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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2017 (06.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/114602 A1

(51) International Patent Classification:
G06Q 20/34 (2012.01)

(21) International Application Number:
PCT/EP2016/068449

(22) International Filing Date:
2 August 2016 (02.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201511030882.7 31 December 2015 (31.12.2015) CN

(71) Applicant: **GEMALTO SA** [FR/FR]; 6, Rue de la Verrerie, 92190 Meudon (FR).

(72) Inventors: **MU, Hongyu**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). **JIANG, Qicong**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). **QIAO, Lingfeng**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). **ZHOU, Song**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR).

(74) Agent: **LOTAUT, Yacine**; Gemalto SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 Meudon (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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.

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR MONITORING THE NUMBER OF DOWNLOADING OF AN APPLICATION

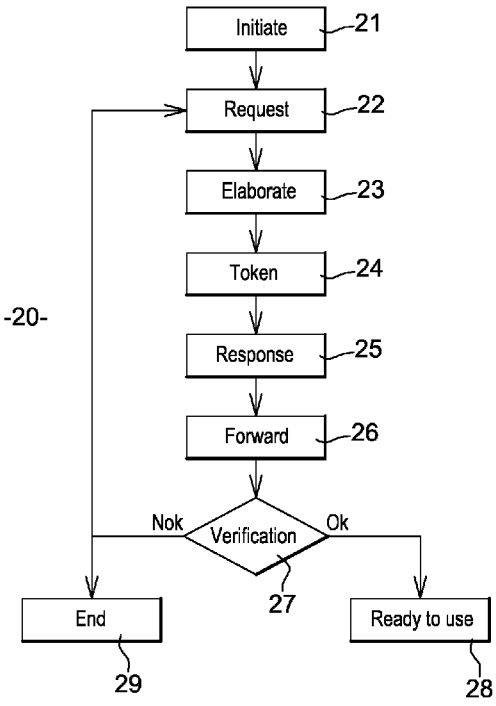

Fig. 2

(57) Abstract: The present invention relates generally to the field of controlling by an application provider through a third party, via cryptographic techniques, the number of download of an application into an electronic device. This invention concerns a method and system for monitoring by an application provider a download of an application into an electronic device via a third party, wherein - during installation of the application into the electronic device, the third party being operated to send to the application provider an authorization request message to request from the application provider the authorization to put the application in a ready to use state, - the application provider being operated: - to generate a token from the data of the authorization request message, - to increment a counter for each token generated, - to send as response to the third party request the generated token, - the application being operated to verify the authenticity of the token forwarded by the third party and to set up the application in a ready to use state when the authentication verification is successful. The counter value is used by the application provider as a basis for calculating the fee to be paid by the third party.

WO 2017/114602 A1

(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).

Published:

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

METHOD AND APPARATUS FOR MONITORING THE NUMBER OF DOWNLOADING OF AN APPLICATION

TECHNICAL FIELD

The present invention relates generally to the field of controlling by an application provider through a third party, via cryptographic techniques, the number of download of an application into an electronic device.

Particularly, the present invention relates to a method and system for monitoring the download of application onto a smart card via a third party.

BACKGROUND ART

The term "smart card" refers generally to wallet-sized or smaller cards incorporating a microprocessor or microcontroller to store and manage data within the card. More complex than magnetic-stripe and stored-value cards, smart cards are characterized by sophisticated memory management and security features. A typical smart card includes a microcontroller embedded within the card plastic which is electrically connected to an array of external contacts provided on the card exterior. A smart card microcontroller generally includes an electrically-erasable and programmable read-only memory (EEPROM) for storing user data, random access memory (RAM) for scratch storage, and read only memory (ROM) for storing the card operating system. Relatively simple microcontrollers are adequate to control these functions.

The card can interface with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance.

Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, including applications such as stored-value; credit/debit; loyalty programs, etc.

Prior to issuance of a smart card to a card user, the smart card is initialized such that some data is placed in the card. For example, during initialization, the smart card may be loaded with at least one application, such as credit or stored cash value, a file structure initialized with default values, and some initial cryptographic keys for transport security. Once a card is initialized, it is typically personalized. During personalization, the smart card is loaded with data which uniquely identifies the card. For example, the personalization data can include a maximum value of the card, a personal identification number (PIN), the currency in which the card is valid, the expiration date of the card, and cryptographic keys for the card. Once the

applications are loaded on the card and when the personalization is done, the card is ready to use and can be distribute to end users.

In traditional systems, a sole card provider (such a card manufacturer, MNO, Bank card issuer…) is able to closely control content, application and personalization data loaded into the smart cards. Charging and billing for such loaded data into the smart card is therefore relatively easy since the single card provider typically maintains control over all aspects of loading data into the smart card.

Under new system models, however, smart card environments have been developed that allow new application and personalization data to be downloaded onto smart cards by a variety of parties. Therefore, content data, personalization data and even services or applications may be provided by different third party companies other than the main card provider. Such third-party provider may utilize system resources that are not provided or maintained by the third-party provider, but rather by the main card provider.

When data (application, personalization data…) provided by the third-party provider is downloaded into the smart card, the third-party provider usually wants to collect money for this data. Currently, to collect a fee, the third-party provider has to setup a relationship with the card provider loading the third party data. The card provider pays a royalty to the third-party provider, and makes the third party data available to the cards provided by the card provider.

This service method is lacking because the third-party provider must setup a relationship with multiple card providers if they want their third party dada made available into the cards. Moreover, because the third-party provider does not necessarily control the distribution and usage of his data, the third-party provider may not be able to monitor such usage, and charge fees for the distribution and use of his third party data.

What is needed, therefore, is a system that allows a third party provider to charge and collect usage fees based on each download of third party data into each smart card through the card provider.

SUMMARY OF THE INVENTION

The following summary of the invention is provided in order to provide a basic understanding of some aspects and features of the invention. This summary is not an extensive overview of the invention and as such it is not intended to particularly identify key or critical elements of the invention or to delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented below.

The present invention addresses the aforementioned security drawbacks of monitoring the number of times an application provided by an application provider is downloaded into third party electronic device. In an embodiment, the electronic device is a smart card, however, the electronic device can be virtually any device capable of receiving digital information, for example a personal digital assistant (PDA) or a smartphone.

In accordance with further aspects of the present invention, the application provider delegates the download of the application to a third party. The present invention provides techniques to the application provider to monitor this delegated downloading.

In an embodiment, during installation of the application onto the electronic device and just before being in a ready to use state, the third party send a request to complete the installation to the application provider. The application provider generates a token and sends it as response to the third party. The token may be a cryptogram generated by the application provider using cryptographic scheme established between the application provider and the application. This token is then made available to the application, who may then test the cryptogram to determine whether the token is an authenticated one or not. If the token is authenticated, the application put its state into ready to use otherwise the installation is not completed.

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method for monitoring by an application provider a download of an application into an electronic device via a third party, wherein

- during installation of the application into the electronic device, the third party being operated to send to the application provider an authorization request message to request from the application provider the authorization to put the application in a ready to use state,
- the application provider being operated:
- to generate a token from the data of the authorization request message,
- to increment a counter for each token generated,
- to send as response to the third party request the generated token,
- the application being operated to verify the authenticity of the token forwarded by the third party and to set up the application in a ready to use state when the authentication verification is successful.

According an embodiment of the present invention, the authorization request message is sent by the third party to the application provider when the installation of the application is complete and before the application is set up in a ready to use state.

According an embodiment of the present invention, the third party sends the authorization request message to the application provider when said third party receives a token request from the application.

According an embodiment of the present invention, the authorization request message comprises a monitoring data used by the application provider to generate the token.

According an embodiment of the present invention, the monitoring data is a serial number of the electronic device, a hardware identifier of components of the electronic device, a PUF value generated with a physically unclonable function (PUF) circuit, a personalization data related to the holder of the electronic device, and/or a timing information.

According an embodiment of the present invention, the application provider generates the token by encoding the received monitoring data with a cryptographic key according to a particular cryptographic scheme implemented between the application provider and the application.

According an embodiment of the present invention, the particular cryptographic scheme is a cryptographic signature algorithm, a symmetric key encryption algorithm, and/or an integrity algorithm.

According an embodiment of the present invention, the application being operated to setup the verification of the authenticity of the received token from the third party, according to the particular cryptographic scheme implemented between the application provider and the application.

According an embodiment of the present invention, when the verification of the authenticity of the token is unsuccessful, the application being operated to end the loading process, resend a token request to the third party or delete the application already installed.

According an embodiment of the present invention, the electronic device is a smart card.

The present invention also relates to a system for monitoring by an application provider a download of a provided application into an electronic device via a third party, wherein

- during installation of the application into the electronic device, the third party being operated to send to the application provider an authorization request message to request from the application provider the authorization to put the application in a ready to use state,

- the application provider being operated:

  - to generate a token from the data of the authorization request message,

- to increment a counter for each token generated,
- to send as response to the third party request the generated token,
- the application being operated to verify the authenticity of the token forwarded by the third party and to set up the application in a ready to use state when the authentication verification is successful.

The foregoing is a summary and thus may contain simplifications, generalizations, and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting.

For a better understanding of the embodiments, together with other and further features and advantages thereof, reference is made to the following description, taken in conjunction with the accompanying drawings. The scope of the invention will be pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The following detailed description will be better understood with the drawings, in which:

FIG. 1 illustrates the different entities involved in a monitoring of a downloading application.

FIG. 2 is a logic flow diagram in accordance with an exemplary embodiment of this invention during the monitoring of a downloading application via a third party.

DETAILED DESCRIPTION OF THE EMBODIMENTS OF THE INVENTION

It will be readily understood that the components of the embodiments, as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations in addition to the described example embodiments. Thus, the following more detailed description of the example embodiments, as represented in the figures, is not intended to limit the scope of the embodiments, as claimed, but is merely representative of example embodiments.

Reference throughout the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with an embodiment is included in at least one embodiment of the subject matter disclosed. Thus, the appearance of the phrases "in one embodiment" or "in an embodiment" in various places throughout the specification is not necessarily referring to the same embodiment. Further, the particular features, structures or characteristics may be combined in any suitable manner in one or more embodiments.

As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises” and/or “comprising,” when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

In the following description, numerous specific details are provided to give a thorough understanding of embodiments. One skilled in the relevant art will recognize, however, that the various embodiments can be practiced without one or more of the specific details, or with other methods, components, materials, et cetera. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obfuscation.

The present invention is not specific to any particular hardware or software implementation, and is at a conceptual level above specifics of implementation. It is to be understood that various other embodiments and variations of the invention may be produced without departing from the spirit or scope of the invention. The following is provided to assist in understanding the practical implementation of particular embodiments of the invention.

The same elements have been designated with the same referenced numerals in the different drawings. For clarity, only those elements and steps which are useful to the understanding of the present invention have been shown in the drawings and will be described.

Further, the mechanisms of data communication between the parties and their environment have not been detailed either, the present invention being here again compatible with usual mechanisms.

Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternatives or additional functional relationships or physical connections may be present in a practical system. Furthermore, the various entities in FIG. 1 to FIG. 2 may communicate via any suitable communication medium (including the Internet), using any suitable communication protocol.

The applications and/or data can be downloaded to the electronic device in accordance with the present invention. The present invention not only applies to the download of information, but to the updating and deleting of information as well. A variety of software environments may be appropriate in this context, including, for

example, the object-oriented Java programming language or a Windows environment.

Prior to discussing the details of some embodiments of the present invention, description of some terms may be helpful in understanding the various embodiments.

A "key" may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation. A cryptographic algorithm can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc.

A “personalization data” is data linked to the holder of the electronic device. The personalization data may be secret keys, a secret code, for instance. The secret code, may be PIN CODE (for Personal Identification Number CODE) enables the legitimate user to be identified. In the case of a bank card, requesting the user to give his/her secret code prior to a transaction is a common practice, in order to make sure he/she is entitled to request said transaction.

An “application” as used herein is intended to refer to a portable segment of software code. The application can be in the form of one or more suitable programming languages, which are converted to machine language or object code to allow the processor or processors to execute the instructions. The application software can be in the form of a standalone application, implemented in a suitable programming language or framework.

Details of some embodiments of the present invention will now be described.

The present invention is described herein in terms of functional block components and various processing steps. In an embodiment, such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit components, e.g., memory elements, digital signal processing elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. In addition, those skilled in the art will appreciate that the present invention may be practiced in any number of data communication contexts and that the various systems described herein are merely exemplary applications for various aspects of the invention.

The techniques described herein can be used with an electronic device which can be a mobile or other device, such as a smartphone, smart watch, smart glasses, smart card, tablet computer, desktop computer, portable computer, television,

gaming device, music player, mobile telephone, laptop, palmtop, smart or dumb terminal, network computer, personal digital assistant, wireless device, information appliance, workstation, minicomputer, mainframe computer, or other computing device that is operated as a general purpose computer or a special purpose hardware device that can execute the functionality described herein.

The electronic device can include one or more processors suitable for the execution of an application, including both general and special purpose microprocessors. Generally, a processor receives instructions and data stored on a read-only memory or a random access memory or both. Information carriers suitable for embodying the application instructions and data include all forms of non-volatile memory. One or more memories can store instructions that, when executed by a processor, form the modules and other components described herein and perform the functionality associated with the components. The processor and the memory can be supplemented by, or incorporated in special purpose logic circuitry.

In the example of implementation described hereinafter, the present invention provide techniques for controlling the downloading of an application onto a smart card.

As illustrated in the example of FIG. 1, a third party 10 may establish the policies that control an electronic device 11 product management system, and therefore have a significant influence over the overall electronic device management scheme. The third party is an electronic device issuer. In the implementation described herein after, the third party 10 is a card issuer and the electronic device 11 is a smart card. The third party 10 may also own the smart card and be legally responsible for it.

An application provider(s) 12 may develop and own one or more applications 15, and may be legally and technically responsible for them. The application provider 12 establishes business relationships with one or more third party 10, which will put the application provider's application on their cards. The application provider 12 may be a bank card provider, a smart card issuer, a smart card manufacturer, a MNO and/or the like.

A certificate authority (not shown) may generate, manage, and administer public key certificates for both the application 15 provided by the application provider 12 and the application provider 12. The certificate authority may be an external service provider for the application provider 12. In an embodiment, the application provider 12 may be responsible for issuing its own certificates.

Referring to FIG. 1, the application provider 12 delegates to the third party 10 the task of downloading his application onto the electronic device 11. The electronic device 11 is suitably interfaced with the third party 10 using a contact or contactless

communication protocol 13. The third party 10 and the application provider 12 are suitably connected to a network 14 such Internet.

During the deployment of the application 15, the application may go through various states before it is actually ready to be used by a final user. The states which may be of interest in the context of the present invention are Loaded, Installed, and Personalized states:

- The Loaded state indicates that the application has been loaded onto the electronic device 11;
- The Installed state indicates that the loaded application has been instantiated on the card, but the personalization data of the application has not yet been initialized;
- The Personalized state indicates that the installed application has been initialized, personalization data of the application having been set up with particular values;
- The ready to use state indicating the installation and the personalization phase are completed.

The Personalized state may be an optional state. There are applications that have no personalization data and which thus become fully operational once the installation has been performed, i.e. while still in the Installed state, while others applications require a personalization of their data before becoming fully operational.

The monitoring method of the present invention is performed by the application 15 before the ready to use state is set up and after the installation and the personalization phase are completed.

The deployment of the application 15 may occur in a variety of ways. The application 15 may be pre-installed on the electronic device 11 during manufacturing or by the third party, or by a user downloading the application from an application store or from an issuer or a service provider.

In the implementation hereinafter described, the application 15 may comprise a package 16 containing mandatory components corresponding to at least one application, and a custom component 17 corresponding to information required to personalize the said at least one application. When the application 15 is loaded into the electronic device, the application is installed from the said loaded package. The application 15 may be personalized (if needed) as soon as the said application is in the Installed state at the end of the completion of the said step of installing.

Of course the term loading or downloading can refer to the loading of new application, the updating of existing application or the deletion of existing application.

FIG. 2 illustrates a diagram flow 20 of monitoring by the application provider 12 the downloading of the application 15 onto the electronic device 11 through the

third party 10. In an embodiment, the monitoring process may be initiated, in step 21, when the loading of the application 15 is at the step to terminate the installation making the application fully operational, i.e. just before the ready to use state.

It should be noted that the monitoring process may be initiated before or during the installation of the application 15 but only before the application 15 is set up in ready to use state.

In step 22, when the monitoring process is initiated, a termination request status may be set up by the application 15. In an embodiment, the loading of the application 15 remains in this termination request status until the third party 10 sends to the application 15 through the communication protocol 13 an authorization for use (token). In another embodiment, when the termination request status is set up the application 15 may send to the third party 10 a request for the token through the communication protocol 13.

In step 23, when the termination request status is set up, the third party 10 may determine a monitoring data to send to the application provider 12 to monitor the download of the application.

In an embodiment, the monitoring data may be hardware characteristics of the electronic device 11. The hardware characteristic may be a serial number or other assigned hardware identifier of components of the electronic device 11. This monitoring data may be generated by the third party 10 or provided to the third party 10 by the manufacturer of the electronic device 11 or by the electronic device 11 itself upon request.

In an embodiment, the monitoring data may be a PUF value generated with a physically unclonable function (PUF) circuit. PUFs are functions that are derived from the inherently random, physical characteristics of the electronic device 11 in which they are built. For example, a silicon PUF may exploit variations in the delay through interconnects and gates or slight differences in threshold voltage. Since the PUF exploits physical variations of the device or material in which it is built, each PUF should provide a unique (although perhaps noisy) response. This monitoring data may be provided to the third party by the manufacturer of the electronic device or by the electronic device itself upon request.

In an embodiment, the monitoring data may be the personalization data loaded into the application 15 during the personalization phase.

In an embodiment the monitoring data may be a timing information (e.g., such as timestamps, sequence numbers, or the like). The timing information may be used for any suitable purpose, such as stamping the monitoring data with a capture time or interval. The timing information may be generated by the third party or the electronic device 11 upon request.

Of course these examples of monitoring data are merely examples, various kind of may be used such as an identifier of the CPU, sensors identifiers or any combination thereof etc.

In a preferred embodiment, the monitoring data may be retrieved, during the verification step 27, by the electronic device 11 from previously storage or generated when needed.

The third party 10 may generate an authorization request message to request from the application provider 12 the authorization to put the application 15 in a ready state to use. The authorization request message comprises the monitoring data. The authorization request message is sent by the third party 10 to the application provider 12.

In step 24, the application provider 12 generates a token by encoding (enciphering) the received monitoring data with a cryptographic key. The encoding algorithm is a predetermined mathematical operation established between the application provider 12 and the application 15. The recipient of the token (the application 15) may perform a complimentary mathematical operation to unencode (decipher) the token. The enciphering and deciphering of the token is performed utilizing the cryptographic key determined by the particular cryptographic scheme implemented between the correspondents. Consequently, there are certain parameters that must be known beforehand between the correspondents, for example, in public key or symmetric key systems. In all of these schemes, it is assumed that the cryptographic keys, be it the private key, the public key or the symmetric key, is derived and valid as specified in the protocol scheme.

In an embodiment, the cryptographic key is a private key of a certificate provided by the certificate authority. The certificate may be the application provider certificate or the application certificate. Token may be a digital signature provided by a conventional cryptographic signature receiving as inputs the monitoring data and the private key. In an embodiment, the conventional cryptographic signature may be a "one way" hashing function to transform the monitoring data into a form which is unintelligible. A "hashing" function as used is a function which can be applied to an aggregation of data to create a smaller, more easily processed aggregation of data. The signature has a fixed-size set of bits that serves as a unique “digital fingerprint” for the original monitoring data. If the original monitoring data is changed and hashed again, it has a very high probability of producing a different digest. Thus, hash functions can be used to detect altered and forged monitoring data. They provide message integrity, assuring that the monitoring data has not been altered or corrupted. Any conventional cryptographic signature methodology may be employed to generate the token referenced herein.

In an embodiment, the cryptographic key is a secret embedded into the application 15, for example stored as hardcoded data into the application code and onto the application provider side. In an embodiment, the encoding algorithm may be a symmetric key encryption algorithm receiving as inputs the monitoring data and the secret key and generating the token. The symmetric key encryption may include block cipher algorithms, such as the Data Encryption Standard (DES) based algorithm(s) and Advanced Encryption Standard (AES) based algorithm(s), and stream cipher algorithms, such as RC4.

In another embodiment, the encoding algorithm is an integrity algorithm. The integrity algorithm may be a hash algorithm or any suitable algorithm that may be, for example, one version of a cyclic redundancy check (CRC) algorithm, message-digest (MD) algorithm, or secure hash algorithm (SHA). The integrity algorithm receives as inputs the monitoring data and the secret key and generates the token as output.

In an embodiment, after, the monitoring data is hashed, a signature function may be applied to the generated hash to produce a signature. To produce such signature, the signature function may be any one of a number of known techniques such as: SHA-1, MD5 MAC. In this implementation, the token comprises the hash and the signature.

In another embodiment, after the monitoring data is hashed, the digest may then be encrypted using an asymmetric key cryptography scheme. The digest may be locked with a lock having two key slots opened by different (“asymmetrical”) keys. A first key (called the “private” key) is used to lock the lock. A second (different) key (called the “public” key) must be used to open the lock once the lock has been locked with the first key. The encryption algorithm and key length is selected so that it is computationally infeasible to calculate first key given access to second key, the public key encryption algorithm, the clear text digest, and the encrypted digital signature. There are many potential candidate algorithms for this type of asymmetric key cryptography (e.g., RSA, DSA, El Gamal, Elliptic Curve Encryption). In this implementation, the token comprises the digest and the encrypted digest.

A counter (not shown) is provided for each application 15 and implemented within the application provider 12. The counter value associated with is incremented by one for each token generated. The counter value is used as a basis for calculating the fee to be paid to the application provider by the third party 10. The calculation of the fees may be based on any calculation formula; the fee may be simply proportional to the counter value, or a certain fee may be paid when a predetermined counter value is exceeded.

In step 25, in response to the received authorization request, the application provider 12 sends to the third party 10 the generated token. In step 26, the

application provider 12 forwards a command to the electronic device 11 to terminate the installation. The termination command may comprise the token. In an embodiment, if the electronic device 11 is not able to retrieve by itself the monitoring data and provide it to the application 15, the termination command may comprise also the monitoring data used to generate the token.

In step 27, once the termination command is received, the application 15 setup a verification step of the received token according to the particular cryptographic scheme implemented between the application provider 12 and the application 15. The application 15 executes the operation to unencode (decipher) the token. The application 15 tests then the received token against an expected result based upon any suitable cryptographic scheme, such as, for example, based on a known key (in the case of a symmetrical algorithm) or plurality of keys (in the case of an asymmetrical algorithm).

If the token generated is a signature computed with a certificate private key according a PKI signature scheme, the application 15 with the retrieve monitoring data, the public key of the certificate is able to authenticate the token.

The verification of the authenticity of the token is not described further because well-known and depend about the particular cryptographic scheme implemented between the application provider 12 and the application 15 for which some examples are described above.

When the authenticity of the received token is verified by the application 15, in step 28, the installation of the application 15 is terminated and the application 15 is put in ready to use state. In an embodiment, the received token may be stored into the electronic device for next deletion and installation of the application 15. In another embodiment, for each re-installation of the application 15, a new token is requested by the application 15. The generation for a new token during a re-installation or using the received old token will depend about the implementation and the charging fee process of the application provided.

In step 29, when the application 15 cannot verify the authenticity of the token received (i.e., when the signature, the digest and/or the decrypted data does not correspond to the expected data), the application 15 may end the loading process, or re-set up the termination request status in step 22, or delete the installation package 16.

It should be understood that the exemplary process illustrated may include more or less steps or may be performed in the context of a larger processing scheme. Furthermore, the flowchart presented in the drawing figure are not to be construed as limiting the order in which the individual process steps may be performed.

As mentioned above, the present invention is particularly advantageous in the context of so-called smart card environments which allow multiple parties to download applets onto a card. The present invention is not so limited, however, and may also be employed in non-smart card environments, for example, PDAs and cell phones, etc. That is, a downloaded and installed application may be put in the status ready to use based on transfer of information from an information owner to an information device, wherein the information device receives a digitally computed token from the information owner in response to a third party request. Furthermore, a counter is incremented at each generated token.

The features and functions of the implementations illustrated by the figures can be arranged in various combinations and permutations, and all are considered to be within the scope of the disclosed invention. Accordingly, the described implementations are to be considered in all respects as illustrative and not restrictive. The configurations, materials, and dimensions described herein are also intended as illustrative and in no way limiting. Similarly, although physical explanations have been provided for explanatory purposes, there is no intent to be bound by any particular theory or mechanism, or to limit the claims in accordance therewith.

The terms and expressions employed herein are used as terms and expressions of description and not of limitation, and there is no intention, in the use of such terms and expressions, of excluding any equivalents of the features shown and described or portions thereof. In addition, having described certain implementations in the present disclosure, it will be apparent to those of ordinary skill in the art that other implementations incorporating the concepts disclosed herein can be used without departing from the spirit and scope of the invention.

CLAIMS

1. A method for monitoring by an application provider a download of an application into an electronic device via a third party, wherein

- during installation of the application into the electronic device, the third party being operated to send to the application provider an authorization request message to request from the application provider the authorization to put the application in a ready to use state,

- the application provider being operated:

  - to generate a token from the data of the authorization request message,

  - to increment a counter for each token generated,

  - to send as response to the third party request the generated token,

- the application being operated to verify the authenticity of the token forwarded by the third party and to set up the application in a ready to use state when the authentication verification is successful.

2. The method according to the previous claims, wherein the authorization request message is sent by the third party to the application provider when the installation of the application is complete and before the application is set up in a ready to use state.

3. The method according to any previous claims, wherein the third party sends the authorization request message to the application provider when said third party receives a token request from the application.

4. The method according to any previous claims, wherein the authorization request message comprises a monitoring data used by the application provider to generate the token.

5. The method according to the previous claim, wherein the monitoring data is a serial number of the electronic device, a hardware identifier of components of the electronic device, a PUF value generated with a physically unclonable function (PUF) circuit, a personalization data related to the holder of the electronic device, and/or a timing information.

The method according to the previous claims 4 to 5, wherein the application provider generates the token by encoding the received monitoring data with a

cryptographic key according to a particular cryptographic scheme implemented between the application provider and the application.

6. The method according to the previous claim 6, wherein the particular cryptographic scheme is a cryptographic signature algorithm, a symmetric key encryption algorithm, and/or an integrity algorithm.

7. The method according to the previous claim 6, wherein the application being operated to setup the verification of the authenticity of the received token from the third party, according to the particular cryptographic scheme implemented between the application provider and the application.

8. The method according to any previous claims, wherein when the verification of the authenticity of the token is unsuccessful, the application being operated to end the loading process, resend a token request to the third party or delete the application already installed.

9. The method according to any previous claims, wherein the electronic device is a smart card.

10. A system for monitoring by an application provider a download of a provided application into an electronic device via a third party, wherein

- during installation of the application into the electronic device, the third party being operated to send to the application provider an authorization request message to request from the application provider the authorization to put the application in a ready to use state,
- the application provider being operated:
  - to generate a token from the data of the authorization request message,
  - to increment a counter for each token generated,
  - to send as response to the third party request the generated token,
- the application being operated to verify the authenticity of the token forwarded by the third party and to set up the application in a ready to use state when the authentication verification is successful.

11. The system according to the previous claim, wherein the authorization request message is sent by the third party to the application provider when the

installation of the application is complete and before the application is set up in a ready to use state.

12. The system according to any of the previous claims 10 and 11, wherein the third party sends the authorization request message to the application provider when said third party receives a token request from the application, said authorization request message comprising a monitoring data used by the application provider to generate the token.

13. The system according to the previous claim, wherein the monitoring data is a serial number of the electronic device, a hardware identifier of components of the electronic device, a PUF value generated with a physically unclonable function (PUF) circuit, a personalization data related to the holder of the electronic device, and/or a timing information.

14. The system according to any of the previous claims 12 to 13, wherein the application provider generates the token by encoding the received monitoring data with a cryptographic key according to a particular cryptographic scheme implemented between the application provider and the application.

15. The system according to the previous claim 6, wherein the particular cryptographic scheme is a cryptographic signature algorithm, a symmetric key encryption algorithm, and/or an integrity algorithm.

16. The system according to any previous claims, wherein when the verification of the authenticity of the token is unsuccessful, the application being operated to end the loading process, resend a token request to the third party or delete the application already installed.

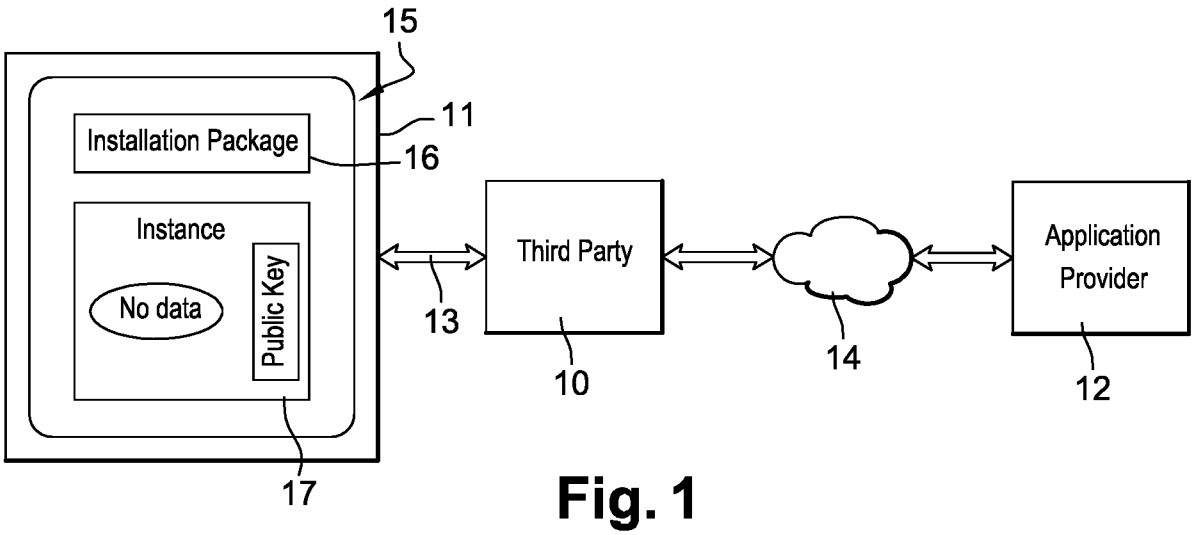
15
11
Installation Package
16
Instance
No data
Public Key
17
13
Third Party
10
14
Application Provider
12

Fig. 1

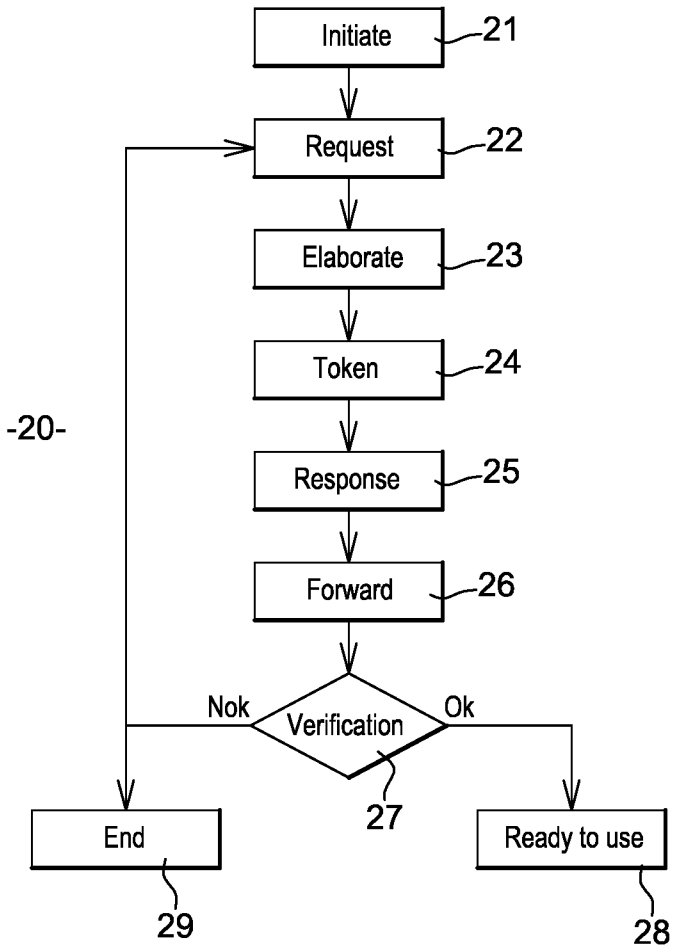
-20-
Initiate
21
Request
22
Elaborate
23
Token
24
Response
25
Forward
26
Nok
Verification
Ok
27
End
29
Ready to use
28

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/068449

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/34
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)
G06Q

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Global Platform: "Open Platform Card Specification", , 7 April 2000 (2000-04-07), XP055305434, Retrieved from the Internet: URL:https://www.informatik.uni-augsburg.de/lehrstuehle/swt/se/teaching/fruehere_semester/ws0708/javacard/Dokumentation/Card-Specification.pdf [retrieved on 2016-09-26] Chapters 4 and 6, sections 4.2.2 and section 6.8 -----	1-16

☐ 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
29 September 2016	21/10/2016

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	Flores Sanchez, L

1