(12) UK Patent Application (19) GB (11) 2517732 (13) A

(43) Date of A Publication 04.03.2015

(21) Application No: 1315420.8

(22) Date of Filing: 29.08.2013

(71) Applicant(s):
Sim & Pin Limited
1st Floor, 2 Woodberry Grove, Finchley, London, N12 0DR, United Kingdom

(72) Inventor(s):
Christopher Iain Johnston
Michel Leduc

(74) Agent and/or Address for Service:
Dehns
St. Bride's House, 10 Salisbury Square, LONDON, EC4Y 8JD, United Kingdom

(51) INT CL:
G06F 21/62 (2013.01) ***G06F 21/34*** (2013.01)

(56) Documents Cited:
WO 2013/124689 A2
CN 102761870 A
US 20120054845 A1
US 20110078762 A1
KR 20130085472
WO 2011/150968 A1
US 8438654 A1
US 20110099616 A1
US 20090183010 A1

(58) Field of Search:
INT CL **G06F, H04L**
Other: **WPI, EPODOC, TXTE**

(54) Title of the Invention: **System for accessing data from multiple devices**
Abstract Title: **Method and system for accessing data from multiple devices**

(57) A method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, comprises: sending a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; verifying, based at least partly on the identification code, whether access to the data is to be allowed or denied; and allowing or denying the device access to the data accordingly. The data may be stored in a cloud computer system. The request to access data may also include a passcode or PIN or genetic or biometric information inherent to the user. The secure element or memory card may be a SIM, SE, TEE, micro SD, USB key or a smartcard. The entered PIN may be passed to the device SIM where the PIN is passed through an encryption algorithm which hashes the PIN with the SIM identification. Other inventions relate to providing to a user an invitation to access data with a verifiable code, registering a device with an access controller and allowing access to data only if at least one other device is already accessing the data.

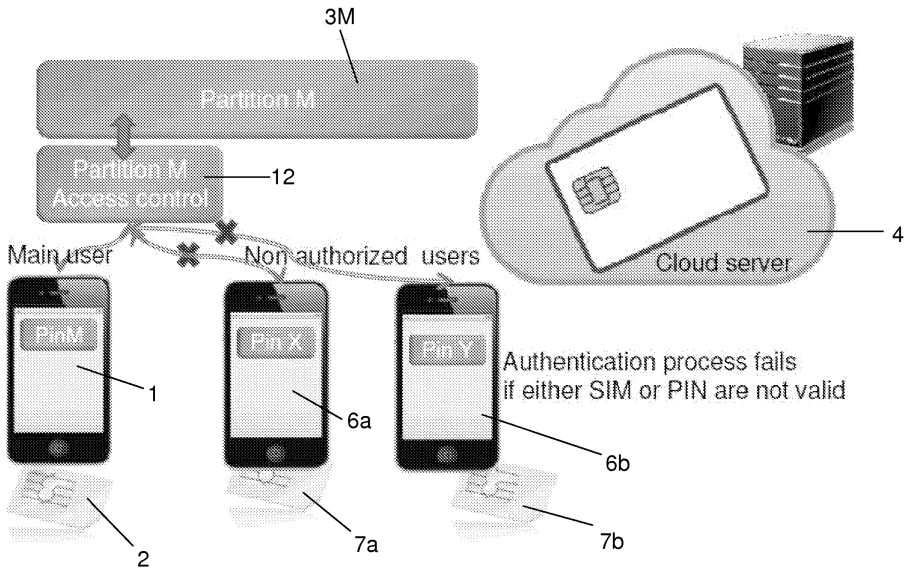

Fig. 3

GB 2517732 A

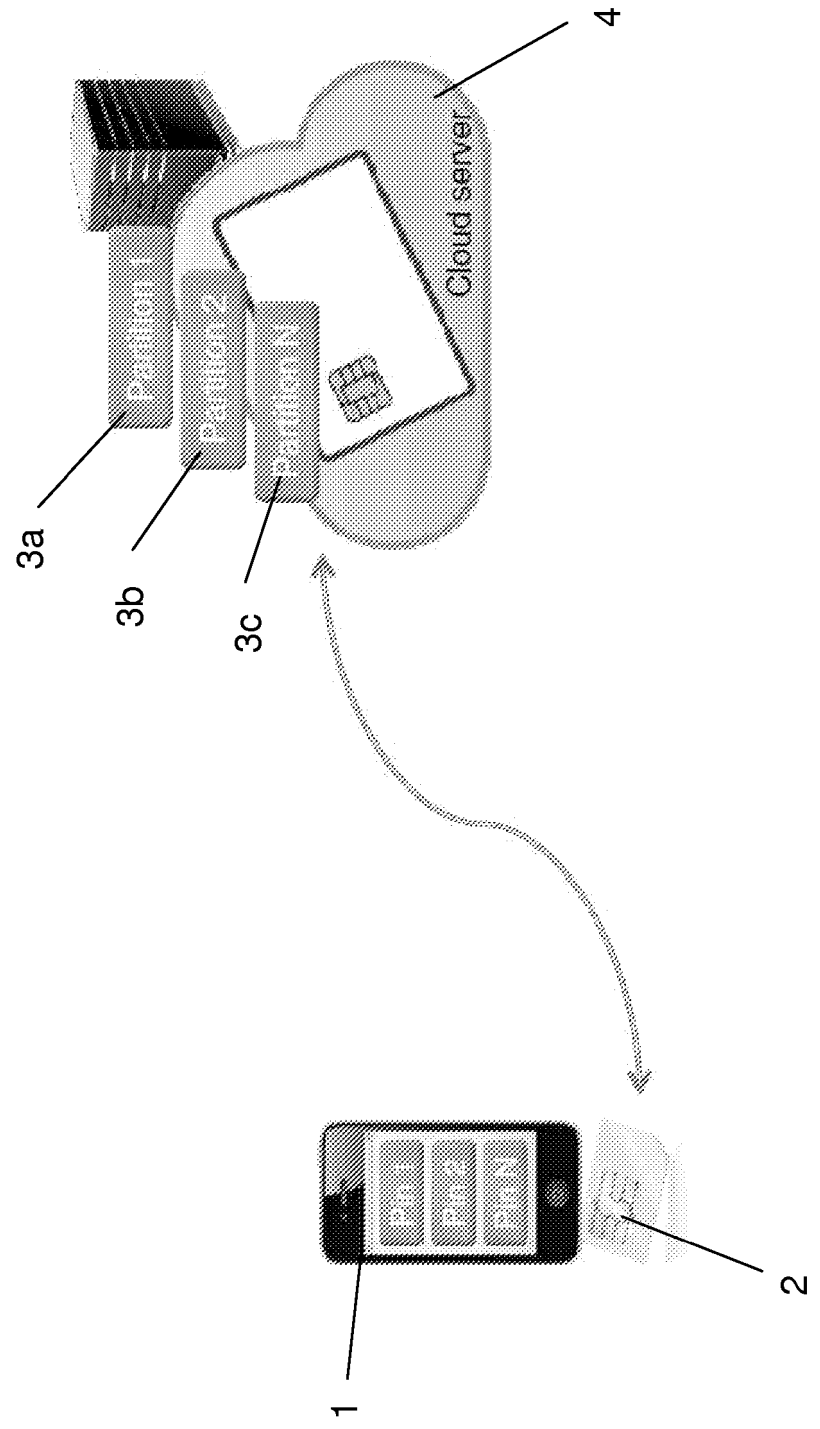
4
Cloud server
3a
3b
3c
Partition 1
Partition 2
Partition N
1
2

Fig. 1

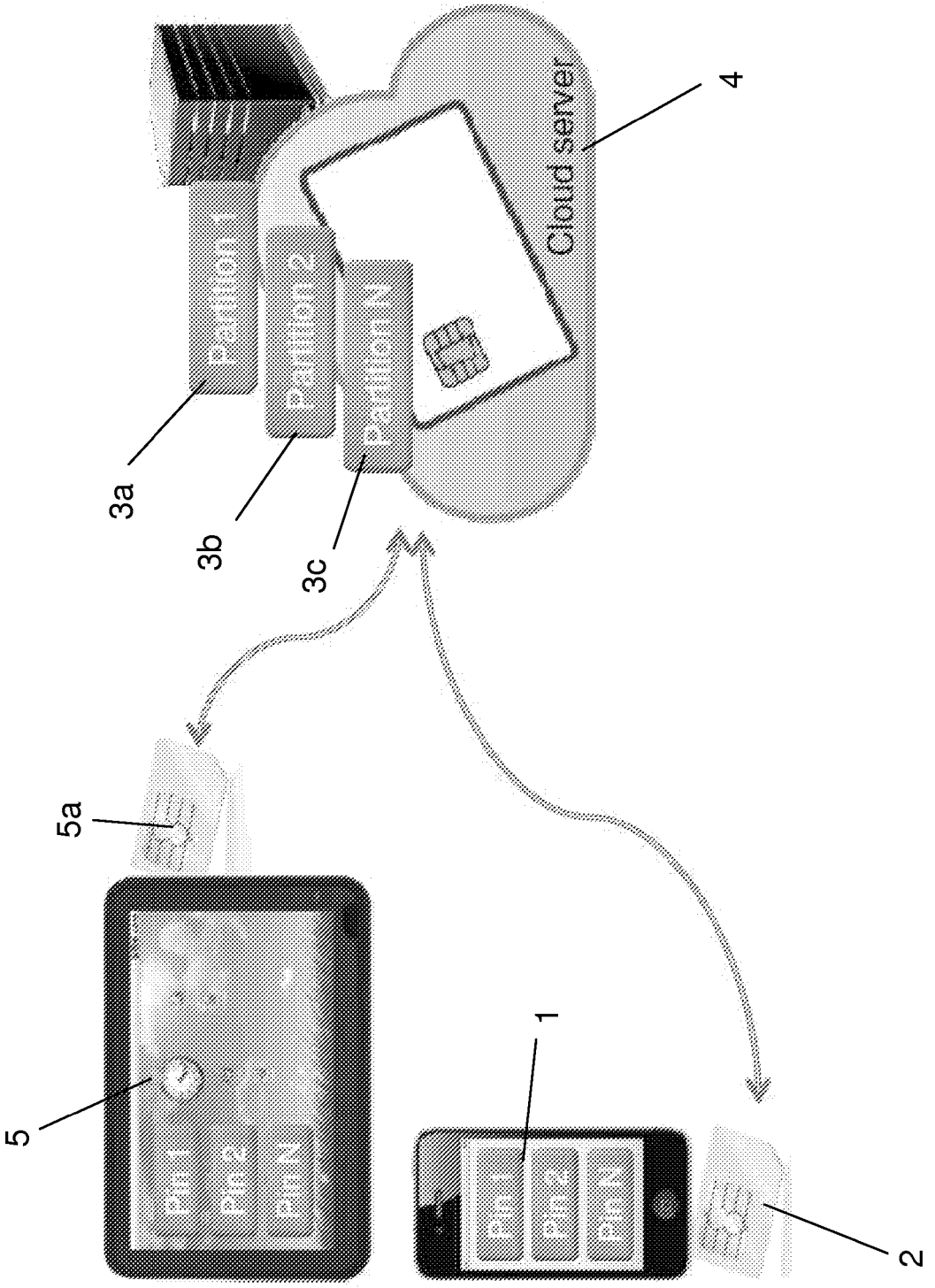
Partition 1
Partition 2
Partition N
Cloud server
4
3a
3b
3c
5a
5
1
2
Pin 1
Pin 2
Pin N

Fig. 2

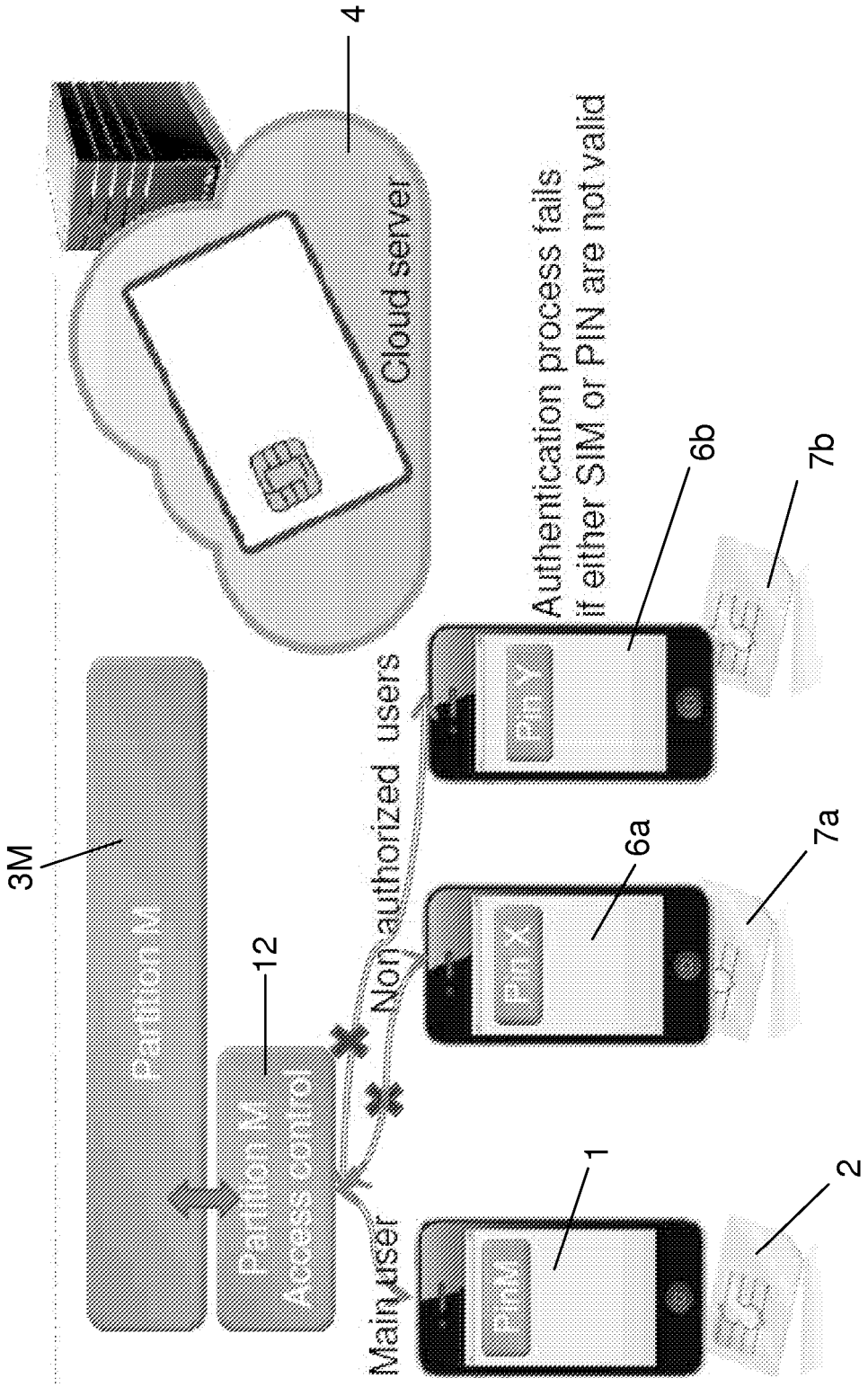
3M
Partition M
12
Partition M
Access control
Main user
Non authorized users
PIN
PIN X
Authentication process fails
if either SIM or PIN are not valid
Cloud server
4
1
2
6a
7a
6b
7b

Fig. 3

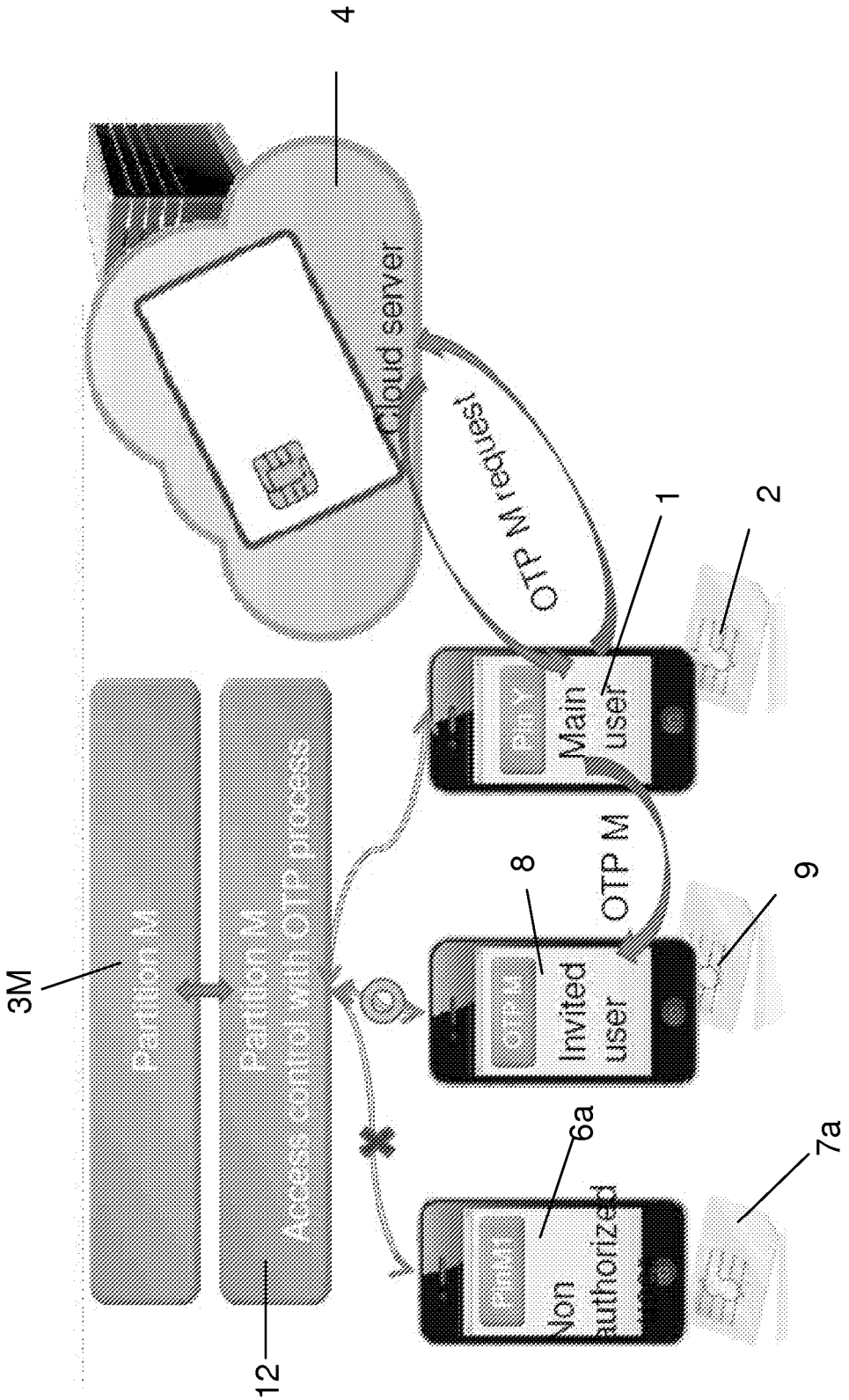
4
Cloud server
OTP Request
1
2
Main user
PIN Y
OTP M
8
9
Invited user
OTP M
6a
7a
Non authorized
PIN Y
3M
Partition M
Partition M
Access control with OTP process
12

Fig. 4

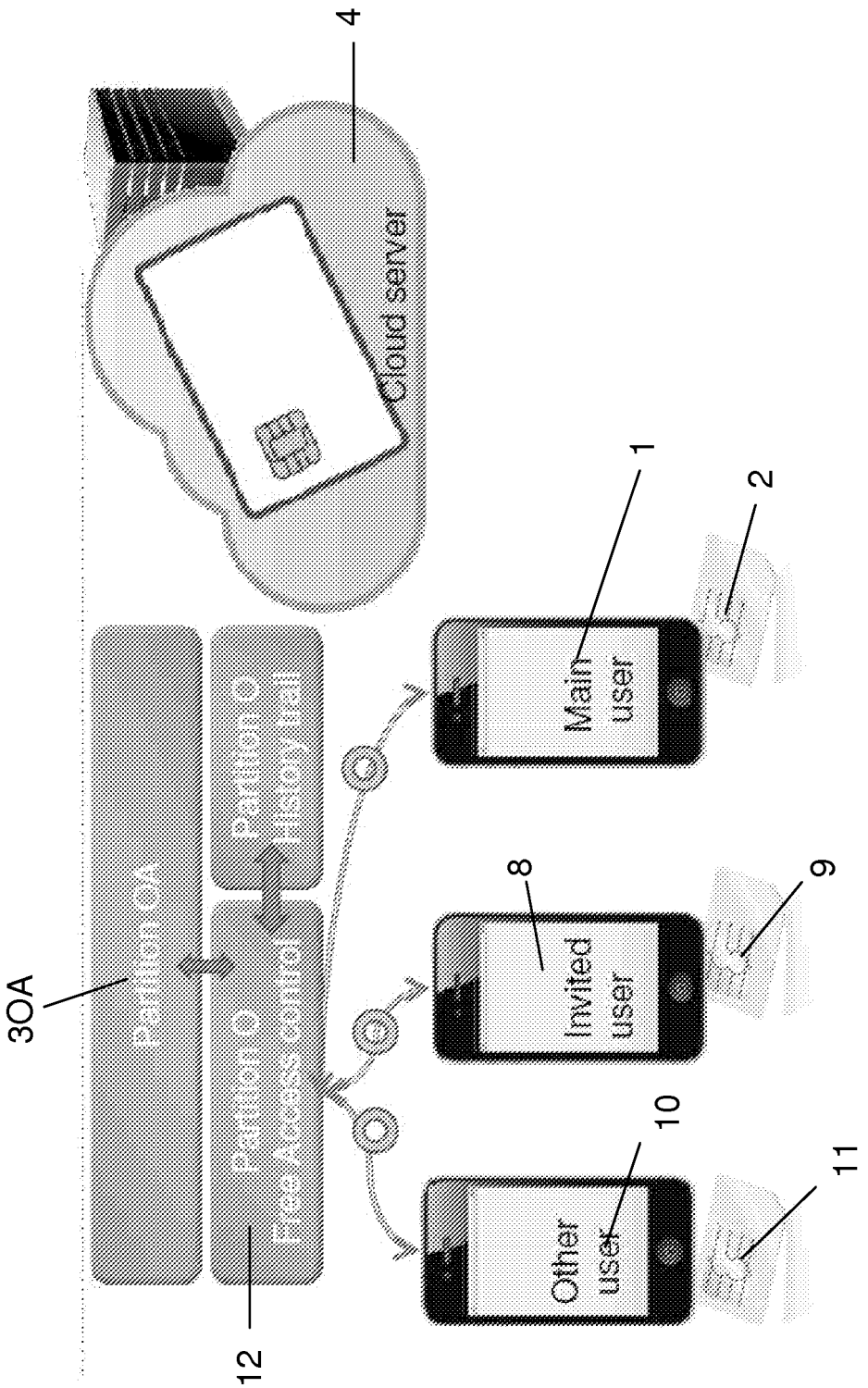
4
Cloud server
1
Main user
2
3OA
Partition A
Partition B
History trail
Partition C
Free Access control
12
8
Invited user
9
10
Other user
11

Fig. 5

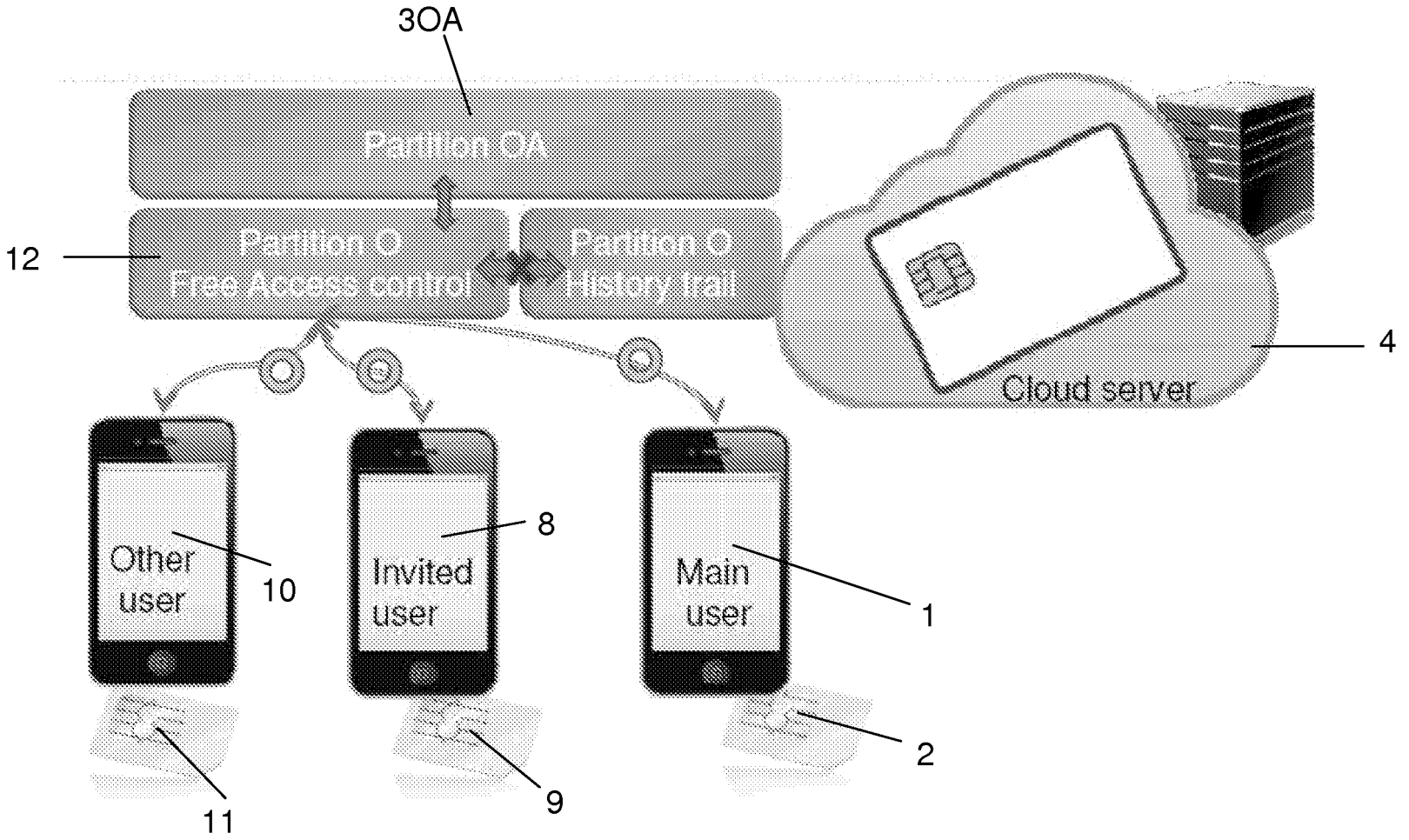
3OA
Partition OA
12
Partition O
Free Access control
Partition O
History trail
4
Cloud server
Other
user
10
Invited
user
8
Main
user
1
11
9
2

Fig. 6

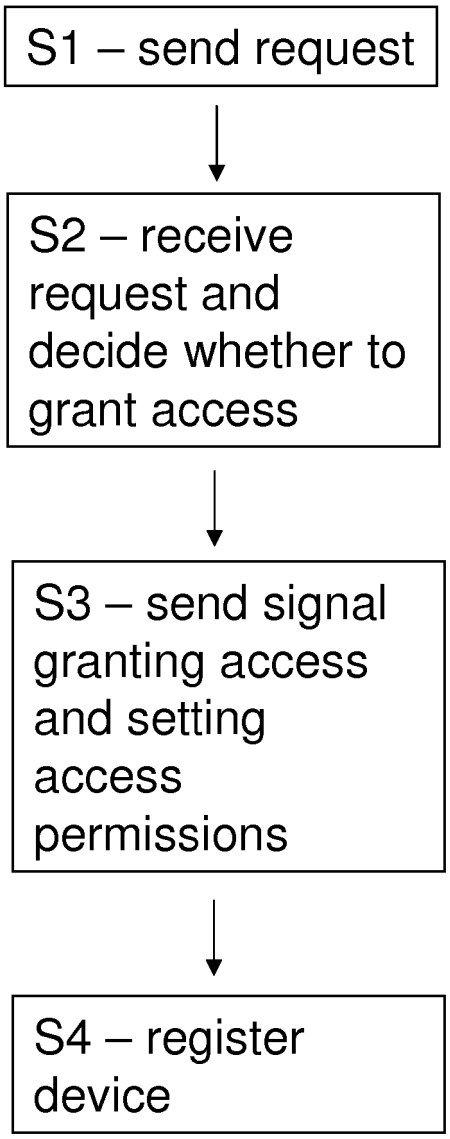
S1 – send request
S2 – receive request and decide whether to grant access
S3 – send signal granting access and setting access permissions
S4 – register device

Fig. 7

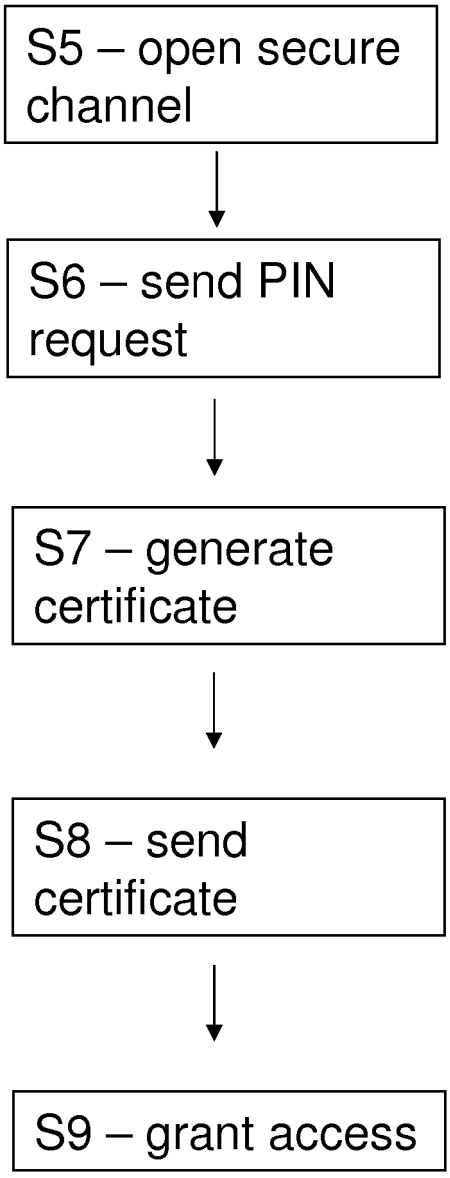
S5 – open secure channel
S6 – send PIN request
S7 – generate certificate
S8 – send certificate
S9 – grant access

Fig. 8

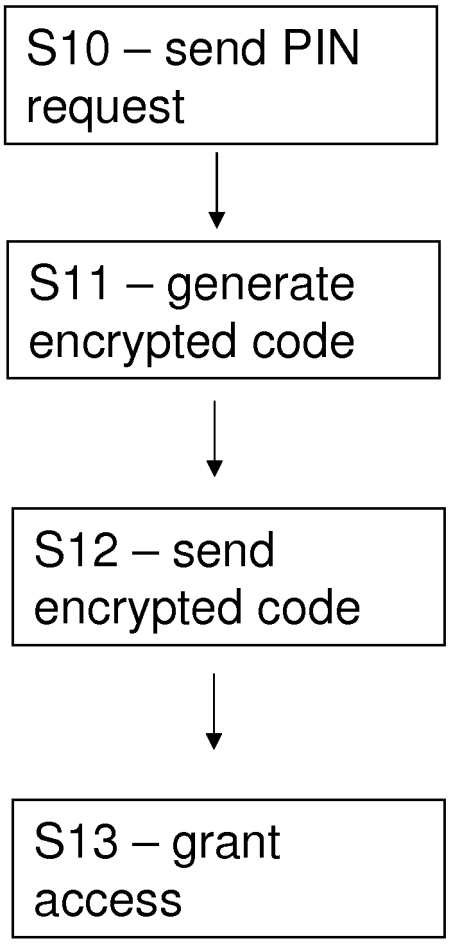
S10 – send PIN request
S11 – generate encrypted code
S12 – send encrypted code
S13 – grant access

Fig. 9

System for accessing data from multiple devices

The present invention relates to the field of data access. More specifically, it relates to a system for accessing data from multiple devices.

It is known in the art to provide a user with cloud-based data storage. This cloud-based storage may be accessed from multiple devices.

For example, Dropbox™ is a system which provides users with cloud-based remote storage for their data. The data may comprise photographs taken with a mobile telephone, for example. Once the data has been uploaded from the mobile telephone, for example, to the remote storage, it may then be accessed from other devices which are connected to the Internet, such as a laptop or desktop computer. The stored data is encrypted with 256-bit AES encryption and a user must enter their registered e-mail address and password via a website before access to their data is granted.

However, one problem with this system is that if a user's email address and password is discovered by a third party then that third party may also access the stored data from any device. Thus, there is a need for a more secure remote storage system which may be accessed from one or multiple devices.

According to a first aspect of the invention, there is provided a method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps: (i) sending a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; (ii) verifying, based at least partly on the identification code, whether access to the data is to be allowed or denied; and (iii) allowing or denying the device access to the data accordingly.

Access to the data is thus only allowed if a correct identification code associated with the device is provided. Thus, it is possible to prevent unauthorised devices from accessing the data since they will not be able to provide a correct identification code.

As stated above, the request includes an identification code of a secure element or memory card associated with the device. However, the identification code may be included in the request in a modified form, for example, in an encrypted form and/or combined with one or more further codes, data or information.

The data to be accessed includes any form of data which can be stored in memory. For example, it may comprise one or more data files, databases, applications, software, and/or services. Some examples of services are discussed below.

Preferably, the identification code is sent via a secure channel. Alternatively or additionally, the identification code may be encrypted. This can make the process more secure and help to prevent the identification code being intercepted and/or discovered by a third party.

A further (additional or alternative) possibility would be to generate a code at the device based on the identification code of the secure element or memory card and one or more other elements or codes from the device. This generated code could then be sent and may, for example, only be valid for a particular session. Thus, even if it were intercepted it would be of no use to a third party.

The data may be stored in a removable storage device, the cloud or other forms of remote data storage. For example, the data could be stored in a USB key, a laptop, a computer server (personal or corporate), a computer network (personal or corporate), a tablet or telephone.

The request may also include a passcode or PIN entered at the device and step (ii) may also comprise verifying based on the passcode or PIN whether access to the data is to be allowed or denied. Thus, two-factor authentication may be required in order to access the data.

The passcode or PIN may be (first) verified by the secure element or memory card associated with the device (e.g. a SIM).

Alternatively (or additionally), the passcode or PIN may be verified remotely from the device, for example at an access controller which is arranged to control access to the data.

In the case that the passcode or PIN is verified by the secure element or memory card, the result of this verification is preferably transferred to, for example, an access controller in a secure and/or protected manner, e.g. via a secure channel. For example, the result could be transferred in the form of a certificate, an encrypted code, a session code or an encrypted session code. Preferably, the result of the verification is only transferred if the verification was successful, i.e. if the correct passcode or PIN were entered.

In the case that the passcode or PIN is verified remotely from the device, for example at an access controller, it is preferred that the passcode or PIN is

transferred, e.g. to the access controller, in a secure and/or protected manner. For example, the passcode or PIN could be transferred via a secure channel and/or by encrypting the passcode or PIN before transfer.

Alternatively or additionally, the request may include data representing something inherent to a user of the device, and step (ii) may also comprise verifying based on the data representing something inherent to the user of the device whether access to the data is to be allowed or denied. Thus, two- or three-factor authentication may be required in order to access the data and only authorised users may be granted access to the data.

The data representing something inherent to the user of the device may comprise data representing genetic and/or biometric information about the user such as a fingerprint or iris data, for example.

The secure element or memory card is, for example, a "smart object" or a secure or tamper-proof hardware device with a unique identification code, which itself is also ideally secure and tamper-proof. The secure element or memory card could, for example, be a SIM, SE (secure element), TEE (trusted execution environment), Micro SD, Memory card, USB key or Smartcard.

The identification code of the secure element or memory card is preferably well-protected and stored, for example, in a safe box in the secure element or memory card.

In preferred embodiments of the invention, the secure element or memory card is used to create a secure channel and/or to encrypt the identification code and/or the PIN or passcode.

The data may be stored in a partition, e.g. a memory partition, associated with the device, and the request may comprise data specifying the partition, e.g. the partition to be accessed.

The data specifying the partition could comprise one or more of: a PIN or passcode; and data representing something inherent to the user of the device. The data representing something inherent to the user of the device could comprise data representing genetic and/or biometric information about the user, for example.

The device may be or comprise a telephone (mobile or fixed), a smartphone, a tablet, a laptop computer, a desktop computer, a TV, a set top box, a camera, a car, a games consol, glasses, a watch, Chromecast, a smart meter (e.g. for measuring electricity, gas or water consumption at a building), jewellery, a travel card, a bank cards, an ATM machine, clothing, sports equipment, an E-reader,

binoculars, an MP3 player, a hand-held gaming consol, a vehicle such as a plane, a train, a bike, a boat or a bus, an EPO, a kitchen appliance, a mirror, a handbag, a wallet, a hat, a pram, a Hi-fi or other music player or radio, or any other device which is, or has means associated with it which is, capable of sending and receiving data to remote or removable devices.

The device, or preferably the secure element or memory card, preferably has data access software code installed on it for accessing the data. Preferably, in order to install the data access software code, the device must register with the system for example by submitting information related to at least an identification code of the secure element or memory card.

The method preferably comprises, prior to steps (i)-(iii): registering an identification code of a secure element or memory card, or a code or certificate based on this, with the data.

Identification codes of more than one secure element or memory card may be associated with the data. Thus, it can be possible for more than one device to be registered with the data and access the data securely.

A master device may register or request the registration of the identification codes associated with further devices, for example.

As discussed above, the identification codes are preferably an identification codes associated with smart object of the devices. The smart object may be a SIM, SE (secure element), TEE (trusted execution environment), Micro SD, Memory card, USB or Smartcard associated with the device, for example. Different smart objects could be used to provide the identification codes for different devices.

In some cases, a device may only be allowed to access the data if at least one further device is also accessing the data. In some cases, the at least one further device may have to be a particular specified device, such as an administrator device.

According to a further aspect, there is provided a method of controlling access to data from a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps: (i) receiving a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; (ii) verifying, based at least partly on the identification code, whether access to the data is to be allowed or denied; and (iii) allowing or denying the device access to the data accordingly.

This aspect may comprise any of the additional or optional features of the first aspect described above.

Preferably, the method of this aspect is performed by a data access controller. The data access controller may be remote from the device which wishes to access the data. For example, the data access controller may be in the cloud.

According to a further aspect, there is provided a data access controller for controlling access to data stored remotely from a device or in removable storage, the data access controller being arranged to perform the following steps: (i) receive a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; (ii) verify, based at least partly on the identification code, whether access to the data is to be allowed or denied; and (iii) allow or deny the device access to the data accordingly.

The data access controller may be remote from the device which wishes to access the data. For example, the data access controller may be in the cloud.

According to a further aspect, there is provided a system comprising a device and a data access controller for controlling access from the device to data stored remotely from the device or in removable storage, wherein the device is arranged to send a request to access the data to the data access controller, the request including an identification code of a secure element or memory card associated with the device; and the data access controller is arranged to verify, based at least partly on the identification code, whether access to the data is to be allowed or denied, and to allow or deny the device access to the data accordingly.

According to a further aspect, there is provided a computer program for controlling access to data stored remotely from a device or in removable storage, the program being configured to perform the following steps when executed by a processor: (i) receive a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; (ii) verify, based at least partly on the identification code, whether access to the data is to be allowed or denied; and (iii) allow or deny the device access to the data accordingly.

According to a further aspect, there is provided a method of registering a device with an access controller such that the device may access data via the access controller, the data being stored remotely from a device or in removable storage, wherein the method comprises: sending a request to register a device for access to data, the request including an identification code of a secure element or

memory card associated with the device; checking whether access to the data is to be allowed; and if access is to be allowed, registering the identification code against the data to be accessed.

The request preferably includes a two or three factor code based on, for example, the identification code of a secure element or memory card associated with the device and one or more of a PIN or passcode, and data representing something inherent to the user. This allows for an auditable trail of which devices have requested access to a partition.

The request may be in the form of an email or SMS.

The method preferably further comprises sending information related to the request to an administrator device, wherein the administrator device preferably decides whether or not access to the data is to be granted. The information related to the request may be sent from an access controller or the device which is seeking registration, for example. The administrator device may be used to set access permissions for the device requesting access, such as read only or the ability to edit/delete/add additional content to the data.

For example, in the case where the secure element or memory card of a child's device (e.g. a phone or tablet) is registered such that it can access a parent's data, the secure element or memory card of a parent's device (e.g. a phone or tablet) could be registered as the administrator for that data so that it can monitor and control the child's access to the data. The data itself could actually be stored in the parent's administrator device. Thus, a device (or multiple devices) may (each) allow one or more further devices to access data stored in that device but with limited or specified read/right permission, for example.

Preferably, if the administrator decides to allow the device to have access to the data, a signal is sent from the administrator to the access controller indicating this.

According to a further aspect, there is provided a method of registering a device with an access controller such that the device may access data via the access controller, the data being stored remotely from a device or in removable storage, wherein the method comprises: receiving a request to register a device for access to data, the request including an identification code of a secure element or memory card associated with the device; checking whether access to the data is to be allowed; and if access is to be allowed, registering the identification code against the data to be accessed.

According to a further aspect, there is provided a data access controller for controlling registration of devices with access to data, the controller being arranged to perform the following steps: receive a request to register a device for access to data, the request including an identification code of a secure element or memory card associated with the device; check whether access to the data is to be allowed; and if access is to be allowed, register the identification code against the data to be accessed.

According to a further aspect there is provided a system comprising a device and a data access controller for controlling registration of devices with access to data, the controller being arranged to perform the following steps: receive from the device a request to register the device for access to data, the request including an identification code of a secure element or memory card associated with the device; check whether access to the data is to be allowed; and if access is to be allowed, register the identification code against the data to be accessed.

The system preferably further comprises an administrator device.

The data access controller is preferably arranged to send a signal to the administrator device to check whether access to the data is to be allowed for the device to be registered.

The administrator device is preferably arranged to send a signal confirming whether access to the data is to be allowed for the device to be registered and/or setting access permissions for the device requesting access, such as read only or the ability to edit/delete/add additional content to the data.

According to a further aspect, there is provided a computer program for controlling registration of devices with access to data, the program being configured to perform the following steps when executed by a processor: receive from the device a request to register the device for access to data, the request including an identification code of a secure element or memory card associated with the device; check whether access to the data is to be allowed; and if access is to be allowed, register the identification code against the data to be accessed.

According to a further aspect, there is provided a method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising: receiving at the device an invitation to access the data, the invitation comprising a password, code or PIN; sending a request from the device to access the data, the request including the password, code or PIN; verifying, based at least partly on the password, code or PIN, whether access to the

data is to be allowed or denied; and allowing or denying the device access to the data accordingly.

Thus, it is possible for a user to send invitations to further devices (his own or those or another user) so that further devices may also access data. These devices (or an identification code associated therewith) need not necessarily be registered with the data in order to be granted access.

According to this aspect, access may be granted to the device for an unlimited time or for a predetermined length or time. In either case, access may be prevented, for example by another user, at some point after access has been granted.

The password, code or PIN may be generated by a random number generator, for example.

The password, code or PIN is preferably a one-time-password. This can provide a secure method of granting access to further users.

Preferably, the password, code or PIN is only valid for a specified period of time. Thus, if it is not used within the specified period, access will not be granted based on that password, code or PIN. The period may be up to 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 20, 25, 30, 45, 60, 90 or 120 minutes, for example. The period is preferably 24 hours or less. On the other hand, in some embodiments, the password, code or PIN may not have a particular expiry time.

Preferably, the password, code or PIN, at least, is sent to and/or from (preferably to and from) the device via a secure channel.

In some embodiments, the password, code or PIN is generated by a device controlling access to the data, such as a master device

The method may be a method of a first device allowing a second device to access data, wherein the data is stored remotely from the first and second devices, the invitation being sent from the first device to the second device, the request to access the data being sent from the second device and access to the data is allowed or denied to the second device.

In this case, the password, code or PIN may be generated in the first device.

Alternatively, the password, code or PIN may be generated remotely from both the first and second devices, for example at a processor controlling access to the data.

In either case, the method preferably further comprises registering the generated password, code or PIN with the data to be accessed.

The step of registering the generated password, code or PIN with the data to be accessed may comprise verifying that the first device is allowed to invite further devices to access the data before registering the generated password, code or PIN.

The method may further comprise sending a request from the first device for the password, code or PIN to be generated, wherein the password, code or PIN to be generated is only generated after it has been verified that the first device is allowed to invite further devices to access the data.

Thus, in either case, only authorised devices may invite further devices to access the data.

The step of verifying that the first device is allowed to invite further devices to access the data preferably comprises verifying an identification code associated with the device, such as an identification code of a secure element or memory card associated with the device as described above.

The step of verifying that the first device is allowed to invite further devices to access the data further may comprise verifying data specifying the partition sent from the first device.

The data specifying the partition preferably comprises one or more of: - a PIN or passcode; and - data representing something inherent to the user of the device such as genetic and/or biometric information.

According to a further aspect, there is provided a method of allowing access to data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising: sending to the device an invitation to access the data, the invitation comprising a password, code or PIN; sending a request from the device to access the data, the request including the password, code or PIN; verifying, based at least partly on the password, code or PIN, whether access to the data is to be allowed or denied; and allowing or denying the device access to the data accordingly.

The invitation may be sent from an administrator device, preferably via an access controller. The invitation may be in the form a message such as an email or SMS message and/or it could be sent and viewable via a messaging system within a data access application. When the invited user opens or logs into this application, they may see that an invitation has been received to access certain data. The user may then access the data.

The invitation may include a OTP (one-time-password), for example a OTP which the user may enter in a web browser in order to access the data via the web browser (e.g. as opposed to via the data access application)

According to a further aspect, there is provided a system comprising a first device, a second device and a data access controller, the first device being arranged to allow access to data at the second device, wherein the data is stored remotely from the second device or in removable storage, wherein the first device is arranged to send to the second device an invitation to access the data, the invitation comprising a password, code or PIN; the second device is arranged to send a request to access the data, the request including the password, code or PIN; and the data access controller is arranged to verify, based at least partly on the password, code or PIN, whether access to the data is to be allowed or denied, and to allow or deny the second device access to the data accordingly.

According to a further aspect, there is provided a method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps: (i) sending a request from the device to access the data, the request including data related to the request; (ii) verifying, based at least partly on the data, whether access to the data is to be allowed or denied; and (iii) allowing the device access to the data accordingly and only if there is at least one further device accessing the data.

Such a method can provide a secure environment in which certain actions, such as financial transactions, messaging and/or viewing (e.g. confidential) data, may be performed only when a further device is present. The further device (e.g. an administrator device) could then monitor any actions performed by the device. Prompt action, such as blocking or preventing further access to the data could then be taken, if appropriate.

The method preferably comprises, prior to step (iii), checking whether at least one further device is accessing the data. The at least one further device may be a particular specified device, such as a "master" device, for example.

According to a further aspect, there is provided a method of controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps: (i) receiving a request from the device to access the data, the request including data related to the request; (ii) verifying, based at least partly on the data, whether access to the data

is to be allowed or denied; and (iii) allowing the device access to the data accordingly and only if there is at least one further device accessing the data.

According to a further aspect, there is provided a data access controller for controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the data access controller being arranged to perform the following steps: (i) receive a request from the device to access the data, the request including data related to the request; (ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and (iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

The data access controller is also preferably arranged to check whether at least one further device is accessing the data prior to performing step (iii).

According to a further aspect, there is provided a system comprising a device and a data access for controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the data access controller being arranged to perform the following steps: (i) receive a request from the device to access the data, the request including data related to the request; (ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and (iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

Preferably, the device is arranged to send the request to access the data to the data access controller.

The data access controller is also preferably arranged to check whether at least one further device is accessing the data prior to performing step (iii).

According to a further aspect, there is provided a computer program for controlling access to data stored remotely from a device or in removable storage, the program being configured to perform the following steps when executed by a processor: (i) receive a request from the device to access the data, the request including data related to the request; (ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and (iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

The program is also preferably configured to check whether at least one further device is accessing the data prior to performing step (iii).

A further aspect of the invention relates to a method of accessing data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the method comprising the following steps: (i) sending a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information; (ii) verifying, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and (iii) allowing or denying the device access to the data accordingly.

The data is preferably stored in a partition. In this case, the PIN or passcode, and/or the data representing something inherent to the user of the device such as genetic and/or biometric information, is associated with the partition which the user is seeking to access. For example, the PIN or passcode, and/or the data representing something inherent to the user of the device such as genetic and/or biometric information may identify the data or partition where the data is stored.

In the case of genetic and/or biometric information, one option could be that finger prints from different fingers are associated with different data or partitions so that, depending on which finger print is entered and sent, the corresponding data or partition is accessed.

A further aspect of the invention relates to a method of controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the method comprising the following steps: (i) receiving a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information; (ii) verifying, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and (iii) allowing or denying the device access to the data accordingly.

A further aspect of the invention relates to a data access controller for controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the data access controller being arranged to perform the following steps: (i) receive a request to access the data, the

request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information; (ii) verify, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and (iii) allow or deny the device access to the data accordingly.

A further aspect of the invention relates to a computer program for controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the program being configured to perform the following steps when executed by a processor: (i) receive a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information; (ii) verify, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and (iii) allow or deny the device access to the data accordingly.

Aspects of the invention may comprise any of the features, including preferred or optional features, of any of the other aspects of the invention.

In any aspect, the data is preferably encrypted. Preferably, the data is decrypted by the device accessing the data. In this case, the device preferably has a key for decrypting the data. The key is preferably stored in a secure element or memory card but may be stored remotely. Preferably the key itself is encrypted. The key is preferably transferred to the device in a secure manner, for example by a TSM (trusted service manager).

From the above, it can be appreciated the embodiments of the invention may provide methods and systems in which:

- multiple devices can have partition access
- users can share securely with other users (devices) whilst maintaining control and audit trails
- transactions can be performed securely.

Multiple devices may access the same remote partition.

Upon accessing data or a partition(s), the device may be able to access one or more of the following services: messaging, media, TV, films, radio, magazines, social media, E-commerce, smart devices (e.g. utilities and home control), corporate services, pictures, photos and video sharing, government services,

financial services, medical services, travel services, music and games. Of course, there may also be further services not mentioned here, which could also or alternatively be accessed.

The devices may be able to offer a two or three factor authentication in order to access the partitions. The devices may be secured with one factor of the authentication being an identification code of smart object (a memory card or secure element) and a further factor or factors being either a passcode or PIN, or some form of genetic or biometric identification data.

The following table lists example devices from which a user may wish to access a partition and their possible corresponding "smart objects" (i.e. secure element or memory card). The smart object is the object of the device whose identification code is associated with a partition and which must be verified in order to access to the partition to be allowed.

Device	**Smart object**
Telephone	SIM, SE, TEE, Micro SD, Memory card, NFC smart object (for a NFC smartphone)
Tablet	SIM, SE, TEE, Micro SD, Memory card
Laptop	SIM, SE, TEE, Micro SD, Memory card, USB key , Smartcard
Desktop	SIM, SE, TEE, Micro SD, Memory card, USB key , Smartcard
TV	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Set Top Box	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Camera	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Car	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Games Consol	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Glasses	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Watch	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Chromecast	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard
Smart meter (home utilities)	SIM, SE, TEE, Micro SD, Memory card, USB key, Smartcard

Different types of partition may be provided such as:

- closed partitions to which only the user has access to
- closed partitions which can be shared with other users by invitation only

- open partitions which have audited history trails

- open and anonymous partitions which have no history or audit trails of users

Any kind of partition may be toggled to be open or closed based on criteria such as time slots. For example, a partition could be set to be open at a particular predefined time and closed at a particular predefined time.

Users may register multiple devices against partitions and may toggle, edit and upload functionality against the additional devices they register. For example, a user may wish their camera to have the ability to upload pictures to a partition and view pictures within partitions but not have the ability to delete or edit any content within the partition.

A user may elect to make one or multiple devices as the administrator device(s) of a partition. This could allow the administrator to control access to the partitions and stop access if they deem it necessary. The user could also, in an administrator capacity, have access to all other users' devices that have been granted access to the partitions for which the user is administrator. This could allow the user, in real time, to edit or remove access permissions to the partitions. It could also allow the user to bar access to devices if he loses or no longer owns a device.

The administrator device may have the ability to create a preferably time sensitive code which may be user toggled and which may give him access to log onto a machine which is not connected to a registered smart object. This code could be any length and/or could be inputted into an interface which is connected to access controller and access to partitions could be allowed on non-registered devices such as desktops or laptops. The user could have the ability to halt this session at any point from the administrator device, for example by initiating a halt button on the administrator device. The code which is created is preferably as a result of a two or three factor authentication with the administrator device.

The smart objects may manage multiple partitions which may have the same or different passcodes/authenticators attached to them. Within partitions the system may allow the user to sign up to or automatically sign up to many different third party services. Within the partitions the system may turn the user ID and password set by the user into an alphanumeric string for both password and user ID. This could be passed to the third party service provider. These codes may be renewed based on best practice guidelines for the service. For example they could

be renewed every 60 days if the user is accessing medical records in the UK in line with NHS Information Governance requirements.

Partitions may also be subject to multiple smart object locks. For example, a partition may only be opened when two or more different users are logged into the partition. This is particularly relevant when it comes to the sharing of documents in a corporate landscape or undertaking confidential meetings. The use of multiple smart object to open a partition could also be used to secure the identity of a third party when allowing services such as transaction with third party vendor or more informal transactions such as peer to peer transactions needing a secure environment.

Preferred embodiments of the invention will now be described by way of example only and with reference to the figures, in which:

Fig. 1 is a schematic diagram of a system comprising a mobile telephone and its corresponding cloud-based remote storage;

Fig. 2 is a schematic diagram of a system comprising a mobile telephone and a tablet device and their corresponding cloud-based remote storage;

Fig. 3 is a schematic diagram illustrating authorised and non-authorised access attempts to remotely stored data from mobile telephones;

Fig. 4 is a schematic diagram illustrating authorised, invited and non-authorised access attempts to remotely stored data from mobile telephones;

Fig. 5 is a schematic diagram illustrating authorised, invited and non-authorised access attempts to remotely stored data from mobile telephones with access monitoring;

Fig. 6 is a schematic diagram illustrating authorised, invited and non-authorised access attempts to remotely stored data from mobile telephones without access monitoring;

Fig. 7 is a flow diagram illustrating the process for registering a device so that it can access a partition;

Fig. 8 is a flow diagram illustrating an authentication process; and

Fig. 9 is a flow diagram illustrating an access code encryption process.

As shown in Fig. 1, a mobile telephone 1 comprises a SIM 2 and has access to data-storage partitions 3a, 3b, 3c in a cloud server 4. The SIM 2 contains software for accessing remote data partitions.

The mobile telephone 1 can only access a partition 3a, 3b, or 3c upon entering the correct passcode or PIN for that partition 3a, 3b, or 3c. Each partition has its own passcode or PIN which is set by the user.

In addition to the correct passcode or PIN, an identification code from the correct SIM 2 must also be provided for access to the data in a partition 3a, 3b or 3c to be granted.

When a user wishes to access a particular partition 3a, 3b, or 3c, they enter the passcode or PIN for that partition 3a, 3b, or 3c by typing on the keypad or touch-sensitive screen of the mobile telephone 1. The entered passcode or PIN is then passed to the SIM 2 where it is passed an encryption algorithm combining it with the SIM identification code to create a hash.

The hash is then passed to a processor at the cloud server 4 where it is decrypted to extract the passcode or PIN and identify which partition 3a, 3b or 3c the user is seeking to access. Then, if the hash corresponds to a hash already stored in memory at the cloud server 4 for that partition 3a, 3b or 3c, access to the requested partition 3a, 3b or 3c is allowed and data stored in that partition 3a, 3b or 3c can be accessed via the mobile telephone 1.

In some embodiments, a third form of authentication such as something the user "has", e.g. a form of genetic or biometric ID (e.g. a finger-print or iris scan) is also required in order for access to the partition 3a, 3b or 3c to be granted. In other embodiments, this is required instead of a passcode or PIN for the partition 3a, 3b or 3c.

The content or data stored in each partition 3a, 3b and 3c is encrypted, so that when access to a particular partition 3a, 3b or 3c is allowed, the content of that partition 3a, 3b or 3c is decrypted using the passcode or PIN for the partition 3a, 3b or 3c and SIM identification code, or a key stored in the SIM 2.

When access to a partition 3a, 3b or 3c has been granted and its content decrypted, the content can be viewed on a screen of the mobile telephone 1.

The mobile telephone 1 is the administrator device which controls the partitions 3a, 3b and 3c. However, a user (or other users) may have further devices from which they would like to access the partitions 3a, 3b and 3c. For example, as shown in Fig. 2, a user has a tablet device 5 with a SIM 5a from which the user would like to access the partitions 3a, 3b and 3c. The SIM 5a of the tablet device 5 is also registered with the partitions 3a, 3b or 3c so that on entry of the correct PIN or passcode and/or the correct genetic or biometric information at the

tablet device 5, the table device 5 is granted access to the partition 3a, 3b or 3c. The way in which access to the partition 3a, 3b or 3c is granted is controlled in the same way as described above for the mobile telephone 1.

Fig. 3 illustrates the case where non-authorised users seek to access a partition 3M stored at a cloud server 4. A non-authorised user has a mobile telephone 6a or 6b with SIM 7a or 7b, respectively. Access to the partition is controlled by the access controller 12. The access controller 12 is located in the cloud. In some embodiments, the access controller 12 is part of a mobile telephone provider system.

The non-authorised user enters a PIN or passcode in their mobile telephone 6a or 6b but access to the partition 3M is not granted because the PIN or passcode is incorrect and/or the SIM identification code is incorrect. The access controller 12 does not allow the mobile telephones 6a and 6b to access the partition 3M. However, it allows the main mobile telephone 1 to access the partition 3M.

Fig. 4 illustrates the case where a non-authorised user and an invited user seek to access a partition 3M stored at a cloud server 4.

In this case, as with the case of Fig. 3, the access controller 12 denies access to partition 3M to the mobile telephone 6a of the non-authorised user.

In order for access to be granted to the invited user, the main user sends a request from their mobile telephone 1 to the cloud server 4 for a one-time-password (OTP) in relation to access to partition 3M. The cloud server 4 verifies that the identification code of the SIM 2 of the mobile telephone 1 is registered with the partition 3M, and that the user associated with that SIM 2 is allowed to invite other users to access partition 3M, and, if so, sends a OTP back to the mobile telephone 1. The main user then sends this OTP on to the mobile telephone 8 of the invited user. The invited user then sends a request to the access controller 12 to access the partition M and enters the OTP. The access controller 12 verifies the OTP and if the OTP is correct then the invited user is granted access to the partition 3M.

In an alternative embodiment (not shown), the main user generates an OTP in their mobile telephone 1 and then sends that OTP to the cloud server 4 for registration against the partition 3M. The OTP is also sent from the mobile telephone 1 to the mobile telephone 8 of the invited user. Once the OTP is registered against the partition 3M the invited user can access the partition 3M by entering the OTP as described above.

In some embodiments, the OTP is only valid for a certain period of time, such as 5 minutes.

In some embodiments, access to the partition 3M is only granted to the invited user for a certain period of time such as 1-24 hours.

In some embodiments, the OTP is only valid for a single access attempt to partition 3M. Once it has been used once then it can no longer be used again to access 3M. A further OTP must be requested by the main user for subsequent access to the partition 3M.

In some embodiments, the main user is able to monitor and/or block access to the partition 3M to the invited user if desired.

When a partition is set up at a cloud server 4, it may be set as an "open" partition such that anyone may access the data stored there. Fig. 5 shows an example of such an open partition 3OA. In some embodiments some users only have "read" access to the data stored in the partition 3OA whereas other users such as invited and/or main users have both "read" and "write" access to the data stored there.

In the case shown in Fig. 5, since partition 3OA is an open partition which is accessed from a main mobile telephone 1, a mobile telephone 8 of an invited user and a mobile telephone 10 of another (non-invited) user, access to the partition 3OA is monitored and recorded in memory 3OA-h. The data recorded consists of an identification code associated with the device accessing the partition 3OA and/or the time of the access attempt for example. Other data may also be recorded. This can allow a main user to monitor access to the partition 3OA and, based on the recorded data and, if desired, block access to the partition 3OA to a particular user.

Fig. 6 is similar to Fig. 5 except that there is no monitoring of access to the partition 3OA.

In order to register a device so that it can access a particular partition, the device must have installed on it appropriate software (e.g. an application) for accessing the partitions. This is, for example, stored in a secure element or memory card associated with the device.

In order to register a device so that it can access a particular partition, the following process, as illustrated in Fig. 7, is then performed:

The user of the device to be registered sends a request to gain access to a partition or partitions from the device to an administrator device, via the partition access controller S1. The request is in the form of an email or SMS, for example.

The request includes a two-factor authenticated code. This code is created from an identification code of a secure element or memory card associated with the device and either a passcode or PIN, or data representing something inherent to the user. This allows for an auditable trail of which devices have requested access to a partition.

When the partition administrator receives the request at the administrator device, the administrator decides whether to grant access to the partition(s) or deny access S2. The administrator can also set access permissions for the user such as read only or the ability to edit/delete/add additional content to the partition.

If the owner has decided to allow access to a partition to a user then they will send a signal from the administrator device to the access controller confirming their agreement for the device to be registered against the partition so that the device can access the partition (with the access partitions specified by the administrator) S3.

The access controller then registers the device (i.e. the identification code associated with its memory card or secure element) against the partition(s) with the access partitions specified S4.

When the user opens or logs into the application for accessing the partitions, they can access the partition(s) by entering the PIN or passcode or data representing something inherent to the user that corresponds to that partition. Different devices can have a different PIN or passcode or data representing something inherent to the user for accessing a given partition.

The user of the device to be registered can be the same person as the administrator or a different person.

The administrator of the partition can also invite someone to access a partition and send an invitation to them to do so. As with the above case, the invited user must have installed on their device appropriate software (e.g. an application) for accessing the partitions. The invitation is sent via the access controller. The invitation can be in the form a message such as an email or SMS message and/or it could be sent and viewable via a messaging system within the partition access application. When the user opens or logs into this application, they can see that an invitation has been received to access a particular partition. The user can then access the partition.

The invitation can include a OTP (one-time-password) which the user can enter in a web browser in order to access the partition via the web browser (as opposed to via the partition access application)

In order for any user to open or log in to the partition access application, they must enter their PIN or passcode for the application, or biometric information, and this is checked together with the identification code for the secure element or memory card associated with their device.

Fig. 8 is a flow diagram illustrating an embodiment of the authentication or verification process of a device. A user of the device opens the partition access application on their device and logs in. This automatically causes a signal to be sent to the partition access controller to say that the application has been opened. A machine-machine handshake is then performed, which includes the access controller checking that the identification code of the SIM (or other secure element or memory card) is registered, as well as the device checking an ID certificate of the access controller. This is performed by a "challenge" being sent from the access controller to the device, which then replies with and "answer". If this the checks are confirmed as being correct then a secure channel is opened between the device and the access controller S5.

The access controller then sends a request to the device, via the secure channel, for the user to enter their PIN or passcode for the partition they wish to access S6.

The user enters the PIN or passcode and the SIM (or other secure element or memory card associated with the device) checks that this is correct. If so, then the SIM (or other secure element or memory card) then generates a certificate based on the entered PIN or passcode S7.

In an alternative embodiment, instead of or in addition to the PIN or passcode, the user could be requested to, and then enter data representing something inherent to them, such as biometric data. The certificate would then be based on this data.

The generated certificate is then sent from the device to the access controller via the secure channel S8.

The access controller checks the certificate and, if it is registered against the requested partition, permission for the device to access the requested partition is granted and the device accesses the requested partition S9.

Fig. 9 is a flow diagram illustrating how an access code for an invited user to access a partition can be encrypted.

When an administrator wishes to provide an access code for a partition so that another user can access that partition (or so that the administrator can access the partition) from an unregistered device, a PIN request is sent from the access controller to the administrator device S10.

The administrator enters a PIN into the administrator device for the partition to which they would like to grant access, and the SIM of the administrator device (or other secure element or memory card associated with the device) then generates an encrypted code S11.

The encrypted code is then sent from the administrator device to the access controller via a secure channel S12.

The access controller then registers the encrypted code against the partition so that, if subsequently entered, access to that partition can be granted S13.

The access controller also sends the encrypted code to the invited device via a secure channel so that the invited device can access the partition.

In some embodiments the encrypted code is only valid for a single access and/or for a limited period of time. In other embodiments, the encrypted code may be valid indefinitely or does not expire.

In some embodiments, the partition access application is an API that is accessed as an Apache Cordova Javascript bridge. It is stored in the secure element or memory card and holds the following keys and PINs which are generated onboard (i.e. in the secure element or memory card):

- One RSA 2048 public/private key pair for the application
- One variable size PIN per partition to authenticate the user
- One 3DES-2 key per partition used for encrypted files

The server or access controller holds two 3DES-2 master keys which can be diversified per device. These two keys are sent to the application following its creation, protected by a Secure Channel of the application Security Domain:

- The Initialization Key used to encrypt Public Key data returned by a Secure Element application in order to verify the authenticity of the application
- The Time Key used to provide a Secure Time source when generating a remote access code for a partition

The Secure Time is a nonce given by the target device followed by the UNIX timestamp, 3DES-2 CBC encrypted by the Time Key.

According to the size of the target file, the partition key can be used to encrypt the file data directly, or a key handled by the handset to encrypt the file data.

The following describes a process which is followed when a user, Sarah, wants to share her partition data with another person, Robert.

Preconditions :

- Robert's device Public Key is registered with the authentication server (access controller), identified by a public identifier (such as Robert e-mail)
- Sarah logs on to the partition to share
- Sarah requests to share this partition with Robert
  - The server obtains the Secure Time Nonce for Sarah's application
  - The server sends Robert's Public Key and the current Secure Time, both encrypted for Sarah's application
  - The handset application obtains the sharing blob, and displays the sharing code to Sarah
  - The sharing blob is sent to the server and associated to Robert public identity
  - Sarah provides the sharing code to Robert (by e-mail, SMS, phone, voice ...)
- Robert sees that a new partition is shared to him by connecting to the server, and enters the sharing code provided by Sarah
  - The server obtains the Secure Time Nonce for Robert's application
  - The server sends the sharing blob and the current Secure Time encrypted for Sarah's application
  - The partition access key is recovered by Robert's Secure Element or Robert's application

The following low level management APIs are defined:

isSecureElementPresent()

returns true if the Secure Element is present

getSecureElementID()

returns the unique ID of the Secure Element (extracted from the CPLC) as an HexString

getCCSEApplicationVersion()

returns the version of the CCPartition application as a string, or "undefined" if the application is not installed

The following application update and initialization APIs are defined:

getKeysetCounter(aid, keysetVersion) (HexString, Number)

returns the counter for the given Security Domain AID and keyset version

executeAPDUScript(apdus) (Array of HexString)

execute an APDU script on the Secure Element, expecting a 90 00 Status Word for each APDU.

The following high level mangement APIs are defined:

getPublicKey()

returns the Public Key of the application, 3DES-2 CBC encrypted with the Initialization Key

createPartition(shortName, pin) (String, HexString)

create a partition given a short name and a PIN, returns a one byte partition ID.

listPartitions()

returns an Array of [id, shortName] identifying the partitions created on the Secure Element

deletePartition(id) (Number)

deletes a partition. The user must be logged on to the partition to delete, or the PIN of the partition must be blocked

The following Usage APIs are defined:

loginPartition(id, pin) (Number, HexString)

logins to a given partition

logoutPartition()

logout from the currently logged in partition

encryptData(data, iv) (HexString, HexString)

encrypts data using a 3DES-2 CBC encryption with the given IV and the currently selected partition key

decryptData(data, iv) (HexString, HexString)

decrypts data using a 3DES-2 CBC encryption with the given IV and the currently selected partition key

getSecureTimeNonce()

returns an 8 bytes nonce to be passed to the server to provide the next Secure Time

getSharingCode(secureTime, encryptedPublicKey, validityMinutes) (HexString, HexString, Number)

get a sharing code for another device. Returns an Array of two elements, a blob to be passed to the remote device and the generated 8 digits code, for example. The blob contains the timestamp of the end of the validity period of the sharing code concatenated with the sharing code concatenated with the partition key and encrypted by the remote device Public Key using PKCS #1 padding. In other embodiments, the code can be of any length and/or cane be alpha numeric.

useSharingCode(secureTime, blob, accessCode) (HexString, HexString, String)

use a sharing code obtained from a remote device. If the blob, access code and time validity are approved by the application, files can be encrypted and decrypted with the extracted partition key using the partition Id 0xff until the user logs out or the Secure Element is powered off.

Claims:

1. A method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps:

(i) sending a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device;

(ii) verifying, based at least partly on the identification code, whether access to the data is to be allowed or denied; and

(iii) allowing or denying the device access to the data accordingly.

2. A method as claimed in claim 1, wherein the data is stored in the cloud.

3. A method as claimed in claim 1 or 2, wherein the request includes a passcode or PIN entered at the device and step (ii) also comprises verifying based on the passcode or PIN whether access to the data is to be allowed or denied.

4. A method as claimed in any preceding claim, wherein the request includes data representing something inherent to a user of the device, and step (ii) also comprises verifying based on the data representing something inherent to the user of the device whether access to the data is to be allowed or denied.

5. A method as claimed in claim 4, wherein the data representing something inherent to the user of the device comprises data representing genetic and/or biometric information about the user.

6. A method as claimed in any preceding claim, wherein the a secure element or memory card is a SIM, SE, TEE, Micro SD, Memory card, USB key or Smartcard associated with the device.

7. A method as claimed in any preceding claim, wherein the data is stored in a partition associated with the device, and the request comprises data specifying the partition.

8. A method as claimed in claim 7, wherein the data specifying the partition comprises one or more of:
- a PIN or passcode; and
- data representing something inherent to the user of the device.

9. A method as claimed in claim 8, wherein the data representing something inherent to the user of the device comprises data representing genetic and/or biometric information about the user.

10. A method as claimed in any preceding claim, wherein the device is a telephone, a tablet, a laptop computer, a desktop computer, a TV, a set top box, a camera, a car, a games consol, glasses, a watch, Chromecast, a smart meter or any other device which is capable of sending and receiving data to remote devices.

11. A method as claimed in any preceding claim, the method comprising, prior to steps (i)-(iii):

registering an identification code of a secure element or memory card with the data.

12. A method as claimed in claim 11, wherein identification codes of more than one secure element or memory card are associated with the data.

13. A method of controlling access to data from a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps:

(i) receiving a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device;

(ii) verifying, based at least partly on the identification code, whether access to the data is to be allowed or denied; and

(iii) allowing or denying the device access to the data accordingly.

14. A method as claimed in claim 13, further comprising any of the features of claims 1-12.

15. A method as claimed in claim 13 or 14, wherein the method is performed by a data access controller.

16. A method as claimed in claim 15, wherein the data access controller is remote from the device.

17. A data access controller for controlling access to data stored remotely from a device or in removable storage, the data access controller being arranged to perform the following steps:

(i) receive a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device;

(ii) verify, based at least partly on the identification code, whether access to the data is to be allowed or denied; and

(iii) allow or deny the device access to the data accordingly.

18. A data access controller as claimed in claim 17, wherein the data access controller is remote from the device which wishes to access the data.

19. A system comprising a device and a data access controller for controlling access from the device to data stored remotely from the device or in removable storage, wherein the device is arranged to send a request to access the data to the data access controller, the request including an identification code of a secure element or memory card associated with the device; and the data access controller is arranged to verify, based at least partly on the identification code, whether access to the data is to be allowed or denied, and to allow or deny the device access to the data accordingly.

20. A computer program for controlling access to data stored remotely from a device or in removable storage, the program being configured to perform the following steps when executed by a processor: (i) receive a request from the device to access the data, the request including an identification code of a secure element or memory card associated with the device; (ii) verify, based at least partly on the identification code, whether access to the data is to be allowed or denied; and (iii) allow or deny the device access to the data accordingly.

21. A method of registering a device with an access controller such that the device may access data via the access controller, the data being stored remotely from a device or in removable storage, wherein the method comprises:

sending a request to register a device for access to data, the request including an identification code of a secure element or memory card associated with the device;

checking whether access to the data is to be allowed; and

if access is to be allowed, registering the identification code against the data to be accessed.

22. A method as claimed in claim 21, wherein the request includes a two or three factor authentication code.

23. A method as claimed in claim 22, wherein the two or three factor authentication code is based on the identification code of a secure element or memory card associated with the device and one or more of a PIN or passcode, and data representing something inherent to the user.

24. A method as claimed in any of claims 21-23, wherein the request is in the form of an email or SMS.

25. A method as claimed in any of claims 21-24, further comprising sending information related to the request to an administrator device, wherein the administrator device preferably decides whether or not access to the data is to be granted.

26. A method of registering a device with an access controller such that the device may access data via the access controller, the data being stored remotely from a device or in removable storage, wherein the method comprises:

receiving a request to register a device for access to data, the request including an identification code of a secure element or memory card associated with the device;

checking whether access to the data is to be allowed; and

if access is to be allowed, registering the identification code against the data to be accessed.

27. A data access controller for controlling registration of devices with access to data, the controller being arranged to perform the following steps:

receive a request to register a device for access to data, the request including an identification code of a secure element or memory card associated with the device;

check whether access to the data is to be allowed; and

if access is to be allowed, register the identification code against the data to be accessed.

28. A system comprising a device and a data access controller for controlling registration of devices with access to data, the controller being arranged to perform the following steps:

receive from the device a request to register the device for access to data, the request including an identification code of a secure element or memory card associated with the device;

check whether access to the data is to be allowed; and

if access is to be allowed, register the identification code against the data to be accessed.

29. A computer program for controlling registration of devices with access to data, the program being configured to perform the following steps when executed by a processor:

receive from the device a request to register the device for access to data, the request including an identification code of a secure element or memory card associated with the device;

check whether access to the data is to be allowed; and

if access is to be allowed, register the identification code against the data to be accessed.

30. A method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising:

receiving at the device an invitation to access the data, the invitation comprising a password, code or PIN;

sending a request from the device to access the data, the request including the password, code or PIN;

verifying, based at least partly on the password, code or PIN, whether access to the data is to be allowed or denied; and

allowing or denying the device access to the data accordingly.

31. A method as claimed in claim 30, wherein the password, code or PIN is generated by a random number generator.

32. A method as claimed in claim 30 or 31, wherein the password, code or PIN is a one-time-password.

33. A method as claimed in claim 30, 31 or 32, wherein the password, code or PIN is only valid for a specified period of time.

34. A method as claimed in any of claims 30-33, wherein the password, code or PIN is generated by a device controlling access to the data.

35. A method as claimed in any of claims 30-34, wherein the method is a method of a first device allowing a second device to access data, wherein the data is stored remotely from the first and second devices, the invitation being sent from the first device to the second device, the request to access the data being sent from the second device and access to the data is allowed or denied to the second device.

36. A method as claimed in claim 35, wherein the password, code or PIN is generated in the first device.

37. A method as claimed in claim 35, wherein the password, code or PIN is generated remotely from both the first and second devices.

38. A method as claimed in claim 36 or 37, the method further comprising registering the generated password, code or PIN with the data to be accessed.

39. A method as claimed in claim 38 when dependent on claim 36, wherein the step of registering the generated password, code or PIN with the data to be accessed comprises verifying that the first device is allowed to invite further devices to access the data before registering the generated password, code or PIN.

40. A method as claimed in claim 38 when dependent on claim 37, the method further comprising sending a request from the first device for the password, code or PIN to be generated, wherein the password, code or PIN to be generated is only generated after it has been verified that the first device is allowed to invite further devices to access the data.

41. A method as claimed in claim 40, wherein the step of verifying that the first device is allowed to invite further devices to access the data comprises verifying an identification code associated with the device, such as an identification code of a secure element or memory card associated with the device.

42. A method as claimed in claim 41, wherein the step of verifying that the first device is allowed to invite further devices to access the data further comprises verifying data specifying the partition sent from the first device.

43. A method as claimed in claim 42, wherein the data specifying the partition comprises one or more of:

- a PIN or passcode; and
- data representing something inherent to the user of the device such as genetic and/or biometric information.

44. A method of allowing access to data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising:

sending to the device an invitation to access the data, the invitation comprising a password, code or PIN;

sending a request from the device to access the data, the request including the password, code or PIN;

verifying, based at least partly on the password, code or PIN, whether access to the data is to be allowed or denied; and

allowing or denying the device access to the data accordingly.

45. A system comprising a first device, a second device and a data access controller, the first device being arranged to invite the second device to access data, wherein the data is stored remotely from the second device or in removable storage,

wherein the first device is arranged to send to the second device an invitation to access the data, the invitation comprising a password, code or PIN;

the second device is arranged to send a request to access the data, the request including the password, code or PIN; and

the data access controller is arranged to verify, based at least partly on the password, code or PIN, whether access to the data is to be allowed or denied, and to allow or deny the second device access to the data accordingly.

46. A method of accessing data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps:

(i) sending a request from the device to access the data, the request including data related to the request;

(ii) verifying, based at least partly on the data, whether access to the data is to be allowed or denied; and

(iii) allowing the device access to the data accordingly and only if there is at least one further device accessing the data.

47. A method as claimed in claim 46, further comprising the features of any of claims 1-28.

48. A method as claimed in claim 46 or 47, wherein the further device is an administrator device registered with the data.

49. A method as claimed in any of claims 46-48, further comprising, prior to step (iii), checking whether at least one further device is accessing the data.

50. A method of controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the method comprising the following steps:

(i) receiving a request from the device to access the data, the request including data related to the request;

(ii) verifying, based at least partly on the data, whether access to the data is to be allowed or denied; and

(iii) allowing the device access to the data accordingly and only if there is at least one further device accessing the data.

51. A data access controller for controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the data access controller being arranged to perform the following steps:

(i) receive a request from the device to access the data, the request including data related to the request;

(ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and

(iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

52. A data access controller as claimed in claim 51, wherein the data access controller is arranged to check whether at least one further device is accessing the data prior to performing step (iii).

53. A system comprising a device and a data access for controlling access to data at a device, wherein the data is stored remotely from the device or in removable storage, the data access controller being arranged to perform the following steps:

(i) receive a request from the device to access the data, the request including data related to the request;

(ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and

(iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

54. A system as claimed in claim 53, wherein the device is arranged to send the request to access the data to the data access controller.

55. A system as claimed in claim 53 or 54, wherein the data access controller is arranged to check whether at least one further device is accessing the data prior to performing step (iii).

56. A computer program for controlling access to data stored remotely from a device or in removable storage, the program being configured to perform the following steps when executed by a processor:

(i) receive a request from the device to access the data, the request including data related to the request;

(ii) verify, based at least partly on the data, whether access to the data is to be allowed or denied; and

(iii) allow the device access to the data accordingly and only if there is at least one further device accessing the data.

57. A program as claimed in claim 56, wherein the program is further configured to check whether at least one further device is accessing the data prior to performing step (iii).

58. A method of accessing data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the method comprising the following steps:

(i) sending a request to access the data, the request including an identification code associated with the device and one or more of:

- a PIN or passcode; and
- data representing something inherent to the user of the device such as genetic and/or biometric information;

(ii) verifying, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and

(iii) allowing or denying the device access to the data accordingly.

59. A method as claimed in claim 58, wherein the data is stored in a partition.

60. A method as claimed in claim 59, wherein the PIN or passcode, and/or the data representing something inherent to the user of the device such as genetic

and/or biometric information, is associated with and can identify the data which a user is seeking to access.

61. A method of controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the method comprising the following steps:

(i) receiving a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information;

(ii) verifying, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and

(iii) allowing or denying the device access to the data accordingly.

62. A data access controller for controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the data access controller being arranged to perform the following steps:

(i) receive a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information;

(ii) verify, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and

(iii) allow or deny the device access to the data accordingly.

63. A computer program for controlling access to data at a device, wherein the data is stored remotely from the device, in removable storage or in the device itself, the program being configured to perform the following steps when executed by a processor:

(i) receive a request to access the data, the request including an identification code associated with the device and one or more of: a PIN or passcode; and data representing something inherent to the user of the device such as genetic and/or biometric information;

(ii) verify, based on the identification code, and the PIN or passcode and/or data representing something inherent to the user, whether access to the data is to be allowed or denied; and

(iii) allow or deny the device access to the data accordingly.

5

Intellectual Property Office

Application No:	GB1315420.8	**Examiner:**	Mr Andrew Hole
Claims searched:	1-20, 58-63	**Date of search:**	29 January 2014

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	US 2009/0183010 A1 (SCHNELL et al.) Please see abstract, drawings and paragraphs 22-55 in particular.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	US 2011/0078762 A1 (BIJLSMA) Please see abstract, drawings and paragraphs 19-35 in particular.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	CN 102761870 A (ZTE CORP) Please see EPODOC abstract and WPI/Thomson abstract, accession number 2013-B49447.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	KR 20130085472 A1 (INTELLECTUAL DISCOVERY) Please see EPODOC abstract and WPI/Thomson abstract, accession number 2013-K64674.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	US 2012/0054845 A1 (RODRIGUEZ et al.) Please see abstract, drawing and paragraph 41 in particular.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	WO 2011/150968 A1 (MALVACOM) Please see abstract and drawings and page 15, lines 11-25 in particular.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	US 2011/0099616 A1 (MAZUR et al.) Please see drawings, abstract and paragraphs 23-35 in particular.
X	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	US 8438654 A1 (von EICKEN et al.) Please see abstract, drawings and column 9, line 55 to column 11, line 45 in particular.
X,E	1, 13, 17, 19, 20, 58, 61, 62, & 63 at least.	WO 2013/124689 A2 (SILICON GREEN) Please see whole document.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

Worldwide search of patent documents classified in the following areas of the IPC

G06F; H04L

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, TXTE

International Classification:

Subclass	Subgroup	Valid From
G06F	0021/62	01/01/2013
G06F	0021/34	01/01/2013