(12) UK Patent (19) GB (11) 2556638 (13) B

(45) Date of B Publication 12.12.2018

(54) Title of the Invention: Protecting usage of key store content

(51) INT CL: ***G06F 21/45*** (2013.01) ***G06F 21/62*** (2013.01)

(21) Application No: **1620553.6**

(22) Date of Filing: **02.12.2016**

(43) Date of A Publication **06.06.2018**

(56) Documents Cited:
WO 2006/069194 A2 **US 20070168292 A1**
US 20060242068 A1
Android Keystore System, accessed from the Internet at https://developer.android.com/training/articles/keystore.html on 03/05/2017

(58) Field of Search:
As for published application 2556638 A viz:
INT CL **G06F**
Other: **WPI, EPODOC, Internet**
updated as appropriate

Additional Fields
INT CL **H04L, H04W**

(72) Inventor(s):
Tuomas Mikael Kärkkäinen
Ossi Mikael Kalevo
Mikko Sahlbom

(73) Proprietor(s):
Gurulogic Microsystems Oy
Linnankatu 34, Turku FI-20100, Finland

(74) Agent and/or Address for Service:
Basck Ltd
16 Saxon Road, CAMBRIDGE, Cambridgeshire, CB5 8HS, United Kingdom

GB 2556638 B

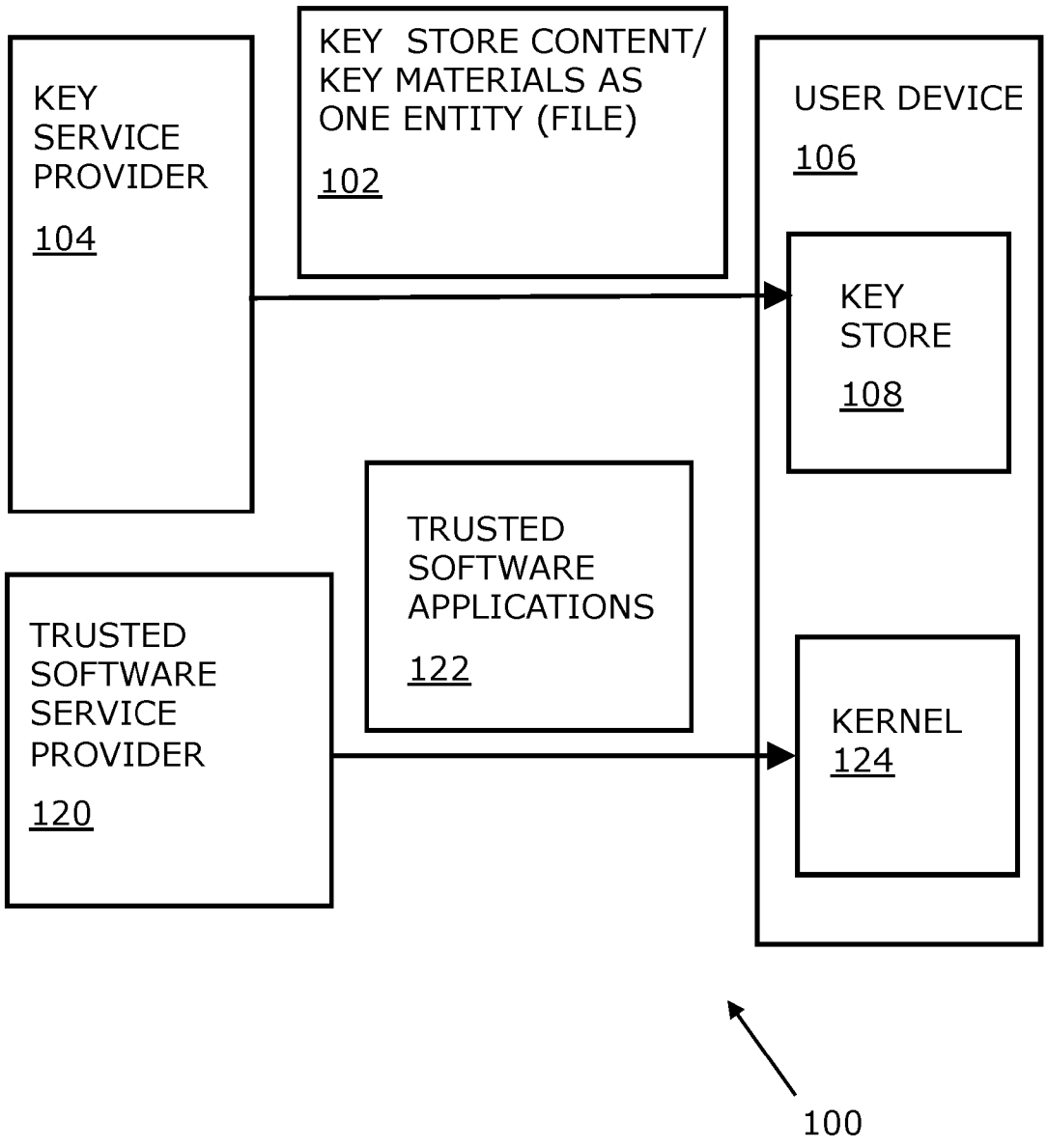
KEY SERVICE PROVIDER
104
KEY STORE CONTENT/ KEY MATERIALS AS ONE ENTITY (FILE)
102
USER DEVICE
106
KEY STORE
108
TRUSTED SOFTWARE APPLICATIONS
122
TRUSTED SOFTWARE SERVICE PROVIDER
120
KERNEL
124
100

FIG. 1

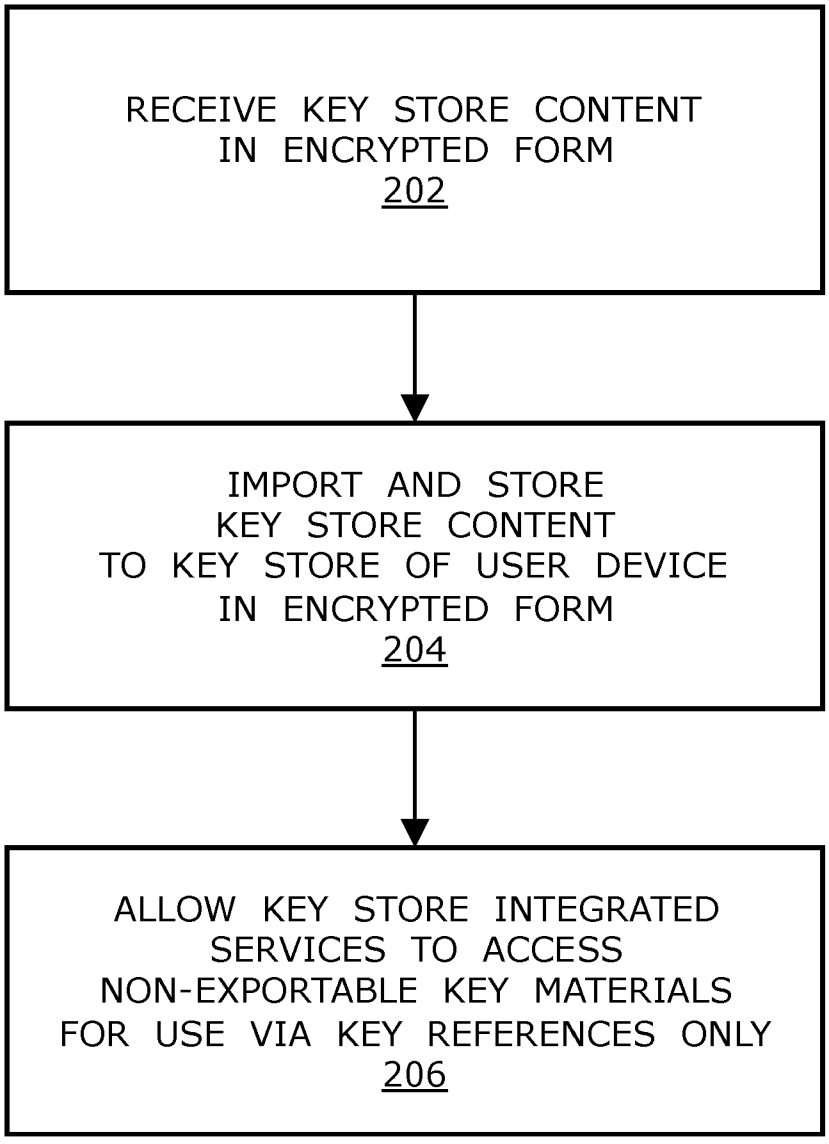
RECEIVE KEY STORE CONTENT
IN ENCRYPTED FORM
202
IMPORT AND STORE
KEY STORE CONTENT
TO KEY STORE OF USER DEVICE
IN ENCRYPTED FORM
204
ALLOW KEY STORE INTEGRATED
SERVICES TO ACCESS
NON-EXPORTABLE KEY MATERIALS
FOR USE VIA KEY REFERENCES ONLY
206

FIG. 2

PROTECTING USAGE OF KEY STORE CONTENT

TECHNICAL FIELD

The present disclosure relates to systems for protecting usage of key store content at user devices of end users, for example, to data security systems that are reliant upon using key materials to achieve data security. Moreover, the present disclosure also relates to methods of protecting usage of key store content at user devices of end users. Furthermore, the present disclosure also relates to computer program products comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the aforementioned methods.

BACKGROUND

There often arises a need to store user-sensitive data on user devices, because there are presently available various services and functionalities that are designed to run as software applications on user devices, for example software applications for making payments. As a first example, there are presently available multiple applications for banking and payment services, wherein the multiple applications require secure arrangements for maintaining strong protection for customers when using the banking and payment services in order to try to avoid malicious third parties from hacking into such services for stealing money. As a second example, a user may need to store secret or private keys to access protected e-mails. For these and many other reasons, it is very desirable to provide a robust solution for handling key store pertaining to key materials.

There are many security service providers that are accessible via multiple "*eco-system*" platforms, whose key stores are based on software. For example, the Android™ eco-system platform is contemporarily much in public focus, because there are numerous examples of mobile devices worldwide, for example tablet-like computing devices, that utilize the Android™ eco-

system platform. Referring to Google documents, the Android™ Keystore system stores cryptographic keys in a container to make it more difficult to extract from a given Android-compatible device. The Android™ Keystore system is most advanced amongst contemporarily available key store systems in security matters, but still unfortunately lacks very important functionalities needed to provide an efficient security solution in contemporary devices that are sold in large numbers in the market. The Android™ Keystore offers a substantially complete set of security algorithms, for example, such as crypto, key generator, key factory, key pair generator, mac, and signature. All of these services run inside hardware that is backed by the key store system to make it efficient and convenient to use, but there is not taken into account real world cryptographic requirements.

Moreover, in only a few years, there have recently been a huge increase in the use of mobile phones, and there are multiple vendors with different sets of device models, which are powered by different eco-systems, for example, such as Google® Android™, Apple® iOS™, Microsoft® Windows®, and so on. There arises an issue from a security perspective in that every eco-system has its own security solutions to protect user-sensitive data in hardware-based or software-based key stores. This makes it very difficult for application developers to understand security related implementations even theoretically, although it is understood at a basic level. Almost every eco-system has its own key store solution, but from a point of current urgent need, it is desired to focus on mobile platforms, because almost every human will soon have some kind of smartphone and a great amount of different applications that require properly implemented key stores for holding user-sensitive key materials inside. On paper, key stores almost fulfill any known security issues, but in reality their software implementations do not meet the solid solutions with the System on Chip (SoC) hardware design.

Firstly, the Android™ Keystore is not designed to import thousands or millions of secret keys (namely, key materials), but has been designed to maintain only a few secret keys. Secondly, the Android™ Keystore supports importing

only one plain raw key at a time, which is potentially exposed to malicious parties.

Moreover, there are some conventionally-known software-based key store solutions, from which "*Bouncy Castle*" alias "*BC*" is the most known provider. When compared to the hardware-based Android™ Keystore, BC supports key store import functionality for protected key materials in Abstract Syntax Notation One (ASN.1) format, which can import securely more than one key at a time into the key store. The main problem with BC is that, the key material is not completely protected against extraction prevention, because the key material is requested from outside of the key store and is provided to another software application that then uses the key material. This makes it possible for a malicious third party to retrieve a key material from the key store in connection with an authenticated request. In particular, the key materials are not indexed in a given BC's key store, which potentially forces revealing the sensitive key materials to malicious parties.

In a published PCT patent application WO2006069194 A2 (Fabrice Jogand-Coulomb et al; *"Memory system with versatile content control"*), there is described a method for storing data in a memory system which comprises a rewritable non-volatile memory, and a memory controller controlling access to the non-volatile memory. The method comprises:

(i) causing the controller to generate a key useful for encrypting and/or decrypting data stored in the memory by the controller, the key being substantially inaccessible to devices external to the system; and

(ii) storing in the memory a policy concerning different permissions granted to authorized entities to use the key for encrypting and/or decrypting data stored in the memory.

In a published US patent application US20070168292 A1 (Fabrice Jogand-Coulomb et al.; *"Memory system with versatile content control"*), there is described a system for storing data. The system comprises:

(i) a rewritable non-volatile memory storing data; and

(ii) a controller controlling access to the non-volatile memory;

wherein a cryptographic key is stored in the non-volatile memory or controller, the key being useful for encrypting and/or decrypting data stored in the memory by the controller, the key being substantially inaccessible to devices external to the system; and wherein the memory also stores a policy concerning different permissions granted to authorized entities to use the key for encrypting and/or decrypting data stored in the memory.

In another published US patent application US20060242068 A1 (Fabrice Jogand-Coulomb et al.; «*Method for versatile content control*"), there is described a method for storing data in a memory system which comprises a rewritable non-volatile memory, and a memory controller controlling access to the non-volatile memory. The aforesaid method comprises:

(i) causing the controller to generate a key that is useful for encrypting and/or decrypting data stored in the memory by the controller, the key being substantially inaccessible to devices external to the system; and

(ii) storing in the memory a policy concerning different permissions granted to authorized entities to use the key for encrypting and/or decrypting data stored in the memory.

SUMMARY

The present disclosure seeks to provide an improved system for protecting usage of key store content at a given user device of an end user.

Moreover, the present disclosure seeks to provide an improved method of protecting usage of key store content at a given user device of an end user.

A further aim of the present disclosure is to at least partially overcome at least some of the problems of the prior art, as discussed above.

In a first aspect, embodiments of the present disclosure provide a method of protecting usage of key store content at a given user device of an end user, characterized in that the method includes steps of:

(i) receiving, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) importing the key store content to a key store of the given user device and storing the key materials of the key store content at the key store in the encrypted form, wherein all the key materials of the key store content are imported at one go, and wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allowing one or more key store integrated services of the given user device to access the non-exportable key materials for use via key references only, wherein a given key reference is employed for referencing a key material to be used.

Embodiments of the present disclosure are of advantage in that complete protection of the key store content against unauthorized access is facilitated by employing a complete process from the key service provider to the given user device of the end user, wherein the key materials of the key store content are never exposed or treated unsafely at any step in the process, are non-exportable once stored at the key store of the given user device, and are accessible for use by the services that are integrated with the key store, via the key references only.

Optionally, the method includes, internally within the key store of the given user device, decrypting one or more of the key materials to be used by the one or more key store integrated services of the given user device.

Optionally, the method includes receiving, within the key store content, the key references for referencing the key materials.

Alternatively, optionally, the method includes generating, at the given user device, the key references for referencing the key materials upon receiving the key store content at the given user device, for example as a consecutive sequence of key references, for example at initial registration of the given user device to the key service provider.

More optionally, at the step (ii), the key store content is imported to the given user device as a single data file.

According to an embodiment of the present disclosure, the key store is hardware-based. Optionally, in such a case, the importing at (ii) includes binding the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device.

Optionally, the secure area of the processing hardware is implemented by way of dedicated hardware that is configured to disallow externally-loaded software applications or programs to operate on the dedicated hardware. More optionally, the secure area of the processing hardware is implemented by way of Trusted Execution Environment (TEE; see reference [1]).

According to an embodiment of the present disclosure, the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a Public Key Infrastructure (PKI)-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization and similar,

(d) one or more key generators for generating keys.

Moreover, according to an embodiment of the present disclosure, the method includes integrating, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device. Such integrated

software applications or ecosystem processes are referred to as "*key store integrated services*" throughout the present disclosure.

Optionally, in this regard, the method includes importing, from a trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

Furthermore, according to an embodiment of the present disclosure, the method includes encrypting the key store content, at the key service provider, using encryption key data provided by the given user device or by the key service provider.

Optionally, the method includes encrypting the key store content, at the key service provider, using a token of the end user's bio-credential. Optionally, in this regard, the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user. As an example, the facial features of the end user could be captured using a camera of the end user's device and verified against a reference template using image correlation or use of neural network algorithms. It will be appreciated that the end user's bio-credential may alternatively correspond to any other type of biometrical verification feasible in future.

Optionally, the method includes providing the end user's bio-credential to the key service provider. Optionally, the end user's bio credential is provided when importing the key store. Each time the key store is used, verification is optionally performed using the same bio-credential.

Optionally, the method includes encrypting the key store content, at the key service provider, by employing symmetric Advanced Encryption Standard

(AES; see reference [2]) encryption, for example, using a 128-bit key or a 256-bit key.

Moreover, according to an embodiment of the present disclosure, the key store content is received at (i) via unsecured transportation.

In a second aspect, embodiments of the present disclosure provide a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the method pursuant to the aforementioned first aspect.

In a third aspect, embodiments of the present disclosure provide a system for protecting usage of key store content at a given user device of an end user, characterized in that the system is operable to:

(i) receive, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) import the key store content to a key store of the given user device and store the key materials of the key store content at the key store in the encrypted form, wherein all the key materials of the key store content are imported at one go, and wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allow one or more key store integrated services of the given user device to access the non-exportable key materials for use via key references only, wherein a given key reference is employed for referencing a key material to be used.

Optionally, the system is operable to, internally within the key store of the given user device, decrypt one or more of the key materials to be used by the one or more key store integrated services of the given user device.

Optionally, the system is operable to receive, within the key store content, the key references for referencing the key materials

Alternatively, optionally, the system is operable to generate, at the given user device, the key references upon receiving the key store content at the given user device, for example as a consecutive sequence of key references, for example at initial registration of the given user device to the key service provider.

More optionally, when importing at (ii), the system is operable to import the key store content to the given user device as a single data file.

According to an embodiment of the present disclosure, the key store is hardware-based. Optionally, in such a case, when importing at (ii), the system is operable to bind the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device.

Optionally, the secure area of the processing hardware is implemented by way of dedicated hardware that is configured to disallow externally-loaded software applications or programs to operate on the dedicated hardware. More optionally, the secure area of the processing hardware is implemented by way of TEE (see reference [1]).

According to an embodiment of the present disclosure, the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a PKI-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization and similar,

(d) one or more key generators for generating keys.

Moreover, according to an embodiment of the present disclosure, the system is operable to integrate, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device.

Optionally, in this regard, the system is operable to import, from a trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

Furthermore, according to an embodiment of the present disclosure, the key service provider is operable to encrypt the key store content using encryption key data provided by the given user device or by the key service provider.

Optionally, the key service provider is operable to encrypt the key store content using a token of the end user's bio-credential. Optionally, in this regard, the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user. As an example, the facial features of the end users could be captured using a camera of the end user's device and verified against a reference template using image correlation or use of neural network algorithms.

Optionally, the key service provider is operable to encrypt the key store content by employing symmetric AES encryption (see reference [2]), for example, using a 128-bit key or a 256-bit key.

Moreover, according to an embodiment of the present disclosure, when receiving at (i), the system is operable to receive the key store content via unsecured transportation.

Additional aspects, advantages, features and objects of the present disclosure would be made apparent from the drawings and the detailed description of the illustrative embodiments construed in conjunction with the appended claims that follow.

It will be appreciated that features of the present disclosure are susceptible to being combined in various combinations without departing from the scope of the present disclosure as defined by the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The summary above, as well as the following detailed description of illustrative embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the present disclosure, exemplary constructions of the disclosure are shown in the drawings. However, the present disclosure is not limited to specific methods and apparatus disclosed herein. Moreover, those in the art will understand that the drawings are not to scale. Wherever possible, like elements have been indicated by identical numbers.

Embodiments of the present disclosure will now be described, by way of example only, with reference to the following diagrams wherein:

FIG. 1 is a schematic illustration of a system for protecting usage of key store content at a given user device of an end user, in accordance with an embodiment of the present disclosure; and

FIG. 2 is a flow chart depicting steps of a method of protecting usage of key store content at a given user device of an end user, in accordance with an embodiment of the present disclosure.

In the accompanying drawings, an underlined number is employed to represent an item over which the underlined number is positioned or an item to which the underlined number is adjacent. When a number is non-underlined and accompanied by an associated arrow, the non-underlined number is used to identify a general item at which the arrow is pointing.

DETAILED DESCRIPTION OF EMBODIMENTS

The following detailed description illustrates embodiments of the present disclosure and ways in which they can be implemented. Although some modes of carrying out the present disclosure have been disclosed, those skilled in the art would recognize that other embodiments for carrying out or practising the present disclosure are also possible.

In a first aspect, embodiments of the present disclosure provide a method of protecting usage of key store content at a given user device of an end user, characterized in that the method includes steps of:

(i) receiving, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) importing the key store content to a key store of the given user device and storing the key materials of the key store content at the key store in the encrypted form, wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allowing one or more key store integrated services of the given user device to access the non-exportable key materials for use via their corresponding key references only.

Throughout the present disclosure, the term "*end user*" encompasses a human user as well as a machine. As an example, the end user could be a registered relay machine. This is particularly beneficial for cases where the aforementioned method is used to recognize and verify servers that perform machine-to-machine communication.

Optionally, the method includes, internally within the key store of the given user device, decrypting one or more of the key materials to be used by the one or more key store integrated services of the given user device.

Optionally, the method includes receiving, within the key store content, the key references for referencing the key materials.

Alternatively, optionally, the method includes generating, at the given user device, the key references for referencing the key materials upon receiving the key store content at the given user device, for example as a consecutive sequence of key references, for example at initial registration of the given user device to the key service provider.

Pursuant to embodiments of the present disclosure, complete protection of the key store content against unauthorized access is facilitated by employing a complete process from the key service provider to the given user device of the end user, wherein the key materials of the key store content are never exposed or treated unsafely at any step in the process. The key store content is created and delivered to the given user device in encrypted form. This potentially prevents eavesdropping by third parties. At the given user device, the key store content is imported to the key store of the given user device.

At the step (ii), all the key materials of the key store content are imported at one go. More optionally, at the step (ii), the key store content is imported to the given user device as a single data file. It will be appreciated that the number of key materials included within the key store content can be as large as thousands, potentially millions. In such a case, importing the key store content as a single data file has several advantages, as compared to conventional key store techniques.

The key materials may be used for various purposes, for example, such as cryptography, signing, integrity, verification, authentication, authorization and similar. Advantageously, the key materials are made accessible for use, internally within the key store, to the key store integrated services, which access the key materials for use via their corresponding key references only.

In other words, the key materials are not accessible by software applications or ecosystem processes from outside of the key store.

Beneficially, the key references are implemented as indexes to the key materials. In other words, with a given key reference, it is known which key material is to be used, and optionally, in which location of the key store the key material to be used is located. Pursuant to embodiments of the present disclosure, the key material itself is never extracted from the key store.

In an event that a malicious party makes an attempt to use a key reference to access, evaluate or debug its corresponding key material, an exception is optionally raised. As an example, if the key store is implemented on Android™ and technical interfaces are built using Java, where a technical implementation of security solutions is mixed between Sun Microsystem®'s Java and Google Android™'s Java, the key store should support exactly required interfaces defined in Google Android™ developer's reference, so that the technical implementation may be done using already existing Java Application Programming Interface (API). However, the technical implementation of the key store does not allow to access, evaluate or debug a key material referenced by a given key reference.

In embodiments of the present disclosure, the key store content is created by the key service provider, in the aforementioned format, so as to be compliant with an import function of the key store of the given user device. Optionally, the key store content is created by the key service provider in a format that is compliant with a key-store import function of a wide spectrum of user devices; for example, the user devices employ various types of proprietary secure key stores implemented in hardware, such as aforementioned TEE, and employ a software-supported interface to provide a portal of standardized functionality presented by the secure key store to a received encrypted key store content file sent by the key service provider. Optionally, in this regard, at the key service provider, the key store content is individually customized to be compatible with various different types of user devices.

Examples of such user devices include, but are not limited to, mobile phones, smart telephones, Mobile Internet Devices (MIDs), tablet computers, Ultra-Mobile Personal Computers (UMPCs), phablet computers, Personal Digital Assistants (PDAs), web pads, Personal Computers (PCs), handheld PCs, laptop computers, desktop computers, and interactive entertainment devices, such as game consoles, Television (TV) sets and Set-Top Boxes (STBs).

Moreover, it will be appreciated that the key store of the given user device may be either hardware-based or software-based, for example implemented using hardware as in TEE ("*trusted execution environment*"), that prevents export of data therefrom after initial loading of the key store content to the key store.

According to an embodiment of the present disclosure, the key store is hardware-based. Optionally, in such a case, the importing at (ii) includes binding the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device. Subsequently, in use, key materials stored in the key store are accessed for use, via use of their references, but are not exportable from the key store. Optionally, a pointer is used to transfer a key reference of a key material to be used by a key store integrated service.

One or more trusted software applications, for example encryption algorithms and/or decryption algorithms that require use of the key materials in the key store are protected in operation by a kernel layer of the given user device. The kernel layer of the given user device, for example, is implemented in a mixture of hardware and software, and is often proprietary to the given user device, for example proprietary to a manufacturer of the given user device. The trusted software applications interface to other software applications supported in other software layers supported in operation on the given user device. Beneficially, the one or more trusted software applications are downloaded in encrypted form from a trusted software service provider. Optionally, the key service provider and the trusted software service provider are the same party. Alternatively, optionally, the key service provider and the trusted software service provider are mutually different parties.

Thus, it will be appreciated, in a given user device including a hardware-implemented key store, that there is also a kernel layer and one or more software layers hosted in the device. Software applications can be imported and then executed in the one or more software layers. Moreover, other trusted software applications provided by the trusted software service provider can be executed in the kernel layer, in which case the trusted software applications are protected by security provisions of the kernel layer that are generally more secure than the one or more software layers; the software applications protected by security provisions of the kernel layer are referred to as "*key store integrated services*" for purposes of the present disclosure. In operation, various data exchanges occur between applications supported in the one or more software layers and the "*key store integrated services*" hosted in the kernel layer.

Optionally, the secure area of the processing hardware is implemented by way of dedicated hardware that is configured to disallow externally-loaded software applications or programs, namely in the aforementioned one or more software layers, to operate on the dedicated hardware. It will be appreciated that such externally-loaded software applications or programs could be maliciously loaded by hostile third parties. More optionally, the secure area of the processing hardware is implemented by way of Trusted Execution Environment (TEE; see reference [1]), for example as aforementioned.

In this way, the method facilitates a solid and strong integration between software and security hardware of the given user device.

According to an embodiment of the present disclosure, the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a Public Key Infrastructure (PKI)-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization and similar,

(d) one or more key generators for generating keys.

Optionally, in this regard, the one or more key generators are used to generate the keys reproducibly. In other words, each time a same input is used, a same key is generated by a given key generator.

Optionally, one or more of the key materials are individually protected with additional encryption. This is particularly beneficial for certain security applications.

Moreover, according to an embodiment of the present disclosure, the method includes integrating, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device. Such integrated software applications or ecosystem processes are referred to as "*key store integrated services*" throughout the present disclosure, as aforementioned. Examples of the key store integrated services include, but are not limited to, data delivery services, content delivery services, banking services, and financial transaction services; such services typically involve encrypting and/or decrypting data using one or more keys.

Optionally, in this regard, the method includes importing, from the trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

Moreover, optionally, when the key store is hardware-based, the key store content is encrypted using symmetric encryption that is compliant with the hardware-based key store. Optionally, in this regard, the method includes encrypting the key store content, at the key service provider, by employing

symmetric Advanced Encryption Standard (AES; see reference [2]) encryption, for example, using a 128-bit key or a 256-bit key.

Alternatively, optionally, when the key store is software based, the key store content is encrypted using asymmetric encryption that is compliant with the software-based key store.

It will be appreciated here that for the given user device to be able to decrypt the encrypted key store content, the encryption credentials used during encryption must be known to the given user device. It will be appreciated that it is not relevant in embodiments of the present disclosure, which encryption algorithm or which kind of encryption credentials are used to encrypt the key store content, because different device vendors and ecosystem providers may implement multiple different security solutions, which may then be implemented by multiple different security service providers on different platforms with their own hardware-based or software-based key stores.

Moreover, according to an embodiment of the present disclosure, the method includes encrypting the key store content, at the key service provider, using encryption key data provided by the given user device or by the key service provider.

Optionally, the method includes encrypting the key store content, at the key service provider, using a token of the end user's bio-credential. Optionally, in this regard, the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user. As an example, the facial features of the end user could be captured using a camera of the end user's device and verified against a reference template using image correlation or use of neural network algorithms. It will be appreciated that the end user's bio-credential may alternatively correspond to any other type of biometrical verification feasible in the future.

Optionally, the method includes providing the end user's bio-credential to the key service provider. Optionally, the end user's bio credential is provided when importing the key store. Each time the key store is used, verification is optionally performed using the same bio-credential.

Furthermore, according to an embodiment of the present disclosure, the key store content is received at (i) via unsecured transportation. As an example, the encrypted key store content can be communicated via non-secured public Internet connection, because when properly-protected the encrypted key store content does not reveal any user-sensitive data. This is possible because the key materials are protected using encryption, and therefore, the transportation of the key materials is not necessary to be protected.

In a second aspect, embodiments of the present disclosure provide a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the method pursuant to the aforementioned first aspect.

Optionally, the computer-readable instructions are downloadable from a software application store, for example, from an "*App store*" to the computerized device.

In a third aspect, embodiments of the present disclosure provide a system for protecting usage of key store content at a given user device of an end user, characterized in that the system is operable to:

(i) receive, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) import the key store content to a key store of the given user device and store the key materials of the key store content at the key store

in the encrypted form, wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allow one or more key store integrated services of the given user device to access the non-exportable key materials for use via their corresponding key references only.

Optionally, the system is operable to, internally within the key store of the given user device, decrypt one or more of the key materials to be used by the one or more key store integrated services of the given user device.

Optionally, the system is operable to receive, within the key store content, the key references for referencing the key materials

Alternatively, optionally, the system is operable to generate, at the given user device, the key references upon receiving the key store content at the given user device, for example as a consecutive sequence of key references, for example at initial registration of the given user device to the key service provider.

When importing at (ii), the system is operable to import all the key materials of the key store content at one go. More optionally, when importing at (ii), the system is operable to import the key store content to the given user device as a single data file.

It will be appreciated here that embodiments of the present disclosure are suitable for various different types of user devices. Examples of such user devices include, but are not limited to, mobile phones, smart telephones, MIDs, tablet computers, UMPCs, phablet computers, PDAs, web pads, PCs, handheld PCs, laptop computers, desktop computers, and interactive entertainment devices, such as game consoles, TV sets and STBs.

According to an embodiment of the present disclosure, the key store is hardware-based. Optionally, in such a case, when importing at (ii), the

system is operable to bind the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device.

Optionally, the secure area of the processing hardware is implemented by way of dedicated hardware that is configured to disallow externally-loaded software applications or programs to operate on the dedicated hardware; for example software applications that are externally loaded are operable to interface via key store integrated services provided by trusted software applications that are protected by the kernel layer of the end user's device, wherein the key store integrated services shield the key store from direct access by the externally loaded software applications. It will be appreciated that such externally-loaded software applications or programs could be maliciously loaded by hostile third parties. However, it will be appreciated that the key store integrated services are implemented using trusted software applications provided from a trusted software service provider, as aforementioned. More optionally, the secure area of the processing hardware is implemented by way of TEE (see reference [1]).

According to an embodiment of the present disclosure, the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a PKI-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization and similar,

(d) one or more key generators for generating keys.

Moreover, according to an embodiment of the present disclosure, the system is operable to integrate, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device. Examples of such key store integrated services include, but are not limited to, data delivery

services, content delivery services, banking services, and financial transaction services.

Optionally, in this regard, the system is operable to import, from a trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

Furthermore, according to an embodiment of the present disclosure, the key service provider is operable to encrypt the key store content using encryption key data provided by the given user device or by the key service provider.

Optionally, the key service provider is operable to encrypt the key store content using a token of the end user's bio-credential. Optionally, in this regard, the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user. It will be appreciated that the end user's bio-credential may alternatively correspond to any other type of biometrical verification feasible in the future.

Optionally, the key service provider is operable to encrypt the key store content by employing symmetric AES encryption (see reference [2]), for example, using a 128-bit key or a 256-bit key.

Moreover, according to an embodiment of the present disclosure, when receiving at (i), the system is operable to receive the key store content via unsecured transportation.

Next, embodiments of the present disclosure will be described with reference to figures.

Referring to FIG. 1, there is provided a schematic illustration of a system **100** for protecting usage of key store content **102**, in accordance with an

embodiment of the present disclosure. The system **100** includes a key service provider **104** and a given user device **106** of an end user, wherein the key service provider **104** and the given user device **106** are coupled in communication via a data communication arrangement.

The key service provider **104** creates the key store content **102** in a format that is compatible with the given user device **106**, encrypts the key store content **102**, and sends it to the given user device **106**. Optionally, the key store content **102** is importable to the given user device **106** as a single data file.

At the given user device **106**, the key store content **102** is imported to a key store **108** of the given user device **106**, wherein the key store content **102** is stored in the encrypted form and in a manner that key materials are non-exportable from the key store **108**, and are accessible for use by key store integrated services via key references only. Optionally, the key references are included in the key store content **102**; alternatively, optionally, the key references are generated in the given user device **106** upon receipt of the key store content **102** at the given user device **106**, for example in a consecutive manner corresponding to an order in which the key materials are included in the key store content **102**.

A trusted software service provider **120** provides one or more trusted software applications **122** that are imported in encrypted form to the given user device **106**, wherein the one or more trusted software applications **122** are executable upon the given user device **106** in a manner that is protected by a kernel **124**, for example a kernel layer, of the given user device **106**. The one or more trusted software applications **122** are operable to use the key references to access the key materials of the key store **108** for various purposes, for example encryption, decryption, verification, authentication, but are prevented from divulging the key materials to other software applications that are supported in one or more software layers of the given user device **106**. As the key materials are stored in the encrypted form, the key materials are required to be decrypted prior to use.

Optionally, the trusted software service provider **120** is a same party as the key service provider **104**. Alternatively, the trusted software service provider **120** is a mutually different party to the key service provider **104**.

FIG. 1 is merely an example, which should not unduly limit the scope of the claims herein. It is to be understood that the specific designation for the system **100** is provided as an example and is not to be construed as limiting the system **100** to specific numbers, types, or arrangements of service providers and user devices; specifically, a single user device has been shown for the sake of simplicity only. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Referring next to FIG. 2, there is provided a flow chart depicting steps of a method of protecting usage of key store content at a given user device of an end user, in accordance with an embodiment of the present disclosure. The method is depicted as a collection of steps in a logical flow diagram, which represents a sequence of steps that can be implemented in hardware, software, or a combination thereof, for example as aforementioned.

At a step **202**, the key store content is received at the given user device. In accordance with the step **202**, the key store content is received in encrypted form, wherein the key store content includes key materials that are encrypted using encryption credentials of the given user device. The key store content is created by and received from a key service provider in a format that is compatible with the given user device.

At a step **204**, the key store content is imported to a key store of the given user device, and the key materials of the key store content are stored at the key store in the encrypted form. Optionally, the key store content includes key references for referencing the key materials. Alternatively, optionally, the key references are generated by the given user device upon receipt of the key store content. In accordance with the step **204**, the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store.

At a step **206**, internally within the key store of the given user device, one or more key store integrated services of the given user device are allowed to access the non-exportable key materials for use, via their corresponding key references only. As aforementioned, such integrated services are provided by executable software that is run within protection of the kernel layer, for example a kernel structure, of the given user device. Optionally, the kernel structure includes hardware, for achieving an enhanced degree of security.

The steps **202** to **206** are only illustrative and other alternatives can also be provided where one or more steps are added without departing from the scope of the claims herein.

Modifications to embodiments of the present disclosure described in the foregoing are possible without departing from the scope of the present disclosure as defined by the accompanying claims. Expressions such as "including", "comprising", "incorporating", "consisting of", "have", "is" used to describe and claim the present invention are intended to be construed in a non-exclusive manner, namely allowing for items, components or elements not explicitly described also to be present. Reference to the singular is also to be construed to relate to the plural; as an example, "*at least one of*" indicates "*one of*" in an example, and "*a plurality of*" in another example; moreover, "*two of*", and similarly "one or more" are to be construed in a likewise manner. Numerals included within parentheses in the accompanying claims are intended to assist understanding of the claims and should not be construed in any way to limit subject matter claimed by these claims.

The phrases "in an embodiment", "according to an embodiment" and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure, and may be included in more than one embodiment of the present disclosure. Importantly, such phrases do not necessarily refer to the same embodiment.

REFERENCES

[1] Trusted execution environment - Wikipedia, the free encyclopedia (accessed November 28, 2016); URL: https://en.wikipedia.org/wiki/Trusted_execution_environment

[2] Advanced Encryption Standard - Wikipedia, the free encyclopedia (accessed November 28, 2016); URL: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

CLAIMS

We claim:

1. A method of protecting usage of key store content at a given user device of an end user, characterized in that the method includes steps of:

(i) receiving, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) importing the key store content to a key store of the given user device and storing the key materials of the key store content at the key store in the encrypted form, wherein all the key materials of the key store content are imported at one go, and wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allowing one or more key store integrated services of the given user device to access the non-exportable key materials for use via key references only, wherein a given key reference is employed for referencing a key material to be used.

2. A method of claim 1, characterized in that the method includes, internally within the key store of the given user device, decrypting one or more of the key materials to be used by the one or more key store integrated services of the given user device.

3. A method of claim 1, characterized in that at the step (ii), the key store content is imported as a single data file.

4. A method of any one of claims 1 to 3, characterized in that the method includes receiving, within the key store content, the key references for referencing the key materials.

5. A method of any one of claims 1 to 3, characterized in that the method includes generating, at the given user device, the key references for referencing the key materials upon receiving the key store content at the given user device.

6. A method of any one of claims 1 to 5, characterized in that the key store is hardware-based, and the importing at (ii) includes binding the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device.

7. A method of any one claims claim 1 to 6, characterized in that the method includes integrating, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device.

8. A method of claim 7, characterized in that the method includes importing, from a trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

9. A method of any one of claims 1 to 8, characterized in that the method includes encrypting the key store content, at the key service provider, using encryption key data provided by the given user device or by the key service provider.

10. A method of any one of claims 1 to 9, characterized in that the method includes encrypting the key store content, at the key service provider, using a token of the end user's bio-credential.

11. A method of claim 10, characterized in that the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user.

12. A method of any one of claims 1 to 11, characterized in that the method includes encrypting the key store content, at the key service provider, by employing symmetric Advanced Encryption Standard (AES) encryption.

13. A method of any one of claims 1 to 12, characterized in that the key store content is received at (i) via unsecured transportation.

14. A method of any one of claims 1 to 13, characterized in that the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a Public Key Infrastructure (PKI)-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization,

(d) one or more key generators for generating keys.

15. A computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method of any one of claims 1 to 14.

16. A system for protecting usage of key store content at a given user device of an end user, characterized in that the system is operable to:

(i) receive, at the given user device, the key store content in encrypted form, the key store content including key materials that are encrypted using encryption credentials of the given user device, the key store content being created by and received from a key service provider in a format that is compatible with the given user device;

(ii) import the key store content to a key store of the given user device and store the key materials of the key store content at the key store in the encrypted form, wherein all the key materials of the key store content are imported at one go, and wherein the key store content is stored at the key store in a manner that the key materials are non-exportable from the key store; and

(iii) internally within the key store of the given user device, allow one or more key store integrated services of the given user device to access the non-exportable key materials for use via key references only, wherein a given key reference is employed for referencing a key material to be used.

17. A system of claim 16, characterized in that the system is operable to, internally within the key store of the given user device, decrypt one or more of the key materials to be used by the one or more key store integrated services of the given user device.

18. A system of claim 16, characterized in that when importing at (ii), the system is operable to import the key store content as a single data file.

19. A system of any one of claims 16 to 18, characterized in that the system is operable to receive, within the key store content, the key references for referencing the key materials.

20. A system of any one of claims 16 to 18, characterized in that the system is operable to generate, at the given user device, the key references for referencing the key materials upon receiving the key store content at the given user device.

21. A system of any one of claims 16 to 20, characterized in that the key store is hardware-based, and when importing at (ii), the system is operable to bind the key materials stored at the hardware-based key store to a secure area of processing hardware of the given user device.

22. A system of any one of claims 16 to 21, characterized in that the system is operable to integrate, with the key store, one or more trusted software applications or ecosystem processes hosted at the given user device that are authorized to use the key store of the given user device.

23. A system of claim 22, characterized in that the system is operable to import, from a trusted software service provider, the one or more trusted software applications for providing key store integrated services, wherein the one or more trusted software applications when executed at the given user device are operable to provide one or more key store integrated services and are provided with protection from a kernel of the given user device.

24. A system of any one of claims 16 to 23, characterized in that the key service provider is operable to encrypt the key store content using encryption key data provided by the given user device or by the key service provider.

25. A system of any one of claims 16 to 24, characterized in that the key service provider is operable to encrypt the key store content using a token of the end user's bio-credential.

26. A system of claim 25, characterized in that the end user's bio-credential includes at least one of: a fingerprint of the end user, facial features of the end user, a DNA profile of the end user, iris recognition of the end user, a walking manner of the end user, a writing manner of the end user, a heartbeat pattern of the end user.

27. A system of any one of claims 16 to 26, characterized in that the key service provider is operable to encrypt the key store content by employing symmetric Advanced Encryption Standard (AES) encryption.

28. A system of any one of claims 16 to 27, characterized in that when receiving at (i), the system is operable to receive the key store content via unsecured transportation.

29. A system of any one of claims 16 to 28, characterized in that the key materials include at least one of:

(a) secret keys for symmetric data encryption,

(b) private keys and public keys for a Public Key Infrastructure (PKI)-equivalent usage,

(c) certificates to be used for cryptography, signing, integrity, verification, authentication, authorization,

(d) one or more key generators for generating keys.