's device each time the user chooses to transact with a different merchant. Thus, the configuration (config files including keys, identifiers and other parameters etc) of the virtual terminal on the user's device is changed for each new merchant. This can be achieved via two approaches:

1) via a standalone app:

in this approach, the SDK does not include any state (config files or keys) for any particular acquirer or merchant; therefore, they need to be injected into the new virtual terminal that is created for each desired transaction; this can be performed via any suitable mechanism such as via a scanning of a QR or clicking a link as explained in more detail below, and the standalone app (which comprises the SDK) is transmitted to the user's device and the new virtual terminal is created on it;

2) via an embedded SDK

in this approach, a particular merchant provides an app that has the SDK embedded in it; as the merchant always uses the same acquirer for each transaction, the virtual terminal does not need to change configuration data for each transaction. In such cases, the configuration data could be encrypted and stored on the phone, ready to be decrypted and used when a transaction is to be performed, or transmitted to the phone for each transaction.

Whichever approach is used, embodiments of the disclosure create a virtual terminal on the user's phone at the start of each transaction, the merchant's configuration data (e.g. config files, cryptographic keys etc) are provided to the virtual terminal, the transaction is performed between the issuer and the acquirer, and upon completion of the transfer the virtual terminal is erased from the user's device.

The user performs the transaction on their device as if it is the merchant's physical payment terminal. This may comprise one or more user authentication sessions that the user must successfully perform in order to perform the transaction. For example, user authentication may comprise one or more of the provision of a secret identifier (e.g. PIN, password, memorable phrase, answer to pre-determined security question etc), biometric authentication, and/or the presentation of a security token or device. User authentication may include presenting a smart card such as a payment card to the virtual terminal on the user's device. This may be achieved by reading data such as cryptographic keys etc from a chip on the smart card or other device. The card data may be obtained from the card by the user's device via wireless means e.g. using Bluetooth, NFC communication etc, or by insertion or proximity of the card into a data reader arrangement provided within or coupled to the user's device.

1. In Use example #1 – Financial Transaction

It would be advantageous for at least the reasons mentioned herein if individuals were able to use their mobile devices to securely purchase goods and services. However, it is well known that mobile phones and other such consumer devices are inherently insecure devices, so traditionally such payments would need to be made through a secure terminal provided by a merchant's acquiring institution (such as a bank) or payments solutions provider (PSP). The secure terminal comprises the necessary state to ensure that it complies with industry standards, ensuring security of the sensitive data associated with the terminal. This includes at least one private, cryptographic key which the terminal provider (AI or PSP) injects into the secure terminal for a given merchant, and which the terminal will provide to the acquirer when a payment is made so that the merchant terminal can verify its identity and prove that the transaction is being made by a legitimate source.

In order to emulate the merchant's device on a user's mobile device, a configuration needs to be performed on the mobile device. This configuration process involves two phases:

1) the invitation:

in this phase, the merchant opens their estate for expansion by first requesting the

generation of an invitation. The request is sent to the merchant's terminal provider such as their acquiring bank or PSP; in response, the terminal provider provides the merchant with an invitation code or other trigger mechanism that can be used to accept the invitation

2) the acceptance:

5 in this phase, if the cardholder (end user/customer) decides to proceed with payment via their mobile device, they need to accept the merchant's invitation to project their payment terminal onto the mobile device. In other words, the cloning of the merchant terminal only occurs if it is permitted to do so by the end user.

10 With particular reference to Figures 1 and 2, an overview of a non-limiting, illustrative embodiment can be described as follows.

In step 1 of Figure 1, a user (Alice, 201) wishes to purchase at least one item or service from a sales resource 203 that is provided by a merchant (Bob, 202). In the example of Figure 2, the sales
15 resource is an online store such as a web site, but in other examples the store may be a physical shop or some other sales location such as a mobile app, an in-game purchase facility or some other type of virtual sales resource that a user (Alice, 201) can obtain services or goods from.

In step 2 of Figure 1, in order to make the transaction for her chosen purchase(s), Alice initiates
20 ('triggers') the remote payment process on her electronic device (e.g. mobile phone or tablet 206, or computer 207 of Figure 2). The trigger mechanism may comprise a variety of technical arrangements such as, but not limited to, a QR code for capture and interpretation by a camera on the device 206/207, or a hyperlink that can be clicked on, or a voice recognition component that is arranged to detect, interpret and act upon the user's audio input etc). The trigger may comprise any suitably
25 arranged technical means.

Alice's device comprises a software application ('SDK') which enables a freshly generated virtual terminal to be constructed on Alice's device for that particular transaction. At this point in the process, the newly generated terminal does not contain the necessary elements or features that
30 would be required to complete the transaction, as it has not yet been bound to, or associated with, the merchant (Bob, 202).

In step 3 of Figure 1, this binding is achieved by sending the configuration data from the acquiring resource 205 to the device 206, 207. The configuration data may comprise at least the set up files

(which may also be called the configuration files) and the cryptographic keys for that transaction session. Once the configuration data has been received at Alice's device, it is used by the SDK to configure the freshly generated virtual terminal. Thus, the combination of the configuration data plus blank terminal on Alice's device provides a functional and secure terminal that emulates a
5 secure physical payment terminal as if Alice was present in Bob's store. At this point in the process, the virtual terminal becomes subject to card payment industry standards.

In step 4 of Figure 1, the relevant transaction data is displayed on Alice's phone e.g. merchant's name, logo, the transaction amount, instructions for making payment etc. In an example
10 embodiment, the transaction data is obtained from information contained in the QR code, the resource referenced by the link etc.

In step 5 of Figure 1, Alice 201 makes the required payment by entering her payment card 208 details into the virtual terminal. This can be achieved via any suitable technical means. For example,
15 this could comprise tapping her payment card 208 against the device for detection by a contactless card reading component, or by retrieving a card payment token stored in a wallet on the device e.g. for Apple™ pay, or swiping a magnetic stripe through a reading device associated with Alice's device 206, 207. (It should be noted that in other use cases, which do not relate to payments and financial solutions, the authentication device may not be a payment card 208. Instead, the authentication
20 device presented by the user may comprise a smart card or some other device that comprises one or more of: a security token, a digital certificate, a cryptographic key, a SIM, a signal emitter, an RFID device etc. For example, this may comprise a key fob for a vehicle, an access card for a building and so on. The authentication device may comprise hardware and executable instructions arranged for execution by the hardware, or the authentication device could comprise a virtual device i.e. it could
25 comprise only machine executable instructions).

In step 6 of Figure 1, the virtual terminal on Alice's device reads the payment card 208 details obtained in step 5.

30 In step 7 of Figure 1, a further user authentication process is performed for additional security; in the example embodiment of Figure 7, a PIN pad is displayed on Alice's device, as known in the art of payment solutions and other secure systems for authentication of a user. The term 'PIN pad' may be used interchangeably herein with 'keypad' and 'keyboard'). The PIN pad may comprise symbols or indicia that are associated with respective keys. The symbols may comprise numeric digits,

alphabetical letters, grammatical and punctuation marks, currency symbols, function symbols etc. IT should be noted that the user authentication can comprise any suitable authentication mechanisms such as comprising the use of one or more of: a password, PIN or other secret identifier check, a biometric check, facial/voice recognition, memorable phrase etc. For the sake of illustration, Alice
5 uses a PIN entry authentication in this example.

In step 8 of Figure 1, Alice enters her authentication identifier (PIN) into the PIN pad. The authentication identifier is a secret that is associated with Alice, and can take any suitable form. In some examples, the identifier may be a sequence of numeric digits (e.g. a PIN) or a combination of
10 symbols such as a password. The identifier may be provided via a touchscreen that is associated with Alice's device, or by some other selection and input arrangements such as a mouse or other pointing device, or a keyboard, joystick etc. In other examples, the secret authentication identifier may comprise audio signals for capture by a microphone provided in association with Alice's device. In any event, Alice enters her secret identifier into the terminal via a suitably arranged
15 hardware/software interface.

In step 9 of Figure 1, the virtual terminal determines whether or not Alice is authorised to make this transaction using the payment card 208 (i.e. authentication device) that she has presented. This comprises checking, with the card provider 204, that the secret identifier that it has received from
20 Alice matches a stored version of the identifier. The virtual terminal may encrypt the received identifier and transmit it to the card provider 204 for comparison with Alice's stored secret. It should be noted that in Figure 2 the issuing bank 204 is shown as that card provider but this may not be the case in every embodiment, and the authentication device 208 may be provided by any authorised party as required for a given implementation.
25

In step 10 of Figure 1, if Alice's input does not correspond to the stored secret known by the card provider 204 to be associated with Alice's payment card, the transaction fails. A 'declined' or 'access denied' message may be provided to Alice to inform her of the failure.

30 In step 11 of Figure 1, an alternative scenario is illustrated in which the input does match the stored secret associated with the payment card 208, and the transaction is completed. This may comprise sending funds from the issuing bank 204 to Bob's acquiring bank 205, or unlocking a resource such as a physical object, building, vehicle etc., or allowing access to an electronic resource such as an account and so on.

Not shown in Figure 2, the virtual terminal is then removed from Alice's device. In other words, the virtual terminal is commissioned on demand when a particular authentication session is initiated, and is decommissioned when it is concluded in success (step 11) or failure (step 10).

5

With particular reference to Figures 1 and 2, we now provide more detail relating to illustrative embodiments in use.

1.1 Scenario 1 – Online shopping

- 10 Consider a non-limiting example, in which a customer/user (Alice 201) has an electronic device (mobile phone) and wishes to use it to perform a transaction for the purchase of goods in a merchant (Bob's) online store 203. In other words, when Alice wants to make her purchases, she will have to make a 'card not present' transaction.
- 15 Alice 201 has a payment card 208 that has been issued by a third entity, Carole 204. Bob 202 has an account with David. David is an acquiring institution 205 such as a bank or a payments solution provider that Bob has chosen to use for payments via his web site. David has created an SDK (which we may also refer to as a 'terminal application', 'software component' or 'payment app') that Bob makes available to Alice via his web site so she can download the SDK to her phone 206, 207 as
- 20 described in more detail below. The SDK is operative to facilitate or perform a method in accordance with any embodiment of the present disclosed herein.

- When Alice has finished shopping on Bob's online store 203, she chooses the "go to checkout" option so that she can pay for the items in her basket. In a traditional, in-store scenario, Alice would
- 25 approach the payment desk where Bob's Point-of-Sale payment terminal (i.e. further electronic device) is located, and present her payment card. She would tap the card on the payment terminal for a contactless transaction or insert the card into the terminal and enter her PIN. In our online store scenario, however, Bob's payment terminal is not physically available to Alice. When she chooses the "pay now" option on Bob's web site, Alice opts to download and install the SDK in order
- 30 to perform the transaction directly from her phone. By installing and executing the app, Alice provides her consent to allow David 205 (via the SDK) to interact with Alice's mobile device remotely and temporarily as if the phone 206 was Bob's traditional payment terminal. In accordance with the disclosure, the security and functionality of Bob's physical merchant device is cloned on Alice's device instead in accordance with an embodiment of the present disclosure.

- The download and installation of the SDK on Alice's phone can be initiated in different ways, as explained above. In one example, Alice may be using her laptop to shop online via Bob's web site. When she proceeds to checkout and make the payment, she performs a triggering event which
- 5 causes the download, installation, configuration and execution of David's SDK to occur on her phone. This triggering event may be, for example, entering her phone number into an input field on the store's check out screen, or using her phone's camera to scan a QR code presented on the checkout screen of Bob's store or by receiving a push message or other signal/communication from Bob's device etc as explained above. The QR code may comprise instructions that initiate the
- 10 download and installation of the SDK on the phone. The SDK may be downloaded from a remote location controlled by David. In such cases, the device that Alice uses to initiate the transaction is not the same device that she uses to authenticate and pay with i.e. she is using her laptop to make selections in the online store but generating and performing the payment transaction on her mobile phone.
- 15
- In another example scenario, Alice may be shopping at Bob's online store on her phone and may simply click on a link provided on the checkout page instead of scanning a QR code from a separate device. In such cases, the purchase selection process (shopping) and the transaction process are performed on the same device.
- 20
- Whichever type of triggering event is used to initiate the SDK installation, by QR code, link click or menu option selection etc, the result is that a software application is downloaded and installed on Alice's phone. In other scenarios, Alice has already downloaded and installed Bob's app which contains the SDK and, therefore, the SDK has already been installed ready for execution.
- 25
- Upon execution, the SDK provides a blank merchant terminal on the phone. Instead of being referred to as a blank terminal, the alternative wordings 'virgin terminal', 'virtual terminal' or 'stateless terminal' could be used, and we use these terms interchangeably herein.
- 30
- The blank terminal that is generated on Alice's phone is blank in the sense that it may comprise at least some of the functionality of a traditional payment terminal but it is not configured or functional for use as a particular instance of a payment terminal. In other words, it comprises a shell of a payment terminal but has not been set up or initialised to serve as a terminal belonging to any

particular merchant. So at this point in the process, the blank terminal has been generated on Alice's phone, but it is not yet associated with Bob.

5 Data relating to the transaction is presented (visually and/or via audio means) on Alice's phone for her to check. If the data eg price does not match her expectation, or if she has simply changed her mind, she can abort the transaction. If, however, she agrees to proceed, she can authorise the payment to complete the transaction i.e. transfer of funds. In some cases, if the transaction amount is small enough, she might choose to make a contactless payment by simply tapping her payment card on the phone. The NFC reader built into the phone reads the data from the chip on Alice's
10 payment card, performs the usual transactions steps and completes the transaction. These traditional transaction steps can include contacting the issuing bank (Carole, 204) with the card, user and payment details, requesting payment, waiting for authorisation from the issuer (Carole), presenting confirmation of successful payment (or otherwise) to the user (Alice) on the phone's screen.

15

There is a need to secure the Alice's PIN entry and other sensitive data such as payment card details against unauthorised access by malicious actors. For example, such data needs to be protected in the event of the phone being compromised e.g. by a virus or malware on the phone. Therefore, in a preferred embodiment the SDK is installed, stored and/or executed in a secure enclave or security
20 hardened portion of the phone. This may be or comprise one or more of: a Secure Element (SE), a Trusted Execution Environment (TEE), Trusted Platform Module (TPM), Hardware Security Module (HSM), Software Guard Extensions (SGX), a Trusted User Interface (TUI).

In order to prevent security exploits such as 'man-in-the-middle' attacks, in which an unauthorised
25 third party intercepts the installation of the virtual terminal SDK on Alice's phone, an attestation platform is also installed as part of the SDK. This ensures that the SDK is being installed into a secure environment and also provides ongoing checks to ensure that the phone or installation process have not been compromised.

30 In other embodiments, the phone's built-in camera and biometric equipment can be utilised to further enhance security and reduce the risk of fraud or theft. In some embodiments, two-factor (2F) authentication can be utilised by taking an image of the face of the person making the transaction and holding the phone. Facial recognition can be used to check the face of the person holding the phone matches a stored picture of the legitimate user. Additionally, or alternatively, a

picture of the person holding the phone can be captured and stored for future reference so that it can be used as evidence in the event of a query or claim relating to the legitimacy of the transaction.

1.2 Scenario 2 – In-store shopping

- 5 In our next example scenario, Alice goes into Bob's physical store to make her purchase. Before she leaves the store, she uses the camera on her phone to capture a QR code that is displayed at the checkout or some other location in the store. In other examples, a link or code could be provided that Alice enters into her phone instead of capturing the QR code. The process then continues as for
- 10 scenario 1, in that the triggering event causes installation of the SDK on Alice's phone, a blank terminal is generated and that blank terminal is then configured so as to emulate the security and functionality of Bob's physical payment terminal. The user interface is provided as before, the PIN and any instructions are captured, and the payment is made upon successful verification of the user via PIN and/or other authentication methods such as biometrics, face recognition etc.
- 15 Consider a scenario in which Alice is doing her grocery shopping in a supermarket which provides self-checkout facilities. When Alice gets to the self service check out machine, she scans the items in her trolley via the machine's scanner, chooses "finish and pay" from the touch screen, and then selects "pay on my phone" option. As above in scenario 1, she scans the QR code and the terminal SDK is downloaded to Alice's phone. The scanning of the QR code forms or generates the
- 20 association between Alice's phone and the checkout machine. The terminal configuration and the payment processes are performed as explained above.

- In an alternative scenario, Alice might choose to use the 'scanning while shopping' approach instead of scanning everything at the end at the self serve checkout. In such an approach, Alice takes a hand
- 25 scanner upon entry to the store, scans each item as she moves through the shop, and then downloads the data from the scanner to the self serve check out machine when she is finished. Again, if she chooses the "pay on my phone" option she performs a triggering event to cause the SDK to be installed and the process performed as already described.

30 1.3 Scenario 3 – Shopping Via Merchant's App (in-store or mobile)

In the above scenarios, we describe examples in which Alice performs a triggering event for the download and installation of David's SDK on her phone. However, it may not always be necessary for Alice to re-install the SDK each time she chooses the "pay on my phone" route of payment.

For example, if David is Alice's bank or a PSP that she agrees to use, the SDK can be downloaded and installed on her phone and not removed or uninstalled after each payment is made. In some ways, this is analogous to Alice having a newly manufactured, blank terminal that always resides on her phone. The SDK is not restricted to use with just one merchant. Instead, it provides a general
5 purpose authentication tool that Alice can use to make card payments at different merchants' virtual or physical point of sales. When Alice chooses to check out, the terminal connects to David's platform and downloads all of the data files and keys for that particular merchant. When the transaction finishes, the SDK erases the data files so that it is blank and stateless again.

10 However, in other examples, a particular merchant may choose to embed David's SDK within their own mobile or online application. For example, suppose that Alice often shops at Bob's store online and wants the convenience of having Bob's desktop or mobile shopping application installed on her device. When using Bob's online store as per scenario 1 and she performs the triggering event to install the SDK, Alice can make an association between her phone and that particular retailer (Bob)
15 so that when she is shopping at his store again the payment transaction is sent automatically and directly to her phone. In this way, the SDK can be set as a 'default' payment method by the user for a given merchant. However, this is an optional feature.

Alternatively, if Alice is shopping via Bob's app on her mobile phone, and David's SDK is embedded in
20 Bob's shopping app to enable payments on the shopper's phone, Alice does not need to download and install David's SDK separately as it will be downloaded and installed automatically as part of the download and installation of Bob's app.

In other examples, instead of being embedded in a merchant app the SDK may be embedded in a
25 banking app, a payment app, an authentication app for controlling access to a vehicle, building or other controlled physical/digital resource.

Therefore, there are various in-use possibilities:

- 1) Removal of SDK after a single transaction
30 the SDK can be downloaded and installed upon performance of a triggering event by a user, and then uninstalled (either automatically or upon request/instruction by the user) once the payment has been concluded. The payment may be concluded upon successful completion of payment, or upon being rejected for some reason such as insufficient funds in the user's account, too many failed authentication attempts etc.

2) Ongoing residence of the SDK

as explained above, the SDK can be downloaded and installed on the user's phone as a generic payment method for use with different merchants, or as a built-in payment component of a third party's application. In such cases, the SDK may reside on Alice's phone until she deletes David's standalone SDK from her device or deletes Bob's app which contains it.

Preferably, embodiments of the system disclosed herein are certified under the relevant payment industry standard, such as PCI CPoC, SPoC, MPoC for example. In a preferred implementation, the system may comprise one, some or all of the following components:

- a mobile point of sale application (the mobile application)
- an attestation and monitoring system
- a backend transaction processing system
- attestation and kernel configurations specifically attuned to manage the risk of a cardholder operated transaction.

It is envisaged that embodiments of the system will be provided by the parties such as acquirers, payment service providers, payment aggregators, and so on.

20 2. In Use example #2 – Access Control

In the first use case example, we described how embodiments of the disclosure can be used to provide an on-demand authentication platform for payment-related transactions and transfers. However, embodiments can also be used to advantage in other scenarios and for other purposes and are not limited to use in respect of payment transactions. In fact, embodiments can be deployed by any party that issues smart cards or other processing devices that are enabled with NFC capabilities and PIN functionalities. For example, consider a scenario in which a data owner's stores sensitive data on its computing resources. In this case the data owner might be the 'issuer' of an access card. When an operative or other user wishes to access the data, they must verify their identity by using the card that has been issued to them. Using an embodiment of the disclosure, the user can do this by tapping their card on a reader and/or entering a PIN associated with them. In some cases, the reader could be the user's mobile phone or tablet, which then uses the inputted data from the card to perform the verification process. If successful, the user is granted access to certain files or resources e.g. they may be able to access files etc from their laptop/tablet.

In yet other examples, a driver may download a car manufacturer's app to their phone, the app comprising the SDK as described above. When wishing to unlock the car, the driver may use the app to generate a new virtual terminal as described above. The virtual terminal is configured with the necessary security data eg keys and the drive is able to control the car securely from the phone e.g. unlock the doors.

ENUMERATED CLAUSES FOR ILLUSTRATIVE EMBODIMENTS

- For the purposes of illustration, and without limitation, we now provide some enumerated clauses and alternative wordings to illustrate some of the embodiments disclosed herein. The clause sets below are not intended to be limiting in respect of how features disclosed herein may be combined. Any feature recited in respect of one clause or clause set is not intended to be limited to use in that respect, and may be combined with any other feature(s) from one or more other clauses or clause sets.
- 15 In accordance with one or more embodiments as disclosed herein, the disclosure may provide a computer-implemented method. The disclosure provides corresponding (computer-implemented) systems arranged to perform the steps of any method disclosed herein. The method/system may be described as one or more of:
- A security method/system;
 - 20 • A verification method;
 - A method/system for simulating, generating, recreating, replicating or emulating at least part of the state of a further device on a user's device, wherein the at least part of the state of the further device is specified, required, influenced or otherwise provided by a remote computing resource;
 - 25 • A method of controlling access to a controlled resource;
 - A method of performing, controlling, authenticating, completing and/or processing an electronic transaction or transfer including, but not limited to, an electronic payment or transfer of digital assets.
- 30 Embodiments of the present disclosure provide improved solutions for performing secure transfers of data, and can be used to advantage in any situation wherein:
- where sensitive data needs to be shared securely between at least two participants across an electronic network; and/or

- the identity and authorisation of a would-be accessor needs to be verified prior to granting access to the controlled resource(s) (which may include the sensitive data).

Herein, we may describe example embodiments of the disclosure in the context of making a
5 financial transaction. However, this example is chosen purely for illustrative purposes and because such a use case is well known and readily understood. The disclosure is not limited in this regard and embodiments are as equally well suited for use in other contexts and for other purposes.

While the invention is not limited to such use cases, in situations where an embodiment is
10 implemented within a payments system, the terms 'on-us transaction', 'in-house payment/transaction' or 'on-us check' refers to a payment that is issued and received by the same financial instruction. In other words, the transfer comprises the transfer of an asset between users that belong to or are associated with the same entity. For example, a cheque or electronic transfer initiated from an account held at Bank A, and presented for payment into another account that is
15 also held at Bank A, would be an "on-us" transaction. In such situations, the issuing party can send the payment directly to the acquiring party with no involvement from the clearing networks e.g. the Visa or MasterCard networks. The payment is simply re-routed internally to the receiving account.

On-us transactions can provide the technical benefit of faster processing times because they do not
20 need to go through an inter-bank system. Additionally, as on-us transactions can avoid the need to go to an external network to obtain authorization or funds for the exchange, this can result in significant reductions in energy and processing resources. Further still, an on-us transaction is more secure because the risk of security breaches, exploits or unauthorised interception is greatly reduced. Therefore, on-us transactions provide a more efficient and secure means of conducting
25 exchanges and transfers across electronic networks.

By contrast, when the acquirer and issuer are separate entities, the transaction may be referred to as a 'not-on-us item' or a 'transit check'. Such transactions require the involvement of external networks for transit and clearing of the payment enroute to the acquirer.
30 Thus, there are many situations, both within the payments industries and other application areas where secure access to controlled resource(s) is required, and in which sensitive data needs to be exchanged between sending and receiving parties that do not belong to the same organisation. As a result, the parties involved may lack trust. Technical challenges arise as to how to establish identity, ensure secure communication, storage and processing of sensitive data even on an

insecure end-user device, and how to perform data exchanges across networks in a way that ensures that only authorised parties are able to access sensitive data and other controlled resources. The technical challenges may also comprise how to use a generic, off-the-shelf electronic device to perform secure electronic transfers (i.e. transactions) between different parties
5 that each have/are associated with their own security configuration data, and/or may be associated with different transfer facilitating entities e.g. acquirers.

Clause Set 1:

Any feature or clause in clause set 1 can be combined with or incorporated into any other
10 embodiment or clause set provided herein. An example embodiment of the disclosure may provide:

Clause 1.1a:

A method comprising the step of emulating or providing (at least part of) the state and/or functionality of at least one further electronic device (e.g. a particular merchant's payment terminal)
15 on/to a user's electronic device.

The 'state' or 'estate' may comprise configuration data such as configuration files, encryption data and/or cryptographic keys, and/or machine executable logic code. The at least one further device may be a physical or virtual device.

20 Clause 1.1b:

A method of using a user's electronic device to perform an electronic transfer between the user and second user, the second user being associated with configuration data. The method may comprise the step of providing the second user's configuration data to the user's electronic device to enable the simulation of a further electronic device on the user's electronic device. The further electronic
25 device may be a computing device arranged to perform secure electronic transactions with other parties on behalf of the second user. The configuration data may comprise data such as configuration files, encryption data and/or cryptographic keys, and/or machine executable logic code/instructions that is arranged such that it enables the user's electronic device to emulate/simulate/replicate/clone (at least part of) the state of the further electronic device (e.g. a
30 particular merchant's payment terminal) on the user's electronic device.

Clause 1.1c:

A method comprising the step of:

generating, or enabling or facilitating the generation of, the functionality of at least one further device on a (first) user's electronic device. The further device may be a physical or virtual device. Additionally, or alternatively, the at least one further device may be associated with a second user. The second user may comprise a person, computing resource or an organisation. The at least one

5 further device may comprise a security device arranged to perform the transfer of at least one electronic asset between the first user and at least one other party, which may comprise the second user. The step of generating, or enabling or facilitating the generation of, the functionality of the at least one further device on the (first) user's electronic device may comprise provision, installation, use or execution of configuration data to/on the user's electronic device, wherein the configuration

10 is associated with the second user. The configuration data may be assigned to/associated with the second user by a third user/party/entity. The at least one further device may be or comprise a security device or terminal such as, for example, a payment terminal and/or authentication device.

Preferably, one, some or all of the following options may apply to any of the options for clause 1.1.:

15 i) the user's electronic device comprises a mobile, portable, handheld and/or commercial-off-the-shelf (COTS) device

ii) the further electronic device comprises hardware and/or software arranged to perform a transfer of data with one or more other (computing) devices; the further device may comprise a payment terminal;

20 iii) the further device is arranged for communication with at least one remote resource;

iv) the further device may be provided to a second user e.g. merchant by or on behalf of a controlling (third) entity;

iii) the state comprises at least one cryptographic key;

iv) the state of the further electronic device is dictated, determined by, influenced by, or

25 otherwise provided by a remote/third resource; the third resource may be a computing-based resource/system/device that is provided by, operated by or used by a controlling entity; the controlling entity may be a bank, financial institution or payments-related organisation; for example, an acquiring bank, a credit card provider, a payments services provider etc; additionally, or alternatively, the controlling entity may be the

30 controller of a physical or electronic resource.

In one example form of wording, 'emulation of the state' may comprise, but is not limited to:

- providing or enabling the same, or substantially the same, functionality or behaviour as the further electronic device; the functionality may comprise machine executable

instructions that can be stored in a computer's memory and executed by one or more processors; and/or

- configuration data required by or expected of the further device eg cryptographic keys, merchant/user identifier etc.

5

Clause set 2:

Any feature or clause in clause set 2 can be combined with or incorporated into any other embodiment or clause set provided herein. Additionally, or alternatively, an example embodiment of the disclosure may provide:

10 Clause 2.1. A computer-implemented method comprising the step:

emulating or providing the state of a security device on a user's electronic device (206, 207), wherein:

- i) the user's electronic device; and/or
- ii) the security device arranged to:

- 15
- Control access to a controlled resource; and/or
 - Conduct a transfer (e.g. a financial transaction or other electronic transfer such as the transfer of files, data or communications etc) between a first party and a second party.
- 'Emulating' may comprise 'duplicating', 'copying', 'simulating' or extending'.

20 The first party may be a sender (transferor) and the second party may be a receiver (transferee), or any other party authorised on their respective behalfs.

Preferably, the user's electronic device comprises a mobile and/or commercial-off-the-shelf (COTS) device.

In some examples, the controlled resource may be a physical resource such as a vehicle, building,

25 secure payment terminal/card reader, IoT device such as a smart television etc, or may be a virtual resource such as a bank account, network account, digital wallet, virtual payment terminal etc.

The security device may correspond to the 'further electronic device' recited in clause set 3.

30 Clause 2.2: the method of clause 2.1, wherein:

the step of emulating or providing the state of the security device on the user's electronic device comprises sending configuration data to the user's electronic device to facilitate the generation of an emulation of security device on the user's electronic device.

The configuration data may comprise encryption data, cryptographic key(s), identifiers, machine executable instructions and other data.

The emulation/provision may provide or enable the generation of a new, fresh instance of an emulation of the security device. It may be generated in a secure or protected storage/processing

5 portion of the user's electronic device. The generation of the emulation may be performed in response to a triggering event or condition, such as the receipt of an instruction.

The emulation may be generated by a software component (e.g. 'app' or 'SDK' installed or executing on the user's electronic device.

10 Clause set 3:

Any feature or clause in clause set 3 can be combined with or incorporated into any other embodiment or clause set provided herein. Additionally, or alternatively, an example embodiment of the disclosure may provide:

15 Clause 3.1. A computer-implemented method comprising the step:

Emulating or providing the state of a further electronic device on a user's electronic device (206, 207), wherein:

i) the user's electronic device comprises a mobile and/or commercial-off-the-shelf (COTS) device; and/or

20 ii) the further electronic device is a payment terminal.

In some embodiments, the payment terminal may comprise hardware and software substantially as known in the technical field of payment solutions devices, such as (for example) described at:

https://en.wikipedia.org/wiki/Payment_terminal.

25

Clause 3.2. A method according to clause 3.1 wherein:

the step of emulating the state of the further electronic device on the user's electronic device is performed by a software component installed and/or executed on the user's electronic device.

30

Clause 3.3. A method according to clause 3.1 or 3.2, and further comprising the step:

i) providing, to the user's electronic device, a software component arranged to emulate the state of the further electronic device on the user's electronic device; and/or

- ii) installing and/or executing, on the user's device, a software component arranged to emulate the state of the further electronic device on the user's electronic device.

Clause 3.4. A method according to clauses 3.2 or 3.3, wherein the software component is arranged
5 to obtain authentication data to facilitate authentication of the user's identity and/or the user's authorisation of an electronic transaction.

Clause 3.5. A method according to clause 3.4, wherein the authentication data comprises one or more of:

- 10 a Personal Identification Number (PIN);
a password, code or other identifier;
audio or voice related data;
biometric data;
payment card data;
15 at least one cryptographic key.

In some embodiments, the at least one cryptographic key may be provided in a digital wallet; and/or in a device such as a tag, fob, wearable device, physical token, chip or processing component embedded in a card or host device, or any other suitable device arranged to comprise cryptographic
20 key(s).

Clause 3.6. A method according to claim 3.4 or 3.5, wherein the authentication data is obtained via at least one hardware and/or software component provided on, in or in association with the user's electronic device.

25

Clause 3.7. A method according to clause 3.6, wherein the at least one hardware and/or software component provided on, in or in association with the user's electronic device comprises one or more of:

- 30 a touch screen; a physical or virtual keypad or keyboard; a microphone; a camera; a Near Field Communication (NFC) reader or device; a short-range wireless component; a point-to-point component; a smart card reader; a magnetic strip reader; a fingerprint or iris scanner.

Clause 3.8. A method according to any preceding clause, and further comprising the step of: obtaining, by the user's electronic device:

- i) transaction data relating to an (potential) electronic transaction between a sending resource (204) and a receiving resource (205); and
 - ii) authentication data;
- and

5 using the transaction data and the authentication data to facilitate the electronic transfer.

The electronic transfer may be a potential transfer in that its successful performance may be contingent upon certain criteria being met such as successful verification of the user's identify and authorisation of the transfer.

10

The authentication data may comprise the authentication data mentioned in previous clauses or elsewhere herein.

The sending resource may be associated with the user e.g. the user's issuing bank. The receiving resource may be associated with an owner, operator or controller of the further electronic device

15 such as a merchant, e.g. a merchant's acquiring bank or a payment solutions provider.

Clause 3.9. A method according to any preceding clause wherein the state of the further electronic device comprises:

- i) identification means for uniquely identifying the further electronic device; and/or
- 20 ii) one or more cryptographic keys.

Clause 3.10. A method according to any preceding clause, wherein:

the step of emulating or providing the state of the further electronic device on the user's electronic device is performed upon demand or in response to a trigger event.

25

Clause 3.11. A method according to any preceding clause, wherein:

the state of the further electronic device is emulated temporarily on the user's electronic device.

30 Clause 3.12. A method according to any preceding clause, wherein the state of the further device is:

- i) provided, specified or determined by a remote resource; and/or
- ii) provided, at least in part, to the further device by the remote resource;

Clause 3.13. A method according to any preceding clause, wherein:

the step of emulating the state of the further electronic device on the user's electronic device comprises:

installing configuration data on the user's electronic device.

- 5 Clause 3.14. A method according to any preceding clause, the method further comprising:
removing the emulated/provided state from the user's electronic device;
preferably wherein the state is removed after completion of an operation involving
interaction with a remote processing resource.

- 10 Clause 3.15. A method of performing an electronic transfer between a first party (204) associated
with the user (201) of an electronic device (206, 207) and a second party (205) associated
with merchant (202), the merchant being associated with a payment terminal, comprising
the steps:
i) sending or otherwise providing, from the second party to the user's electronic device:
15 configuration data to generate an emulation of the payment terminal on the user's
electronic device; and data relating to the electronic transfer;
and
ii) using the emulation of the payment terminal to send, from the user's electronic device
to the second party or a party authorised on the behalf of the second party, authorisation
20 data indicating the user's authorisation of the electronic transfer.

Clause set 4:

Any feature or clause in clause set 4 can be combined with or incorporated into any other
embodiment or clause set provided herein. Additionally, or alternatively, an example embodiment
25 of the disclosure may provide:

Clause 4.1. A computer-implemented method comprising the step:

providing at least one software component arranged for one or more of: transmission to,
download by, installation on and/or execution on a user's electronic device,

30 wherein:

- i) the at least one software component is operative to emulate the state and/or
functionality of a security device on the user's electronic device; and
ii) the security device is arranged to:
control access to a controlled resource; and/or

facilitate a transfer (e.g. a financial transaction or other electronic transfer such as the transfer of files or communications etc) between a first party and a second party.

- 5 The method step(s) of any preceding clause set or features disclosed herein may be combined with clause set 4.1.

Additionally, an embodiment of the disclosure may provide computer equipment comprising:

- memory comprising one or more memory units; and
- 10 processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of clause or clause set described herein.
- 15 Additionally, an embodiment of the disclosure may provide a computer program embodied on computer-readable storage and configured so as, when run on one or more processors, to perform the method of any of any clause or clause set described herein.

TERMINOLOGY

- 20 The following terms may be used herein, without limitation, to comprise at least the following meanings:
- Controlling entity:
any entity that has the authority to grant or deny access to a controlled resource; this may, for example, be a resource owner, a system administrator, a data controller, a vehicle or
25 building owner/occupier, an account operator or provider etc.; the controlling entity may comprise at least one human individual, at least one computing resource comprising hardware and/or software, or a combination thereof;
 - Controlled resource:
may comprise any type of physical, virtual or digital resource that a controlling entity wish
30 to keep secure such that access to the resource is only granted to entities that are authorised to do so by the controlling entity; for example, the controlled resource may comprise one or more of: an electronic device such as a mobile phone or laptop, a financial or other account, or a vehicle/building, or a computer network/file system or part thereof etc., sensitive data

- Sensitive data:
sensitive data may comprise any data that a controlling entity wishes or needs to keep secret and unshared, except with entities that are permitted to have access; sensitive data may be described as a 'controlled resource'; it may also be used to secure a further controlled resource such as an electronic device, account, vehicle/building, network etc.; for example, sensitive data may comprise a password, identifier, cryptographic key etc
- User: May comprise at least one human individual, at least one computing resource comprising hardware and/or software, or a combination thereof;
- Authentication: may be used interchangeably with 'validation' and/or 'verification' and comprises a method of checking the identity and/or authorisation of a user that is seeking, requesting or attempting to gain access to a controlled resource
- Install/uninstall: 'install' may be used interchangeably with 'activate', 'set up', 'provide for execution' or 'provide'; correspondingly, the term 'uninstall' may be used interchangeably with 'deactivate', 'disable', 'prevent execution of', 'destroy', 'delete', 'erase' or 'remove';
- Device: the term 'device' should not be constructed as only meaning a single, standalone piece of apparatus; in many cases, a 'device' may comprise a plurality of hardware, software and/or firmware components, and may be implemented as a distributed resource. The term 'resource' may be used interchangeably with 'system' and 'device'.
- Electronic device: The phrase 'electronic device' can be used interchangeably herein with 'computing device' or 'processing device'. The electronic device may comprise hardware and/or firmware arranged to store data and/or execute instructions.
- Obtain: can be constructed as covering any term that results in possessing, such as, but not limited to, receiving (from a sending party), calculating, generating or determining.
- Transaction: The term transaction is used herein to comprise one, some or all of 'transfer', 'interaction' or 'exchange', and is not to be construed as being limited to financially oriented transactions.

ILLUSTRATIVE COMPUTING ENVIRONMENT FOR IMPLEMENTATION OF EMBODIMENTS

We now refer to Figure 3, which illustrates an example device 2500, with a processor 2502 and memory 2504 that can be configured to implement part or all of an embodiment of the methods and processes disclosed in the present application. The skilled person will readily appreciate that many other forms and arrangements of hardware, software and/or firmware can be used for this purpose, and that Figure 3 and the present section of the description is just an illustration of many possible variations. Memory 2504 can also host one or more databases and can include one or more forms of

volatile data storage media such as random-access memory (RAM), and/or one or more forms of nonvolatile storage media (such as read-only memory (ROM), flash memory, and so forth).

Device 2500 is one example of a computing device or programmable device and is not intended to suggest any limitation as to scope of use or functionality of device 2500 and/or its possible architectures. For example, device 2500 can comprise one or more computing devices, programmable logic controllers (PLCs), etc.

Further, device 2500 should not be interpreted as having any dependency relating to one or a combination of components illustrated in device 2500. For example, device 2500 may include one or more of computers, such as a laptop computer, a desktop computer, a mainframe computer, etc., or any combination or accumulation thereof. Device 2500 can also include a bus 2508 configured to allow various components and devices, such as processors 2502, memory 2504, and local data storage 2510, among other components, to communicate with each other.

Bus 2508 can include one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. Bus 2508 can also include wired and/or wireless buses. Local data storage 2510 can include fixed media (e.g., RAM, ROM, a fixed hard drive, etc.) as well as removable media (e.g., a flash memory drive, a removable hard drive, optical disks, magnetic disks, and so forth). One or more input/output (I/O) device(s) 2512 may also communicate via a user interface (UI) controller 2514, which may connect with I/O device(s) 2512 either directly or through bus 2508.

In one possible implementation, a network interface 2516 may communicate outside of device 2500 via a connected network. A media drive/interface 2518 can accept removable tangible media 2520, such as flash drives, optical disks, removable hard drives, software products, etc. In one possible implementation, logic, computing instructions, and/or software programs comprising elements of module 2506 may reside on removable media 2520 readable by media drive/interface 2518.

In one possible embodiment, input/output device(s) 2512 can allow a user (such as a human annotator) to enter commands and information to device 2500, and also allow information to be presented to the user and/or other components or devices. Examples of input device(s) 2512 include, for example, sensors, a keyboard, a cursor control device (e.g., a mouse), a microphone, a scanner, and any other input devices known in the art. Examples of output devices include a display device (e.g., a monitor or projector), speakers, a printer, a network card, and so on.

Various systems and processes of present disclosure may be described herein in the general context of software or program modules, or the techniques and modules may be implemented in pure computing hardware. Software generally includes routines, programs, objects, components, data structures, and so forth that perform particular tasks or implement particular abstract data types.

5 An implementation of these modules and techniques may be stored on or transmitted across some form of tangible computer-readable media. Computer-readable media can be any available data storage medium or media that is tangible and can be accessed by a computing device. Computer readable media may thus comprise computer storage media. "Computer storage media" designates

10 tangible media, and includes volatile and non-volatile, removable, and non-removable tangible media implemented for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer storage media include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other

15 magnetic storage devices, or any other tangible medium which can be used to store the desired information, and which can be accessed by a computer. Some of the methods and processes described above, can be performed by one or more processors. The term "processor" should not be construed to limit the embodiments disclosed herein to any particular device type or system. The processor may include or form part of a computer system. Multiple processors may be used, and

20 these may be running in parallel. The computer system may also include at least one computer processor (e.g., a microprocessor, microcontroller, digital signal processor, general-purpose computer, special-purpose machine, virtual machine, software container, and/or appliance) for executing any of the methods and processes described above. The system may be or comprise a decentralized, peer-to-peer or distributed computing architecture.

25 The computer system may further include a memory such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed disk), an optical memory device (e.g., a CD-ROM), a PC card (e.g., PCMCIA card), or other memory device.

30 Alternatively, or additionally, the processor(s) may include discrete electronic components coupled to a printed circuit board, integrated circuitry (e.g., Application Specific Integrated Circuits (ASIC)), and/or programmable logic devices (e.g., a Field Programmable Gate Arrays (FPGA)). Any of the methods and processes described above can be implemented using such logic devices.

Some of the methods and processes described above, can be implemented as computer program logic for use with the computer processor. The computer program logic may be embodied in various forms, including a source code form or a computer executable form. Source code may include a series of computer program instructions in a variety of programming languages (e.g., an object code, 5 an assembly language, or a high-level language such as C, C++, or JAVA). Such computer instructions can be stored in a non-transitory computer readable medium (e.g., memory) and executed by the computer processor. The computer instructions may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed 10 from a server or electronic bulletin board over a communication system (e.g., the Internet or World Wide Web).

Although only a few example embodiments have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the example embodiments without materially departing from this invention. Accordingly, all such modifications are intended to 15 be included within the scope of this disclosure as defined in the following claims. In the claims, means-plus-function clauses are intended to cover the structures described herein as performing the recited function and not only structural equivalents, but also equivalent structures.

CONCLUDING REMARKS

20 The above-mentioned embodiments are provided for illustration purposes, and not intended to be limiting. The person skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the claims appended herein. Herein: the word "comprising" and "comprises", and the like, can be synonymous with "includes" and does not exclude the presence of features other than those recited in any claim or disclosed in the 25 specification as a whole; "comprises" is intended to mean "includes or consists of" and "comprising" is intended to mean "including or consisting of". The singular reference of an element does not exclude the plural reference of such elements and vice-versa. Embodiments of the disclosure may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device or system claim enumerating several means, several of these 30 means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS:

1. A computer-implemented method comprising the step:
emulating or providing the state of a further electronic device on a user's electronic device
5 (206, 207), wherein:
i) the user's electronic device comprises a mobile and/or commercial-off-the-shelf (COTS)
device; and/or
ii) the further electronic device is a payment terminal.
- 10 2. A method according to claim 1 wherein:
the step of emulating or providing the state of the further electronic device on the user's
electronic device is performed by a software component installed and/or executed on the
user's electronic device.
- 15 3. A method according to claim 1 or 2, and further comprising the step:
i) providing, to the user's electronic device, a software component arranged to emulate the
state of the further electronic device on the user's electronic device; and/or
ii) installing and/or executing, on the user's device, a software component arranged to
emulate or provide the state of the further electronic device on the user's electronic
20 device.
4. A method according to claims 2 or 3, wherein the software component is arranged to obtain
authentication data to facilitate authentication of the user's identity and/or the user's
authorisation of an electronic transaction.
- 25 5. A method according to claim 4, wherein the authentication data comprises one or more of:
a Personal Identification Number (PIN);
a password, code, one time password or other identifier;
at least one memorable word or phrase; an answer to at least one security question;
30 audio or voice related data; biometric data;
payment card data; at least one cryptographic key.

6. A method according to claim 4 or 5, wherein the authentication data is obtained via at least one hardware and/or software component provided on, in or in association with the user's electronic device.
- 5 7. A method according to claim 6, wherein the at least one hardware and/or software component provided on, in or in association with the user's electronic device comprises one or more of: a touch screen; a physical or virtual keypad or keyboard; a microphone; a camera; a Near Field Communication (NFC) reader or device; a short-range wireless component; a point-to-point component; a smart card reader; a magnetic strip reader; a fingerprint or iris scanner.
- 10
8. A method according to any preceding claim, and further comprising the step of: obtaining, by the user's electronic device:
- 15 i) transaction data relating to an electronic transaction between a sending resource (204) and a receiving resource (205);
- ii) authentication data;
- and using the transaction data and the authentication data to facilitate the electronic transfer.
9. A method according to any preceding claim wherein the state of the further electronic device
- 20 comprises one or more of:
- i) identification means for uniquely identifying the further electronic device;
- ii) one or more cryptographic keys;
- iii) one or a plurality of machine executable instructions.
- 25 10. A method according to any preceding claim, wherein:
- the step of emulating or providing the state of the further electronic device on the user's electronic device is performed upon demand and/or in response to a trigger event.
11. A method according to any preceding claim, wherein:
- 30 the state of the further electronic device is emulated or provided temporarily on the user's electronic device.
12. A method according to any preceding claim, wherein the state of the further device is:
- i) provided, specified or determined by a remote resource; and/or

ii) provided, at least in part, to the further device by the remote resource;

13. A method according to any preceding claim, wherein:

the step of emulating or providing the state of the further electronic device on the user's

5 electronic device comprises:

installing configuration data on the user's electronic device.

14. A method according to any preceding claim, the method further comprising:

removing the emulated or provided state from the user's electronic device;

10 optionally wherein the state is removed after completion of an operation involving
interaction with a remote processing resource.

15 15. A method of performing an electronic transfer between a first party (204) associated with the
user (201) of an electronic device (206, 207) and a second party (205) associated with
merchant (202), the merchant being associated with a payment terminal, comprising the
steps:

i) sending, from the second party to the user's electronic device:

configuration data to generate an emulation of the payment terminal on the user's
electronic device; and data relating to the electronic transfer;

20 and

ii) using the emulation of the payment terminal to send, from the user's electronic device
to the second party or a party authorised on the behalf of the second party, authorisation
data indicating the user's authorisation of the electronic transfer.

25 16. A computer-implemented method comprising the step:

providing at least one software component arranged for one or more of: transmission to,
download by, installation on and/or execution on a user's electronic device;

wherein:

30 i) the software component is operative to emulate the state and/or functionality of a
security device on the user's electronic device; and

ii) the security device is arranged to:
control access to a controlled resource; and/or
facilitate a transfer between a first party and a second party.

17. Computer equipment comprising:
- memory comprising one or more memory units; and
- processing apparatus comprising one or more processing units, wherein the memory stores
- code arranged to run on the processing apparatus, the code being configured so as when
- 5 on the processing apparatus to perform the method of any of claims 1 to 16.
18. A computer program embodied on computer-readable storage and configured so as, when run
- on one or more processors, to perform the method of any of claims 1 to 16.