HU000025780T2

(19) **HU**

(11) Lajstromszám: **E 025 780**

(13) **T2**

MAGYARORSZÁG
Szellemi Tulajdon Nemzeti Hivatala

EURÓPAI SZABADALOM
SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 13 158834**
(22) A bejelentés napja: **2013. 03. 12.**

(51) Int. Cl.: ***H04L 29/08*** *(2006.01)*
H04W 4/00 *(2006.01)*

(96) Az európai bejelentés bejelentési száma:
EP 20130158834
(97) Az európai bejelentés közzétételi adatai:
EP 2779580 A1 **2014. 09. 17.**
(97) Az európai szabadalom megadásának meghirdetési adatai:
EP 2779580 B1 **2015. 10. 21.**

(72) Feltaláló(k):
Wang, Hao, 53229 Bonn (DE)
Burkert, Stefan, 53173 Bonn (DE)

(73) Jogosult(ak):
Deutsche Telekom AG, 53113 Bonn (DE)

(74) Képviselő:
SBGK Szabadalmi Ügyvivői Iroda, Budapest

(54) **Eljárás és berendezés alkalmazások mobil eszközökre való telepítésére**

Description

The invention relates to a method and an apparatus for controlling the installation of applications on a mobile device. In particular, the invention relates to a method for installing pre-installed applications on mobile devices.

Field of the invention:

Mobile telephones are often specifically set up with applications in advance by the providers of the mobile radio networks. Herein, a series of applications is installed on the devices in advance before delivery to the customer. Examples of this are disclosed in US 2012129503 and EP 2523107.

These applications are often specifically aligned to the provider of the mobile radio network or adapted therefore. There is thus often a large number of versions of different applications for different mobile radio providers. Furthermore, mobile radio providers often offer products and applications which users can then load onto their mobile device in order then to execute them thereon. With all these applications, neither the mobile radio network provider nor the manufacturer of the software knows how often these applications are used or whether they have even been installed. There are therefore no solid and flexible mechanisms between the operator of a mobile radio network and the applications developers to track agreements on the basis of the use of the applications. In general, applications are also installed from a global market place, as is the case, for example, with the iPhone (App Store) or with Android telephones (Google Play Store). By means of this central download region, it is often not possible for a provider

to recognise which devices are provided with which applications. The same applies to the manufacturers or programmers of the applications, whose applications are loaded through the central market place onto the mobile devices. The application developers therefore have no accurate information concerning the number of active installations and the installed drivers. Revenue distribution models therefore cannot be fairly ensured. At the time of the first delivery, it must be known which applications are to be pre-installed on a mobile device. Since such firmware is often hardly adjusted over the whole product cycle because it must be subjected to extensive tests, the pre-installed applications are often those which were originally installed at the first delivery. It is also to be considered that during the determination of the firmware and the assembly and configuration of the mobile device, the programs must be known. Applications which are to be installed on the mobile device later in the product cycle therefore cannot be taken into account. Therefore a dynamic approach is prevented, since the applications must be known during the configuration of the mobile device by the manufacturer. Changes during the product cycle are therefore only possible with difficulty and cannot be implemented by the network provider since it has no acccess or only a limited access to the firmware.

Summary of the invention:

It is an object of the present invention to provide a method/device with which it can be ensured that the pre-installed applications are dynamically installable and thus the network provider has the possibility of determining the pre-installed applications.

This method is defined by the features of the claims. In detail, it relates to a method for controlling the installation of applications on a mobile device, with an installer which is installed on the mobile device, and which is integrated into the operating system of the mobile device in such way, that a silent installation without action by a user takes place and which knows the network address of a server, wherein the server is provided by the network provider over a network to provide a list of permitted applications, wherein the list includes certificates for each application and their names, on the basis of which it can be clearly determined, whether the application is permitted to install further applications on the mobile device. I.e. the list relates to the applications which are permitted to call up the installer (in the described embodiment, only the "assistant"), further comprising an assistant, which runs as an application on the mobile device, and which knows the address of the server, in order to receive a list of applications to be installed from the same,

comprising the steps:

- downloading of a list of permitted applications and saving this list on the mobile device through the installer, wherein the list has the names and certificates of the permitted applications;
- downloading of a list of applications to be installed through the assistant from the server, preferably at the first start of the mobile device with the end customer, wherein the list includes the memory location of the applications;
- downloading of the applications from the network as installation packets through the assistant, in order to store these as installation packages on the mobile device;

- handing over the storage location of the installation packages to the installer through the assistant;
- checking of the installer by means of the certificates and the names from the list of permitted applications whether the assistant is permitted to determine which applications should be installed if the checking is successful, installing the application without action by a user.

In detail, this relates to a method for controlling the installation of applications on a mobile device. These mobile devices are preferably an Android telephone or another smartphone which has a network interface to an IP network. These smartphones are typically equipped with firmware, the configurations of which can be specified by the provider of the network. With this firmware, an installer is already installed on delivery to the final customer. The installer has the task of installing applications when these are provided and trustworthy. In a preferred embodiment, the installer is configured so that it installs applications on the device in the background without the interaction with a user. In addition, the installer checks whether the assistant has a permitted name and/or a permitted certificate. By means of a safety check of this type, it is ensured that only a permitted assistant installs applications or that the permitted assistant calls up the installer in order to install applications. By means of the verification, it is ensured that no non-permitted application (malware) calls up the installer and can thus install arbitrary apps without the involvement and knowledge of the user. The list with the names and the certificates, which also represent the permitted programs, can be downloaded from a server by the installer. In a preferred embodiment, the

downloading takes place via a Standard Internet Protocol (IP) by means of known secure transfer mechanisms such as HTTP, PS or GLS. The installer is preferably an application that is an integral component of the operating system and supplements the standard installer which herein uses a Market Place or Playstore on the device. The installer has its own functionality and allows applications to be installed independently in the operating system. Thus before an application or a binary app which has been loaded on the device is installed, a check is performed by the assistant that wishes to install this application. The verification is carried out on the basis of signatures or hash values and preferably the name of the application packet or the application itself. In addition, a further application is necessary, which is named the Assistant, which is either also pre-installed or is installed via an application store (App Store). This is an application which is installed above the operating system. This means that it is not an integral component of the operating system in order to extend the functioning of the operating system. This application recognises the first start or the first set-up procedures of a mobile device and downloads the binary programs/apps that should be pre-installed on the mobile device. Following downloading of the applications from an app store or another memory store from the internet (ftp, tftp, etc.), a request is sent to the installer by the assistant in order to install the downloaded applications or application packages/installation packages. The installer checks the assistant on the basis of the name and the certificate in the list that is available to the installer, and installs the applications. The assistant or the assistant application has the advantage that it can be different per application country and device type and/or contract type. The application can therefore take

account of a specific configuration for different types of devices and countries and also for different contracts. The applications therefore allow applications to be installed later without burdening the user with a manual installation process for each application. It is also ensured, by means of the verification of the certificates and application names, that only those applications for which a corresponding agreement with partners exists will receive the right to install further applications. The use of the assistant enables different assistants to be provided for device types, countries and contracts which download only applications which are suitable for the respective device. In a further possible embodiment, the assistant is further able to display advertising or special offers. A consequence of this is that the applications are installed according to device and country and it is ensured by the minimal user interaction that only permitted applications are installed. On the basis of the verification, there is also a separation between an installer program that is integrated into the operating system or the firmware and a normal application like the assistant, which are easy to manage and flexible to use. The installer has typically a functionality or authorisation which permits an installation without queries with the user in the background. The installer acquires this authorisation through corresponding rights in the operating system, that is, the installer runs as a process with very high user rights, particularly root rights or it is part of the operating system functionality. The installer obtains an application list from a particular server via HTTP PS. Other protocols, which are preferably encrypted, are naturally also conceivable. The address of the server is pre-defined. In general, a call takes place via a particular IP address. A list is returned from the server

with signed information about applications that may install further applications. The installer administers this list in a secure storage region. In general, this list is regularly called up to determine changes. The list generally comprises only the application names and the corresponding signatures. After the first starting of the mobile telephone, which can be recognised by corresponding flags, the assistant then loads a specific list of applications from a server which are to be installed for the specific device in the specific configuration. The first starting of the telephone can be recognised in that particular flags are set in a non-volatile memory store. If, for example, a mobile telephone has been reset to its original state, then these flags are deleted. On starting, the assistant then knows that all the programs that were defined in the lists are to be installed anew. The server can therefore administer lists that are specific for device types, contract types or countries, or assemble them dynamically according to rules. By transferring the list to the assistant, the assistant is made aware of which applications are to be downloaded in the next step. Herein, the assistant draws upon the properties of the telephone and the SIM card as well as their information and transfers said information to the server. The installer and the assistant are already configured so that the network address of the server is known. The server is provided by the network provider via a network (IP network) in order to assemble a plurality of signatures and names of applications in specific lists which are then prepared for downloading. The signatures show which applications are supported by the network provider. The provision of the signature is dependent specifically on the installed SIM card and/or the operating system version. Other parameters are also

conceivable and are described below. With this approach, it is possible for the provider of the network to stipulate which applications are supported by it on the mobile devices. With this approach, it is also possible for the application which is running on the mobile device to recognise whether the application is supported by the network provider or not. The application which is installed on the mobile device or is installed by the user can access the server via an interface stipulated in advance. However, in general, the signature serves for checking the execution of applications and the support of the applications for the developer of the application. The assistant receives, for example, information on starting the application or on particular sequences within the application and can thereby keep statistics which are communicated to the provider. The signature can also be requested on a first installation of the application.

The method further comprises the steps:

- downloading from the server by the installer of the signatures that are specific for the mobile device, and
- storing these signatures in a signature storage site on the mobile device.

In a preferred embodiment, the signatures are placed in a storage site on the mobile device 7which is encrypted. The encryption is achieved by known methods, and in particular this can take place by means of an integrated cryptographic module or via the SIM card. It is naturally conceivable that for devices which are permanently online, local storage can be avoided. The storage can also be configured such that the signatures are only cached and no whole list of signatures is downloaded, but

only the signatures that are needed or are to be installed on the mobile device by an application.

The starting of the application can include different functions. Firstly, a request for the signature can take place on first starting or, during the program sequence, requesting the signature at the installer can take place over and again. A query may also be necessary on starting of a particular function. It is also conceivable that the signature is requested only during the installation process.

In a preferred embodiment, the application configures itself on the basis of the signature obtained. The configuration can include certain pictorial representations being used and/or representations and brand indications of the network operator or network provider. Furthermore, special functions can be enabled depending on the signature. It is also possible to deactivate particular functions. The result therefrom is that the signature acts dynamically on the application in that particular functions and aspects are enabled or blocked. By this means, it is possible to differentiate between applications that were originally installed during the initial installation and were thus supported by the provider, and applications which were subsequently installed manually by the user. If, for example, the provider were to support particular applications such as navigation systems, then these applications can request the signatures from the installer or have them checked in order then to enable additional functions. Applications which are subsequently installed can also access this interface, but if the application is not stored in a corresponding list of permitted applications, then no enabling of functions takes place.

The signature generally comprises components which are known from encryption and signature technology. Thus, for example, a public and a private key is conceivable, which is incorporated into the signature. Thus, for example, information which has been encrypted by the public key of the application and/or of the business that has developed the application, can be included in the signature element. The application itself can then check the signature on the basis of the private key that is implemented. In an alternative embodiment, the application routes the signature to the server, which checks the signature. By this means, it can be prevented that the private key is contained in the application itself. Once the confirmation of the signature has taken place, processing by the application is carried out.

Aside from a certificate and/or a public key of the application, the signature preferably comprises an identification for the application, wherein the identification of the application can be the Packet Name of the application.

In a possible embodiment, a quantity of signatures are regularly downloaded from the server and stored. The selection of the signature and/or the assignment of the signature to the mobile device can be based on different filter criteria. In general, particular signatures are only usable for particular telephones from particular manufacturers, taking account of particular providers. On a request for the signature at the server, the signatures are provided on the basis of one or more of the following items of information: SIM information, terminal type, operating system type, operating system version, run time of the signature. Further criteria are naturally also

conceivable, such as the type of mobile radio contract, the output of the mobile telephone, etc.

In the preferred embodiment, the components, such as the server are located in an IP network (internet) which can be queried via the known DNS services. Thus, the server can maintain, for example, a fixed domain name or, likewise, a fixed IP address. It is also conceivable that particular reserved regions of the address are used which are maintained by the network provider. The servers usually run on known computer systems which are equipped with corresponding operating systems such as Linux, Windows or Unix in order to provide the corresponding service in the network. Generally, network protocols, as known from an IP-based network, are used. The mobile device is generally a smartphone on the basis of Android, Apple iOS, Windows Mobile, Symbian or the like. These telephones have processors, baseband processors, memory storage and corresponding layers of an operating system. The operating system is often also referred to as firmware and is stored in a memory storage region which can be altered. Generally, this is a Flash memory store.

A further part of the invention are the individual components which implement the method. These are a server, an installer and an assistant. As described above, the installer is preferably a part of the firmware or an application which is pre-installed in the firmware of the mobile device when it is delivered to the final customer. The server is a computer system which provides a database in which the plurality of signatures is stored. The database can be a relational database or an object-oriented database or any other type of database. In general, a known operating system runs on the computer system, as described above. In a further embodiment,

access to the server is possible only through mobile devices which are provided in the network of the network provider. I.e. in general, masking takes place on the basis of the network addresses or masking takes place on the basis of the identification of the mobile device. The server is generally a system which also maintains a database or web services which the mobile devices and the applications can access.

Brief description of the drawings:
The figures, which illustrate a possible implementation of the invention will now be described, although the figures should not be regarded as restrictive.

Fig. 1 shows a flow diagram of the method;
Fig. 2 shows an example of a structure of a list with signatures;
Fig. 3 shows a structure of the list.

Detailed description of the drawings:

Fig. 2 shows an overview of abbreviations which are used in relation to Figs. 1 and 3.

Fig. 1 shows the different components which are taken into account in the present invention. Firstly the server which is in contact with the installer and secondly the assistant which is also in contact with the server. This server can also involve two different servers which can each have different structures. In a preferred embodiment, however, there is just one server. The installer requests an app list with signatures from the server. This request can take place, for example, by means of the HTTPS protocol which is correspondingly encrypted. Based on the request, the server then returns

a list of applications with signatures, generally also by means of the same encryption type, HTTPS, which are specific to the mobile device. It should be noted herein that the installer runs on the mobile device and the server is reached from the mobile device via a network. The transferred list defines the applications which may communicate with the installer in order to install applications in the background, preferably without any action of the user. The installer thus takes on the task of installation and makes an interface to the system available in order to install applications. Furthermore, an application, called an "Assistant App" runs on the mobile device and, during its execution, particularly during the first starting of the device, loads a list of applications from the server. This request is checked by the server whether it is permitted in this way in order then, in the event of permissibility, to return a list of applications which are to be installed during a first start. Once the list of applications has been downloaded by the assistant, downloading onto the mobile device of the application packages, which are provided for the installation, takes place. These application packages are transferred to the installer or a URI request is transferred with the storage site. With the help of the signature in its list, the installer checks whether the caller, that is the assistant, is a permitted application which also has a permitted signature and has not been modified. Thus a silent installation takes place and the user does not need to intervene therein. A silent installation of which the user has no knowledge is therefore carried out. By this means, the device can be provided with the correct software on first use or first switch-on, without it being already integrated in the firmware. Following successful installation, a suitable message is passed to the assistant that the installation

was successful. If the request was not permitted or the application did not match the pre-settings of the signature or have the relevant name, then a corresponding error is reported.

Fig. 3 shows an example of an application list which, in this case, consists of only one application. This is a list for the application App Assistant whose data are transferred. Firstly, the list is opened by means of <id>. The ID stands for an identification of the list so that the list can be clearly identified at a later time point. In the subsequent process, a packet name is defined from which it is apparent which provider is involved. Firstly, signatures are transferred which make it possible to recognise whether the application is authorised to install other applications with the aid of the installer. For this purpose, the signature which was generated by the PrK_Launcher is used. Based on this signature, it can be determined that what is concerned is a permitted application which was generated by the corresponding server with the private key. In this regard, reference is made again to the table in Fig. 2 and to Fig. 1. There are also public keys from the developers who have developed this application, in order to be able to carry out corresponding checking of signatures.

The elements in detail:

* <published-date>: Publication date of the list; can be used for currency-testing.
* <category>, <category-id>, <title>: This is the header for a category, in this case, this category contains the trustworthy apps. Categories for other purposes can be contained in this file.

- <recommendation>: Each TrustedApp is a <recommendation>. This expression has purely historical reasons.
- <id> is a unique identifier within the Content Management System,
- <package-name>: The package name of the trustworthy app
- <name>, <icon>, <type>, <catalogue-date>, <catalogue-add-date>, <promotion>: Attribute of the trustworthy app
- <platform-attributes>: These contain further attributes, in this case specifically the signature and the public key of the certificate of the trustworthy app.
- <signature>: This is the signature generated with SHA-2 from the package name and the public key of the certificate of the trustworthy app, encoded with the private key (the key is named "PrK_TrustedApp" in the other documents)
- <certificate>: The public key of the certificate of the trustworthy app.

714229/KOT

ELJÁRÁS ÉS BERENDEZÉS ALKALMAZÁSOK MOBIL ESZKÖZÖKRE VALÓ TELEPÍTÉSÉRE

Szabadalmi igénypontok

1. Eljárás alkalmazások mobil eszközre való telepítésének vezérlésére, telepítővel, amely a mobil eszközön van telepítve, és amely úgy van beépítve a mobil eszköz operációs rendszerébe, hogy egy telepítés háttérben felhasználói beavatkozás nélkül történik, és amely ismeri egy kiszolgáló hálózati címét, ahol a kiszolgálót a hálózati szolgáltató bocsátja rendelkezésre, hogy egy listát nyújtson az elérhető alkalmazásokról, amelyek a telepítőn keresztül telepíthetők, ahol a lista tartalmazza az egyes alkalmazások tanúsítványát és nevét, amelyek alapján egyértelműen megállapítható, hogy az alkalmazás hozzáférhet-e a telepítőhöz,
továbbá tartalmaz egy segédprogramot, amely alkalmazásként a mobil eszközön fut, és amely ismeri a kiszolgáló címét, hogy ebből egy listát kapjunk a telepítendő alkalmazásokról,
amely a következő lépéseket tartalmazza:

   - engedélyezett alkalmazások listájának letöltése a telepítőn keresztül, valamint ennek a listának a mentése a mobil eszközön, ahol a lista tartalmazza az engedélyezett alkalmazások nevét és tanúsítványát;
   - telepítendő alkalmazások listájának letöltése a kiszolgálóról a segédprogramon keresztül, előnyösen a mobil eszköznek a végfelhasználónál való első indításakor, ahol a lista tartalmazza az alkalmazások tárolóhelyét;
   - az alkalmazások letöltése a hálózatról a segédprogramon keresztül telepítési csomagokként, hogy ezeket telepítési csomagokként a mobil eszközön tároljuk;
   - a telepítési csomagok tároló helyének átadása a segédprogramokon keresztül a telepítőnek;
   - a segédprogramok ellenőrzése a telepítőn keresztül a megengedett alkalmazások listájából való tanúsítvány és név segítségével, amennyiben az ellenőrzés sikeres, a telepítés engedélyezése a segédprogramokon keresztül a telepítővel lévő kapcsolatban felhasználói beavatkozás nélkül.

2. Az előző igénypont szerinti eljárás, ahol az alkalmazás a tanúsítvány alapján van konfigurálva.

3. Az előző igénypont szerinti eljárás, ahol az alkalmazás a tanúsítvány alapján aktivál funkciókat.

4. Az előző igénypont szerinti eljárás, ahol az alkalmazás azonosítója az alkalmazás telepítési csomagneve.

5. Az előző igénypontok egyike vagy néhánya szerinti eljárás, ahol a tanúsítványok, amelyek a telepítő által le lettek töltve, biztonságos tárolóhelyen tárolódnak.

6. Az előző igénypontok egyike vagy néhánya szerinti eljárás, ahol a telepítőnek és/vagy a segédprogramnak a kiszolgáló általi lekérdezésekor a tanúsítvány vagy a telepítendő alkalmazások listája a következő információk egyike vagy néhánya szerint áll rendelkezésre: SIM információk, eszköz típusa, operációs rendszer típusa, operációs rendszer verziója, a tanúsítvány időtartama.

7. Az előző igénypontok egyike vagy néhánya szerinti eljárás, ahol a telepítő az operációs rendszer része, és olyan jogosultsággal lesz végrehajtva, amely engedélyezi alkalmazások felhasználói beavatkozás nélküli telepítését.

8. Az előző igénypontok egyike vagy néhánya szerinti eljárás, ahol az alkalmazások tárolási helye Market Place/Playstore vagy fájlkiszolgáló, különösen FTP.

9. Az előző igénypontok egyike vagy néhánya szerinti eljárás, ahol a segédprogram alkalmazásként az operációs rendszer alkalmazási szintjén fut.

10. Az előző igénypontok egyike vagy néhánya szerinti eljárás,ahol a segédprogram kapcsolók és/vagy jelzők alapján felismeri, hogy a mobil eszköz eredeti állapotból jön-e.

11. Rendszer alkalmazások mobil eszközön való telepítésének vezérlésére, **azzal jellemezve, hogy** ez telepítőn, kiszolgálón és segédprogramon keresztül történik, amelyek arra van kialakítva, hogy végrehajtsák az 1 – 10. igénypontok egyike vagy néhánya szerinti eljárást.

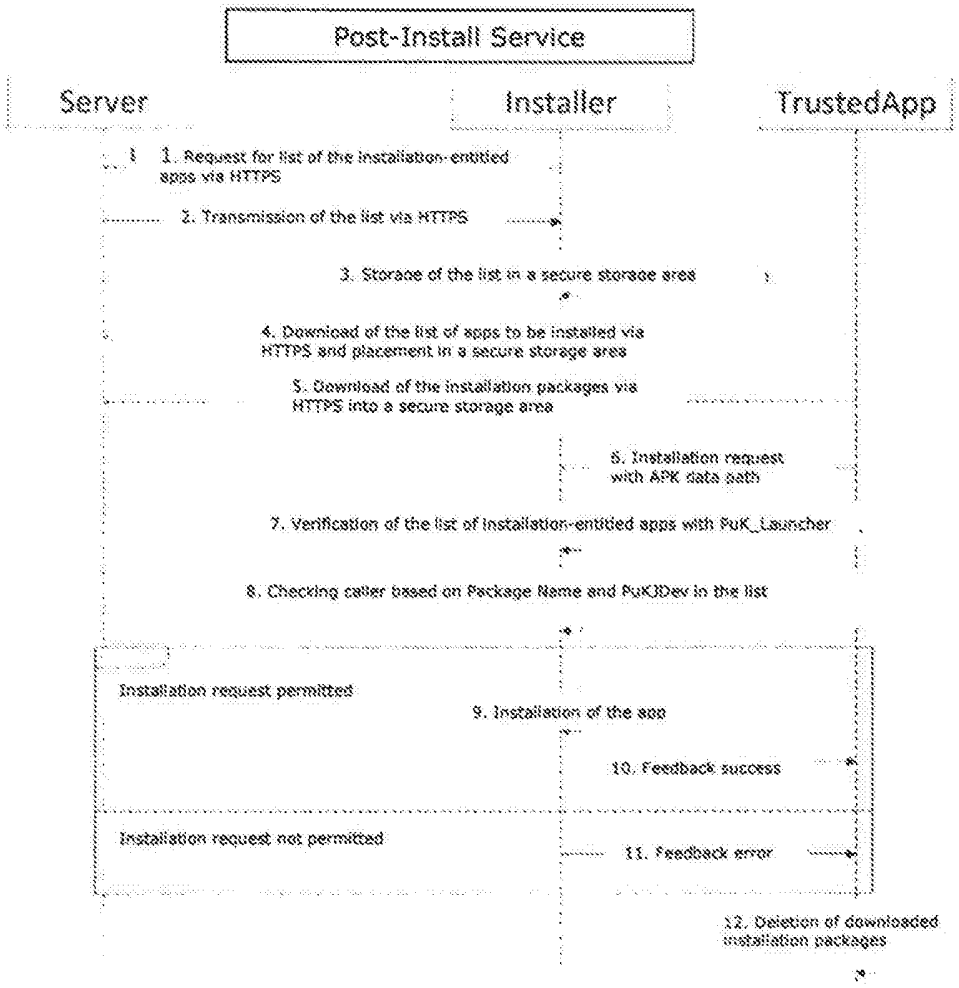
Post-Install Service
Server
Installer
TrustedApp
1. Request for list of the installation-entitled apps via HTTPS
2. Transmission of the list via HTTPS
3. Storage of the list in a secure storage area
4. Download of the list of apps to be installed via HTTPS and placement in a secure storage area
5. Download of the installation packages via HTTPS into a secure storage area
6. Installation request with APK data path
7. Verification of the list of installation-entitled apps with PuK_Launcher
8. Checking caller based on Package Name and PuKIDev in the list
Installation request permitted
9. Installation of the app
10. Feedback success
Installation request not permitted
11. Feedback error
12. Deletion of downloaded installation packages

Fig. 1

Abbreviation	Explanation
Installer	A system service which receives requests from trustworthy apps to install apps without user interaction.
TrustedApp	An app which is authorised to transmit installation requests to the installer.
TrustedApp List	A list of apps which are authorised to transmit installation requests to the installer.
Assistant	A TrustedApp which downloads apps and installs them via the installer; it can also have a user interface.
AppCollection List	A list of app collections which can be installed automatically or by the user, downloaded from back end.
PrK_TrustedApp	Private key with which each element of the TrustedApp list is signed. The key is stored in the back end.
PuK_TrustedApp	Public key for verification of each element of the TrustedApp list, stored in the client.
PuK_SSL	Public key of the SSL certificate for HTTPS, stored in the client.
PuK_Dev	Public key of the developer certificate of a trustworthy app.

Fig. 2

<?xml version="1.0" encoding="UTF-8"?>
<catalogue>
<published-date>2012-10-30T10:40:53</published-date>
<category type="default">
<category-id>installer</category-id>
<title>installer</title>
<recommendation>
<id>56253</id>
<package name>de.telekom.appslauncher</package name>
<name>App Assistant</name>
<icon>http://i.t-mobile-favourites.net/icons/catalogue/de/apptokens/images/1/1/2/4/4/9.png</icon>
<type>application</type>
<catalogue-date>2012-10-30T08:50:33</catalogue-date>
<catalogue-add-date>2012-10-12T11:39:50</catalogue-add-date>
<promotion>false</promotion>
<platform-attributes>
<attribute>
<name>signature</name>
<type>string</type>
<value>ExKJtFwGeds+7ThJ1lTiaag+onorxGZw5TF3qRXcck2AQKKtNRfyorCr+9p/KtdKMUt1PwPtCcd9LYaT9axD7frQfdhK9qnVsXMJ9DPmlqlfwd7dT3a/kl+qshLd9E+vbMxsqWpNzbaj+4xmCUcMyCZt6IblUxcYwyHjAvS7vA=</value>
</attribute>
<attribute>
<name>certificate</name>
<type>string</type>
<value>884ddff1a21a17ae149056dc8f07917887b0b4fe095f36c669b916e4780079ca7ca9071e777ac7f20fffc7df836d2a61089f903cc6bf2e616bc89d7b1188cd943ef2250dd712f2d5507e8476c00007103405 3e52f7504fd7821177ff523ed2beb5c707565a3718d976ba7f0ec51e11874c96f2da15f426bf83a75cb36853886d</value>

```
            </attribute>
          </platform-attributes>
        </recommendation>
    </category>
</catalogue>
```

Fig. 3