(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2018 (12.07.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/127606 A1

(51) International Patent Classification:
G06F 21/62 (2013.01) *G06F 11/14* (2006.01)

(21) International Application Number:
PCT/EP2018/050474

(22) International Filing Date:
09 January 2018 (09.01.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17305020.4 09 January 2017 (09.01.2017) EP

(71) Applicant: **THOMSON LICENSING** [FR/FR]; 1-5 rue Jeanne d'Arc, 92130 Issy-les-Moulineaux (FR).

(72) Inventors: **MARTENS, David**; Technicolor Delivery Technologies Belgium, Prins Boudewijnlaan 47, 2650 EDEGEM (BE). **HARDOUIN, Olivier**; Schone Luchtlaan 23, 1970 Wezembeek Oppem (BE).

(74) Agent: **CODA, Sandrine**; TECHNICOLOR, 1-5 rue Jeanne d'Arc, 92130 Issy-les-Moulineaux (FR).

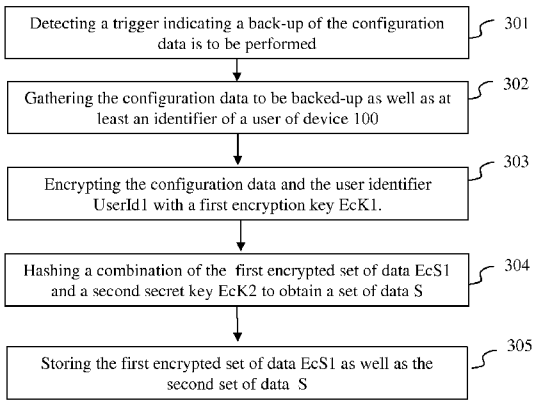
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:
— *with international search report (Art. 21(3))*

(54) Title: METHODS AND APPARATUS FOR PERFORMING SECURE BACK-UP AND RESTORE



(57) Abstract: Back-up procedures for saving configuration data are provided, which enable the restoration of said configuration data on the device when it is reset to default, or on another device when the device is stolen or broken. Since configuration data are sensitive data, it is important to protect their confidentiality and their integrity throughout the back-up and restore process. Current solutions enable a secure back-up and restore process on the same device since the backed-up configuration data are encrypted using credentials that are only known to the device. In order to overcome these drawbacks, a solution is proposed for performing a secure back-up process which enables the restoration of the backed-up data to the same device or to a distinct device. This is made possible by using encryption keys that are common to a pool of devices. Those common encryption keys are provided during the manufacturing of the devices.

Fig. 3

WO 2018/127606 A1

METHODS AND APPARATUS FOR PERFORMING SECURE BACK-UP AND RESTORE

TECHNICAL FIELD

The present invention relates to solutions for restoring configuration data. More particularly, the invention concerns methods for performing secure back-up of configuration data and easy restoring of said back-up data.

BACKGROUND

Existing communication devices, such as residential gateways, access points, repeaters, mobile phones, computers, etc. are configured according to different settings in order to behave as their users want.

Back-up procedures for saving those configuration data are provided which enables to restore said configuration data on the device when it is reset to default or on another device when the device is stolen or broken.

Since configuration data are sensitive data, it is important to protect their confidentiality and their integrity throughout the back-up and restore process.

Current solutions enable a secure back-up and restore process on the same device since the backed-up configuration data are encrypted using credentials that are only known to the device.

Thus, if the configuration data are to be restored on another device, the configuration data are stored in plaintext, i.e. they are not encrypted, allowing the restoration on said other device. This lack of security is a major drawback of existing back-up and restore solutions.

The present invention has been devised with the foregoing in mind.

SUMMARY OF INVENTION

According to a first aspect of the invention there is provided a computer implemented method for performing a secure back-up of configuration data of a first device, said method comprising:

- encrypting said configuration data and at least one identifier of a user of said first device, using a first pre-provisioned encryption key stored in a read only memory of said first device,

- encrypting a set of data obtained by hashing a combination of the encrypted configuration data and the at least one identifier of the user of said first device and a second pre-provisioned secret key stored in said read only memory of said first device,

- storing the encrypted configuration data and at least one identifier of the user of said first device and the encrypted set of data.

Such a solution provides a secure back-up process which enables the restoration of the backed-up data on the same device or on a distinct device. This is made possible by using encryption keys that are common to a pool of devices, such as devices of a same product model or devices of another product model manufactured by the same company and which is pre-loaded in a memory of said device.

Those common encryption keys are, for example, provided during the manufacturing of the devices and are stored in a section of a memory of the devices.

In an embodiment of the invention, the first pre-provisioned encryption key is a symmetric encryption key.

In an embodiment of the invention, the second pre-provisioned encryption key is common secret key.

In an embodiment of the invention, the secure back-up is performed at regular time intervals.

Such an embodiment does not require an action from the user of the device. It enables to have regular back-up which might prove useful depending on the sensitivity of the configuration data.

In an embodiment of the invention, the secure back-up is triggered by an action detected on a user interface of the first device.

The user of the device may trigger a back-up of the configuration data depending on his/her needs.

Another object of the invention concerns a computer implemented method for restoring configuration data on a first device, said method comprising:

- checking an integrity of the second set of data related to the configuration data to be restored using a first pre-provisioned secret key stored in a read only memory of said first device,

- when the integrity of the second set of data is checked, decrypting a second set of data comprising the configuration data using a second pre-provisioned decryption key stored in said read only memory of said first device,

- restoring the configuration data when at least one identifier of a user of said first device comprised in the decrypted second set of data matches at least one identifier of said user of said first device provided to the first device.

Such a solution enables to restore data securely backed-up on a first device on a second device. This is made possible by using pre-provisioned decryption keys that are common to a pool of devices, such as devices of a same product model or devices of another product model manufactured by the same company.

Those common pre-provisioned decryption keys are, for example, provided during the manufacturing of the devices and are stored in a section of a memory of the devices. Thus these decryption keys can be used do decrypt data encrypted with the encryption keys used by the same devices to encrypt their configuration data during the back-up process.

In such a solution, the integrity of the backed-up data is assured since if the integrity of the data to be restored is not checked, the restored process is stopped.

Furthermore, in order to increase the security of the overall process, data are restored on a device only if a final check is done. This final check consists in verifying that the user of the device on which the back-up was performed is the same user of the device on which the data are to be restored. Such a check is important since different devices use the same encryption and decryption keys.

In an embodiment of the invention, checking the integrity of a second set of data comprises:

- generating a third set of data by hashing a combination of the second set of encrypted data and the first pre-provisioned secret key,

- comparing said first set of data with the third set of data,

the integrity of the first set of data being checked when the first set of data is identical to the third set of data.

Another object of the invention is an apparatus capable of performing a secure back-up of configuration data, said apparatus comprising a processor configured to:

- encrypt said configuration data and at least one identifier of a user of said first device during a production of said first device and stored in a read only memory of said first device,

- encrypt a set of data obtained by hashing a combination of the encrypted configuration data and the at least one identifier of the user of said first pre-provisioned device and a second pre-provisioned secret key stored in said read only memory of said first device,

- store the encrypted configuration data and at least one identifier of the user of said first device and the encrypted set of data.

Another object of the invention is an apparatus capable of restoring configuration data on a first device, apparatus comprising a processor configured to:

- check an integrity of the second set of data related to the configuration data to be restored using a first pre-provisioned secret key stored in a read only memory of said first device,

- when the integrity of the second set of data is checked, decrypt that second set of data comprising the configuration data using a second pre-provisioned decryption key stored in said read only memory of said first device,

- restore the configuration data when at least one identifier of a user of said first device comprised in the decrypted second set of data matches at least one identifier of said user of said first device provided to the first device.

Some processes implemented by elements of the invention may be computer implemented. Accordingly, such elements may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit", "module" or "system'. Furthermore, such elements may take the form of a computer program product embodied in any tangible medium of expression having computer usable program code embodied in the medium.

Since elements of the present invention can be implemented in software, the present invention can be embodied as computer readable code for provision to a programmable apparatus on any suitable carrier medium. A tangible carrier medium may comprise a storage medium such as a floppy disk, a CD-ROM, a hard disk drive, a magnetic tape device or a solid state memory device and the like. A transient carrier medium may include a signal such as an electrical signal, an electronic signal, an optical signal, an acoustic signal, a magnetic signal or an electromagnetic signal, e.g. a microwave or RF signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, and with reference to the following drawings in which:

Figure 1 represents a communication device implementing the back-up and restore methods according to an embodiment of the invention,

Figure 2 a schematic block diagram illustrating an example of the communication device according to an embodiment of the invention,

Figure 3 represents a flow chart for explaining a process for performing a secure back-up of configuration data according to an embodiment of the invention,

Figure 4 represents a flow chart for explaining a process for restoring securely backed-up configuration data according to an embodiment of the invention.

DETAILED DESCRIPTION

As will be appreciated by one skilled in the art, aspects of the present principles can be embodied as a system, method or computer readable medium. Accordingly, aspects of the present principles can take the form of an entirely hardware embodiment, an entirely software embodiment, (including firmware, resident software, micro-code, and so forth) or an embodiment combining software and hardware aspects that can all generally be referred to herein as a "circuit", "module", or "system". Furthermore, aspects of the present principles can take the form of a computer readable storage medium. Any combination of one or more computer readable storage medium(a) may be utilized.

As represented on **figure 1**, a first communication device 100 is a home gateway. The first communication device 100 comprises at least one network interface 110 for communicating with a broadband network for example. Such a network interface 110 is for example configured to receive and transmit data from and to a DSLAM (*Digital Subscriber Line Access Multiplexer*) using xDSL (*x Digital Subscriber Line*) or from and to an OLT (*Optical Line Termination*) through an optical fiber.

In an embodiment of the invention, the first communication device 100 may embed both wireless and wired transmission interfaces.

Figure 2 is a schematic block diagram illustrating an example of the first communication device 100 according to an embodiment of the invention.

The first communication device 100 comprises a processor 201, a storage unit 202, an input device 203, a display device 204, and an interface unit 205 which are connected by a bus 206. Of course, constituent elements of the first communication device 100 may be connected by a connection other than a bus connection.

The processor 201 controls operations of the first communication device 100. The storage unit 202 stores at least one program capable of performing a secure back-up and restore of the configuration data of the first communication device 100, to be executed by the processor 201, and

various data, parameters used by computations performed by the processor 201, intermediate data of computations performed by the processor 201, and so on. The processor 201 may be formed by any known and suitable hardware, or software, or a combination of hardware and software. For example, the processor 201 may be formed by dedicated hardware such as a processing circuit, or by a programmable processing unit such as a CPU (*Central Processing Unit*) that executes a program stored in a memory thereof.

The storage unit 202 may be formed by any suitable storage or means capable of storing the program, data, or the like in a computer-readable manner. Examples of the storage unit 202 include non-transitory computer-readable storage media such as semiconductor memory devices, and magnetic, optical, or magneto-optical recording media loaded into a read and write unit. The program causes the processor 201 to perform a process of secure back-up and restore according to an embodiment of the present disclosure as described hereinafter with reference to figures 3 and 4.

The input device 203 may be formed by a keyboard, a pointing device such as a mouse, or the like for use by the user to input commands, to make user's selections of parameters used for selecting the transmission interface to be used. The output device 204 may be formed by a display device to display, for example, a Graphical User Interface (GUI). The input device 203 and the output device 204 may be formed integrally by a touchscreen panel, for example.

The interface unit 205 provides an interface between the first communication device 100 and an external apparatus. The interface unit 205 may be communicable with the external apparatus via cable or wireless communication. In an embodiment, the external apparatus may be an optical acquisition system such as an actual camera.

The invention may be executed in devices other than gateways, such as mobile phones, computers, captors, etc.

Figure 3 is a flow chart for explaining a process for performing a secure back-up of configuration data. The invention relies on the use of a shared secret, such as encryption and secret

keys, between the device for which data are to be back-up and the device on which said backed-up data are to be restored. Those two devices maybe one and the same or distinct devices. The user of the devices does not need to configure the devices with the shared secret.

In a step 301, the processor 201 detects a trigger indicating that a back-up of the configuration data of device 100 is to be performed.

In a first embodiment of the invention, the trigger is the expiration of a timer. For example, a back-up of the configuration data of device 100 is scheduled every day or every hour, or every X minutes, etc. depending on the sensitivity of the configuration data.

In another embodiment of the invention, the trigger is the detection of an action on the input device 203. In this case the detection of this action triggers the back-up process.

In a step 302, the processor 201 gathers the configuration data to be backed-up as well as at least an identifier of a user UserId1 of device 100, such as a customer identifier, a phone number, etc.

In a step 303, the configuration data and the user identifier UserId1 are encrypted using a first pre-provisioned encryption key EcK1. Those encrypted data consist in a first encrypted set of data EcS1.

Such a first encryption key EcK1 is for example provisioned during the manufacturing of device 100 and more generally in all the devices of the same product model as device 100 or devices of other product models of the same manufacturer. The first pre-provisioned encryption key EcK1 consists in truly random data created by a Hardware Security Module (HSM). The first pre-provisioned encryption key EcK1 is stored in a partition of the storage unit 202.

The first pre-provisioned encryption key is a symmetric key according, for example, to the AES-256 protocol (*Advanced Encryption Standard*).

The first pre-provisioned encryption key EcK1 may also be generated by the processor 201 using an encryption common to all the devices of the same product model as device 100 or devices of other product models of the same manufacturer as well as an identifier of the product model and an identifier of the device 100 such as a serial number.

In a step 304, a second set of data S is obtained by hashing a combination of the first pre-provisioned encrypted set of data EcS1and a second pre-provisioned secret key EcK2.using, for example, an HMAC scheme (*keyed-Hash Message Authentication Code).*

Such a second pre-provisioned secret key EcK2 is for example provisioned during the manufacturing of device 100 and more generally in all the devices of the same product model as device 100 or devices of other product models of the same manufacturer. The second pre-provisioned secret key EcK2 consists in truly random data created by a Hardware Security Module (HSM). The second pre-provisioned secret key EcK2 is stored in a partition of the storage unit 202.

The second pre-provisioned secret key EcK2 may also be generated by the processor 201 using an encryption common to all the devices of the same product model as device 100 or devices of other product models of the same manufacturer as well as an identifier of the product model and an identifier of the device 100 such as a serial number.

In an embodiment of the invention, the first pre-provisioned encryption key EcK1 and second pre-provisioned secret key EcK2 are transmitted to the device 100 by a third party such as the manufacturer of the device 100 or a provider managing the device 100. The first pre-provisioned encryption key EcK1 and the second pre-provisioned secret key EcK2 are common to all devices of the same product model as device 100 or devices of other product models of the same manufacturer, enabling the secret to be shared between different devices.

The second set of data S obtained during step 304 is used to check the integrity of the backed-up configuration data during the restoring process.

In a step 305, the processor 201 stores the first encrypted set of data EcS1 comprising the encrypted configuration data and at least one identifier of the user of device a100 as well as the second set of data S.

Those data are stored either in the storage unit 202 of device 100 or in a remote server. This later embodiment enables to remotely retrieve the data needed for restoring a configuration on a

device.

Figure 4 is a flow chart for explaining a process for restoring securely backed-up configuration data. The invention relies on the use of a shared secret, such as decryption and secret keys, between the device for which data are backed-up and the device on which said backed-up data are to be restored. Those two devices maybe one and the same or distinct devices. The user of the devices does not need to configure the devices with the shared secret.

In a step 401, the processor 201 detects a trigger indicating that a restore of the configuration data of device 100 is to be performed.

In an embodiment of the invention, the trigger is the detection of an action on the input device 203 such as a reset command or a boot command. In another embodiment, the trigger is the detection of an action on the input device 203. In this case the detection of this action triggers the restore process.

In a step 402, the processor 201 retrieves a first set of data S and a second encrypted set of data EcS1. The first set of data S is used to check the integrity of the second encrypted set of data EcS1, while the second encrypted set of data EcS1 comprises the configuration data needed to complete the restore process.

In an embodiment, the restoring of the configuration takes place on the same device 100. In this case, the processor 201 may retrieve the first set of data S and the second encrypted set of data EcS1 in the storage unit 202.

In another embodiment, the restoring of the configuration takes place on another device such as a device of the same product model as device 100 or a device of another product model of the same manufacturer. In this case, the processor 201 may retrieve the first set of data S and the second encrypted set of data EcS1 from a remote server.

In a step 403, the processor 201 checks the integrity of the second encrypted set of data EcS1. The processor 201 checks the integrity of said second encrypted set of data EcS1 using a first pre-

provisioned secret key DcK2 which corresponds to the second pre-provisioned secret key EcK2 used during the back-up process described in reference to figure 3.

The first pre-provisioned secret key DcK2 is for example provisioned during the manufacturing of device 100 and more generally in all the devices of the same product model as device 100 or devices of other product models of the same manufacturer. The first pre-provisioned secret key DcK2 consists in truly random data created by a Hardware Security Module (HSM). The first pre-provisioned secret key DcK2 is stored in a partition of the storage unit 202.

The first pre-provisioned secret key DcK2 may also be generated by the processor 201 using an encryption common to all the devices of the same product model as device 100 or devices of other product models of the same manufacturer as well as an identifier of the product model and an identifier of the device 100 such as a serial number.

The processor 201 generates a third set of data S' by hashing a combination of the second set of encrypted data EcS1 and the second pre-provisioned secret key EcK2 using, for example, an HMAC scheme and compares the first set of data S with the third set of data S'.

If the first set of data S and the third set of data S' are identical, then the processor 201 executes step 404, if they are different, then the restore process is stopped.

During step 404, the processor 201 decrypts the second encrypted set of data EcS1 using a second pre-provisioned decryption key DcK1 which corresponds to the first pre-provisioned encryption key EcK1 used during the back-up process described in reference to figure 3.

The second pre-provisioned decryption key DcK1 is for example provisioned during the manufacturing of device 100 and more generally in all the devices of the same product model as device 100 or devices of other product models of the same manufacturer. The second pre-provisioned decryption key DcK1 consists in truly random data created by a Hardware Security Module (HSM). The second decryption key DcK1 is stored in a partition of the storage unit 202.

The second pre-provisioned decryption key DcK1 is a symmetric key according to the AES-256 protocol (*Advanced Encryption Standard*).

The second pre-provisioned decryption key DcK1 may also be generated by the processor 201 using an encryption common to all the devices of the same product model as device 100 or devices of other product models of the same manufacturer as well as an identifier of the product model and an identifier of the device 100 such as a serial number.

The first pre-provisioned secret key DcK2, and the second pre-provisioned decryption DcK1, are common to all devices of the same product model as device 100 or devices of other product models of the same manufacturer, enabling the secret to be shared between different devices.

In an embodiment of the invention, the first pre-provisioned secret key DcK2 and second pre-provisioned decryption key DcK1 are transmitted to the device 100 by a third party such as the manufacturer of the device 100 or a provider managing the device 100.

If the decryption of the second encrypted set of data EcS1 is not possible, meaning the device performing the restore process is not an authorized device, then the restore process is stopped.

If the decryption of the second encrypted set of data EcS1 is successful, the configuration data as well as at least one user identifier UserId1 are retrieved by the processor 201.

In a step 405, the processor 201 compares the user identifier UserId1 retrieved during step 404 with a second user identifier UserId2 provided locally to the device executing the restore process. The first user identifier UserId1 and the second user identifier UserId2 may be the same, e.g. they may be the phone number of the user of device 100.

If the two user identifiers UserId1 and UserId2 match, then the processor 201 can perform the restoring of the configuration data, if the user identifiers UserId1 and UserId2 do not match, the restore process is stopped.

The second user identifier UserId2 may be provided locally through the input device 203 or remotely using processes such as TR-69 before the beginning of the restore process.

Although the present invention has been described hereinabove with reference to specific embodiments, the present invention is not limited to the specific embodiments, and modifications will be apparent to a skilled person in the art which lie within the scope of the present invention.

Many further modifications and variations will suggest themselves to those versed in the art upon making reference to the foregoing illustrative embodiments, which are given by way of example only and which are not intended to limit the scope of the invention, that being determined solely by the appended claims. In particular the different features from different embodiments may be interchanged, where appropriate.

CLAIMS

1. A computer implemented method for performing a secure back-up of configuration data of a first device, said method comprising:

- encrypting said configuration data and at least one identifier of a user of said first device, using a first pre-provisioned encryption key stored in a read only memory of said first device,

- encrypting a set of data obtained by hashing a combination of the encrypted configuration data and the at least one identifier of the user of said first device and a second pre-provisioned secret key stored in said read only memory of said first device,

- storing the encrypted configuration data and at least one identifier of the user of said first device and the encrypted set of data.

2. The method according to claim 1 wherein the first pre-provisioned encryption key is a symmetric encryption key.

3. The method according to claim 1 wherein the second pre-provisioned secret key is a common secret key.

4. The method according to claim 1 wherein the secure back-up is performed at regular time intervals.

5. The method according to claim 1 wherein the secure back-up is triggered by an action detected on a user interface of the first device.

6. A computer implemented method for restoring configuration data on a first device, said method comprising:

- checking an integrity of the second set of data related to the configuration data to be restored using a first pre-provisioned secret key stored in a read only memory of said first device,

- when the integrity of the second set of data is checked, decrypting a second set of data comprising the configuration data using a second pre-provisioned decryption key stored in said read only memory of said first device,

- restoring the configuration data when at least one identifier of a user of said first device comprised in the decrypted second set of data matches at least one identifier of said user of said first device provided to the first device.

7. The method according to claim 6 wherein checking the integrity of the second set of data comprises:

- generating a third set of data by hashing a combination of the second set of encrypted data and the first secret key,

- comparing said first set of data with the third set of data,

the integrity of the first set of data being checked when the first set of data is identical to the third set of data.

8. An apparatus capable of performing a secure back-up of configuration data, said apparatus comprising a processor configured to:

- encrypt said configuration data and at least one identifier of a user of said first device, using a first pre-provisioned encryption key in a read only memory of said first device,

- encrypt a set of data obtained by hashing a combination of the encrypted configuration data and the at least one identifier of the user of said first device and a second pre-provisioned secret key stored in said read only memory of said first device,

- store the encrypted configuration data and at least one identifier of the user of said first device and the encrypted set of data.

9. An apparatus capable of restoring configuration data on a first device, apparatus comprising a processor configured to:

- check an integrity of the second set of data related to the configuration data to be restored using a first pre-provisioned secret key stored in a read only memory of said first device,

- when the integrity of the second set of data is checked, decrypt that second set of data comprising the configuration data using a second pre-provisioned decryption key stored in said read only memory of said first device,

- restore the configuration data when at least one identifier of a user of said first device comprised in the decrypted second set of data matches at least one identifier of said user of said first device provided to the first device.

10. A computer program characterized in that it comprises program code instructions for the implementation of the method according to any of claims 1 to 5 when the program is executed by a processor.

11. A processor readable medium having stored therein instructions for causing a processor to perform the method according to any of claims 1 to 5.

12. A computer implemented method for performing a secure back-up of configuration data of a first device, said method comprising:

- encrypting said configuration data and at least one identifier of a user of said first device, using a first encryption key provided by a third party and stored in a read only memory of said first device,

- encrypting a set of data obtained by hashing a combination of the encrypted configuration data and the at least one identifier of the user of said first device and a second secret key provided by a third party and stored in said read only memory of said first device,

- storing the encrypted configuration data and at least one identifier of the user of said first device and the encrypted set of data.

13. A computer program characterized in that it comprises program code instructions for the implementation of the method according to any of claims 6 to 7 when the program is executed by a processor.

14. A processor readable medium having stored therein instructions for causing a processor to perform the method according to any of claims 6 to 7.

15. A computer implemented method for restoring configuration data on a first device, said method comprising:

- checking an integrity of the second set of data related to the configuration data to be restored using a first secret key provided by a third party and stored in a read only memory of said first device,

- when the integrity of the second set of data is checked, decrypting a second set of data comprising the configuration data using a second decryption key provided by a third party and stored in said read only memory of said first device,

- restoring the configuration data when at least one identifier of a user of said first device comprised in the decrypted second set of data matches at least one identifier of said user of said first device provided to the first device.

1/3

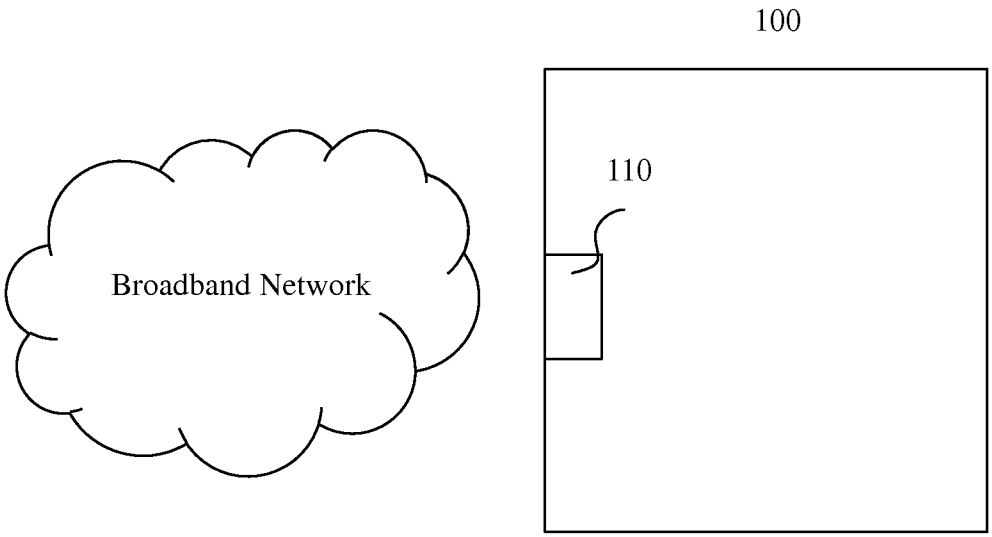

100
110
Broadband Network

Fig. 1

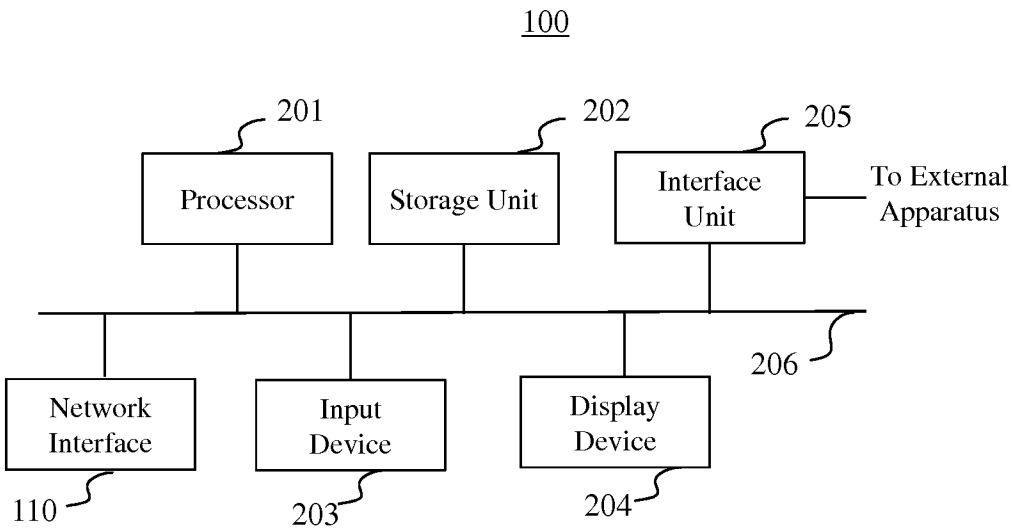

100
201
202
205
Processor
Storage Unit
Interface Unit
To External Apparatus
206
Network Interface
Input Device
Display Device
110
203
204

Fig. 2

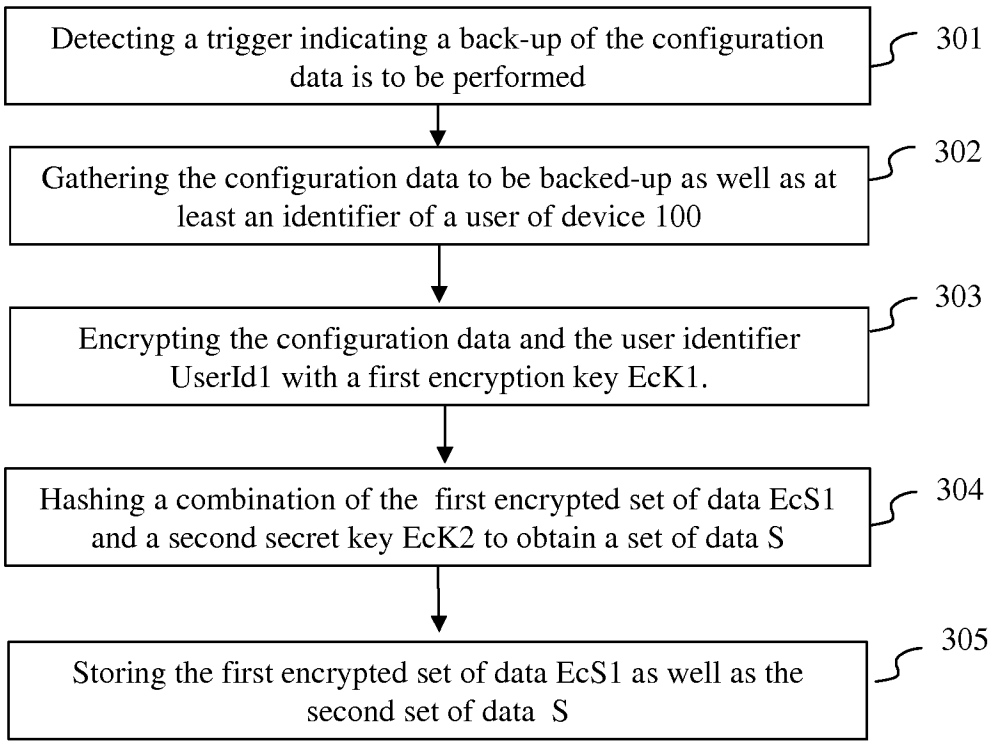

Detecting a trigger indicating a back-up of the configuration data is to be performed
301
Gathering the configuration data to be backed-up as well as at least an identifier of a user of device 100
302
Encrypting the configuration data and the user identifier UserId1 with a first encryption key EcK1.
303
Hashing a combination of the first encrypted set of data EcS1 and a second secret key EcK2 to obtain a set of data S
304
Storing the first encrypted set of data EcS1 as well as the second set of data S
305

Fig. 3

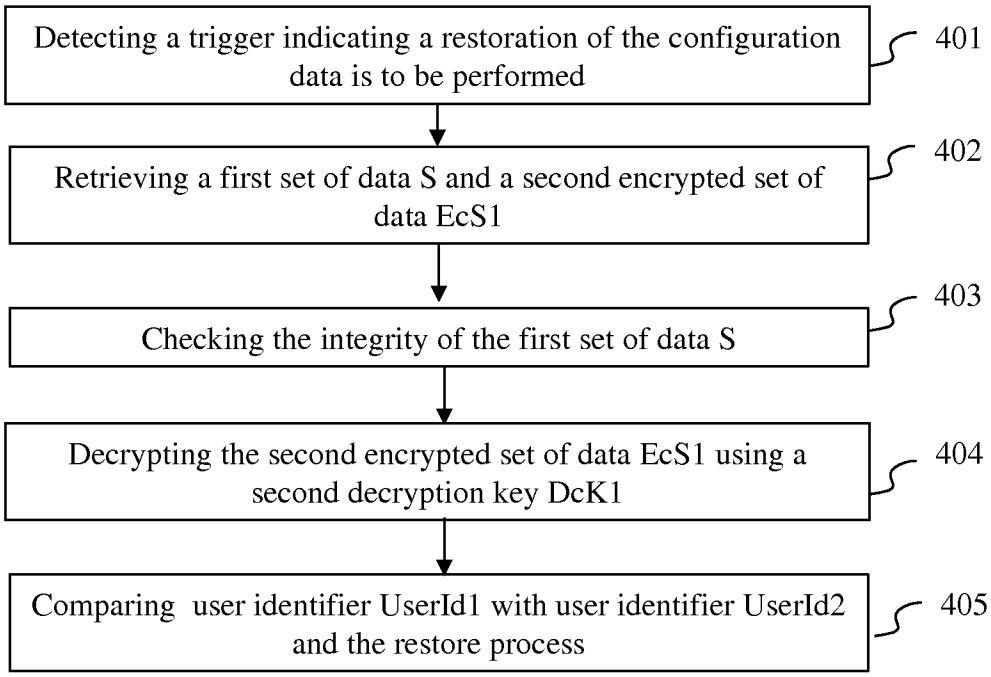

Detecting a trigger indicating a restoration of the configuration data is to be performed
401
Retrieving a first set of data S and a second encrypted set of data EcS1
402
Checking the integrity of the first set of data S
403
Decrypting the second encrypted set of data EcS1 using a second decryption key DcK1
404
Comparing user identifier UserId1 with user identifier UserId2 and the restore process
405

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/050474

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62 G06F11/14
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/189362 A1 (VAN DEN BROECK ROELAND [BE] ET AL) 3 July 2014 (2014-07-03) abstract paragraph [0028] - paragraph [0054]; claims 1-16	1-15
X	US 2005/283662 A1 (LI YI Q [US] ET AL) 22 December 2005 (2005-12-22) abstract paragraph [0014] - paragraph [0022]; claims 18, 19; figures 1-10	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 2018	05/04/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Savvides, George

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/050474

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014189362 A1	03-07-2014	AU 2012300852 A1	06-03-2014
		BR 112014004858 A2	04-04-2017
		CN 104025542 A	03-09-2014
		EP 2751970 A1	09-07-2014
		HK 1198786 A1	05-06-2015
		JP 6154378 B2	28-06-2017
		JP 2014525709 A	29-09-2014
		KR 20140061479 A	21-05-2014
		US 2014189362 A1	03-07-2014
		WO 2013030296 A1	07-03-2013
US 2005283662 A1	22-12-2005	CN 101006428 A	25-07-2007
		EP 1769355 A2	04-04-2007
		JP 2008504592 A	14-02-2008
		US 2005283662 A1	22-12-2005
		WO 2006007329 A2	19-01-2006