



Organización y
Digitalización CSA Ltda



Delegatura de Propiedad Industrial
División de Nuevas Creaciones

PCT

SOLICITUD DE

**PATENTE DE INVENCION
PCT ENTRADA EN FASE NACIONAL**

09-1348

21. EXPEDIENTE No.

54. TITULO: MÉTODO, DISPOSITIVO, APARATO, SISTEMA
ELECTRÓNICO Y PRODUCTO DE PROGRAMA DE
COMPUTADORA PARA ACTUALIZAR UN CRITERIO DE
SEGURIDAD DE DISPOSITIVO ELECTRÓNICO

52. CLASIFICACION INTERNACIONAL: G06F 21/00, H04L 29/06

71. SOLICITANTE: NOKIA SIEMENS NETWORKS OY

DOMICILIO: Karaportti 3, 02610 Espoo, FINLANDIA

74. APODERADO: Dra. MARGARITA CASTELLANOS A.

22. BOGOTA, D.C.,

8 ENE. 2009



PETITORIO

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-001348- -00000-0000

Fecha: 2009-01-08 14:00:38 Dep. 2020 NUECREACION
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 92FORMULARIO UNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

SOLICITUD DE:

①

☒ Patente de Invención.☐ Patente de Modelo de Utilidad.☒ Capítulo I☐ Capítulo II

②

SOLICITANTE (71)

Nombre: NOKIA SIEMENS NETWORKS Oy

Dirección: Karaportti 3, 02610 Espoo,
FINLANDIA

Nacionalidad o Domicilio: Espoo, FINLANDIA

Lugar de Constitución: FINLANDIA

Teléfono:

Fax:

E-mail:

IDENTIFICACIÓN

C.C.



NIT



C.E.



Otro



Cual

Número

③

REPRESENTANTE
O APODERADO

Nombre: MARGARITA CASTELLANOS A.

Dirección: CALLE 94A No. 7A-09

Teléfono: 610 7420 Fax: 610 0706

E-mail: info@castellanosyco.com

IDENTIFICACIÓN

C.C.



NIT



C.E.



Otro



Cual

Número 39'779.654 TPA 70.819

④

INVENTOR (ES) (72)

JYRKI AARNOS

Ohjaskuja 5
FI 36240 Kangasala
FINLANDIAJARI S. VALIMAKI
Karhunkierros 55
FI-36100 Kangasala
FINLANDIA

GABOR PECSY

Gyöngyperje u. 11
HU-1188 Budapest
HUNGRIA

⑤

PCT (86)

Solicitud Internacional No. PCT/IB2007/001557

Fecha 08/06/2007

Publicación Internacional No. WO 2007/141648 A2

Fecha 13/12/2007

⑥

Título (54)

METODO, DISPOSITIVO, APARATO, SISTEMA ELECTRONICO Y PRODUCTO DE
PROGRAMA DE COMPUTADORA PARA ACTUALIZAR UN CRITERIO DE SEGURIDAD
DE DISPOSITIVO ELECTRONICO

⑦

Clasificación Internacional (51) G06F 21/00, H04L 29/06

⑧

Prioridad

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

US

09/06/2006

11/450,932

SI ☒ NO ☐

⑨

Comprobantes de pago Nos.

08-99,292
09-1,404 y 09-1,405Fecha Diciembre 22, 2008
Enero 7 de 2009

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página.

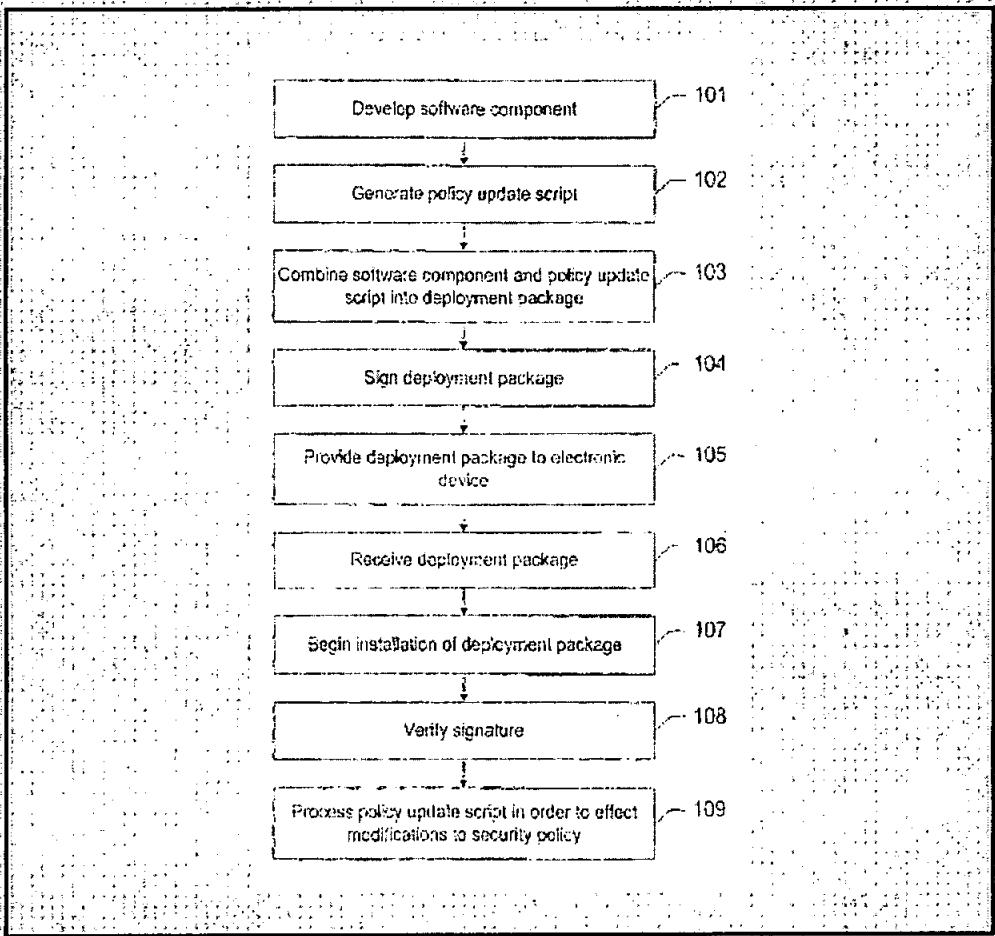
10

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Poderes, si fuere el caso, junto con la sustitución del mismo a mi favor
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Declaraciones.
- ☒ Copia de la solicitud internacional (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos).
- ☐ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☐ Arte final 12x12
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros Tarjeta Propietario y Extracto para la Publicación

11

FIGURA CARACTERISTICA:



12

Solicito la concesión de la patente,

NOMBRE: MARGARITA CASTELLANOS ABONDANO
FIRMA: *Margarita Castellanos*
C.C. No. 39.779.654. Usaquén - TPA 70.819 C.S.J.

8 ENE. 2009

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 08 - 99,292
FECHA : DICIEMBRE 22 DE 2008

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-001348- -00000-0000

Fecha: 2009-01-08 14:00:38 Dep. 2020 NUECREACIONI
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 92

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
ALVARO CASTELLANOS	CONSIGNACION	BANCO DE BOGOTA	062754387	81249475	22/12/2008	6,438,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	501,000.00
		TOTAL :	\$ 501,000.00

SON: QUINIENTOS UN MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

01/01/2000 - 01/01/2000

01/01/2000 - 01/01/2000

01/01/2000 - 01/01/2000
01/01/2000 - 01/01/2000

01/01/2000 - 01/01/2000

DATE	TIME	TYPE	STATUS	REMARKS
01/01/2000	00:00:00	00:00:00	00:00:00	00:00:00

01/01/2000 - 01/01/2000

DATE	TIME	TYPE	STATUS	REMARKS
01/01/2000	00:00:00	00:00:00	00:00:00	00:00:00

01/01/2000 - 01/01/2000
01/01/2000 - 01/01/2000

01/01/2000 - 01/01/2000

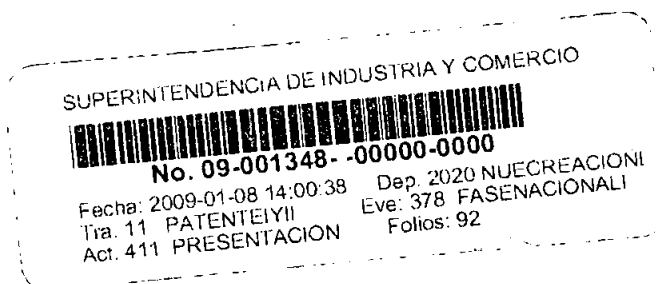
01/01/2000 - 01/01/2000

01/01/2000 - 01/01/2000

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 09 - 1,404
FECHA : ENERO 7 DE 2009



***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
ALVARO CASTELLANOS	CONSIGNACION	BANCO DE BOGOTA	062754387	91417351	07/01/2009	3,783,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-09	OTROS SERVICIOS DE PROPIEDAD I	998 VALOR COMPLEMENTO TARIFA A#0 ANTR
		TOTAL :	\$ 48,000.00

SON: CUARENTA Y OCHO MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 09 - 1,405
FECHA : ENERO 7 DE 2009

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-001348- -00000-0000

Fecha: 2009-01-08 14:00:38 Dep. 2020 NUECREACION
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 92

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
ALVARO CASTELLANOS	CONSIGNACION	BANCO DE BOGOTA	062754387	91417351	07/01/2009	3,783,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
20	50005-01-01	SOLICITUDES	*** REIVINDICACION UNITARIA ADICIONAL
			TOTAL : \$ 500,000.00

SON: QUINIENTOS MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 December 2007 (13.12.2007)

PCT

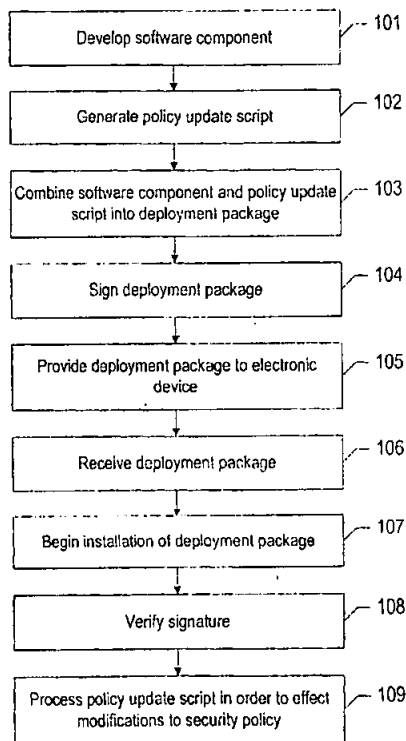
(10) International Publication Number
WO 2007/141648 A2

- (51) International Patent Classification:
G06F 21/00 (2006.01) H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/IB2007/001557
- (22) International Filing Date: 8 June 2007 (08.06.2007)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
11/450,932 9 June 2006 (09.06.2006) US
- (71) Applicant (for all designated States except US): NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).
- (71) Applicant (for LC only): NOKIA INC. [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): AARNOS, Jyrki [FI/FI]; Ohjaskuja 5, FIN-36240 Kangasala (FI). PECSY,

- Gabor [HU/HU]; Gyöngyperje u. 11., H-1188 Budapest (HU). VALIMAKI, Jari, S. [FI/FI]; Karhunkierros 55, FIN-36100 Kangasala (FI).
- (74) Agents: MILLER, Jennifer, F. et al.; Alston & Bird LLP, Bank of America Plaza, 101 South Tryon Street, Suite 4000, Charlotte, NC 28280-4000 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AI, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: METHOD, ELECTRONIC DEVICE, APPARATUS, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR UP-DATING AN ELECTRONIC DEVICE SECURITY POLICY



(57) Abstract: A convenient and safe way is provided to update the security policy associated with an electronic device after a user has purchased the device and taken it away for use. In particular, a scripting tool is provided that can be used to create a policy update script that describes the desired modifications to the electronic device security policy. An OSGi resource processor, referred to as a Policy Update Resource Processor, is further provided, wherein the Policy Update Resource Processor is located on the electronic device and is configured to carry out the security policy modifications outlined in the policy update script.

WO 2007/141648 A2



ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

METHOD, ELECTRONIC DEVICE, APPARATUS, SYSTEM
AND COMPUTER PROGRAM PRODUCT FOR UPDATING
AN ELECTRONIC DEVICE SECURITY POLICY

FIELD

Exemplary embodiments of the present invention relate, generally, to updating an electronic device security policy and, in particular, to an OSGi Policy
5 Update Resource Processor that can be used to effect the policy updates after a user has taken possession of the device for personal use.

BACKGROUND

OSGi, or the Open Services Gateway initiative, is an open standards
10 organization that specified a Java-based service platform that can be remotely managed. More specifically, the OSGi service platform enables the life cycle of the software components of a device, to which the service platform has been added, to be managed from anywhere in the network. The software components, which may provide services to other software components operating on the
15 electronic device, comprise applications that are capable of dynamically discovering and using other software components or applications. These components can be remotely installed, started, stopped, updated and uninstalled without requiring a reboot or otherwise disrupting the operation of the device.

The interaction of the various software components is controlled by the
20 security policy associated with the electronic device on which the components are installed. In particular, the security policy controls how the components interact with each other, what kinds of services respective software components can use, what kinds of services respective software components can provide, and how the software components can access various resources of the electronic device.

25 Each software component may be associated with a respective permission, wherein in order to access the service provided by the software component, other software components or applications of the electronic device must be granted the corresponding permission. However, permissions associated with new software components that are installed after the electronic device has left the hands of the
30 manufacturer or network operator, would not have been granted to the other components of the electronic device. In other words, the security policy associated with the electronic device would not include any reference to the new software

component or its corresponding permission. In addition, the new services would similarly not have been granted the requisite permission(s) for accessing services provided by other software components of the electronic device.

5 As a result, in order for other applications and components of the electronic device to be able to access the new service, and vice versa, the electronic device security policy must be updated or extended to grant the requisite permission(s) to the appropriate components or applications.

10 Other situations may similarly exist where it would be desirable for parties other than the manufacture or network operator, to be able to modify the existing security policy of the electronic device (i.e., in addition to where a new software component is introduced). For example, a software developer may desire to change the security policy on one or more electronic devices in order to test various applications he or she is developing. In addition, companies that provide their employees with mobile devices (e.g., cell phones and/or PDAs) may have
15 specific software that can only be run on that company's devices and require special permissions within the device. It may be desirable for the company to be able to install the necessary rights to the mobile device at the same time the software is being installed.

20 Currently, however, in order to modify the electronic device security policy, a party must have AllPermission, a Java-based permission that grants permission to access everything on the electronic device, or a similar and equally powerful permission. However, manufacturers and, in some instances, network operators are generally the only parties with such a powerful permission. This makes it nearly impossible for any party other than the manufacturer or network
25 operator to modify the existing security policy.

A need, therefore, exists for a way for parties not limited to the device manufacturer or network operator to modify the existing security policy of an electronic device after a user has taken possession of the electronic device.

BRIEF SUMMARY

In general, exemplary embodiments of the present invention provide an improvement over the known prior art by, among other things, providing a convenient and safe way to update the security policy associated with an electronic device, such as a cellular telephone, personal digital assistant (PDA), personal computer (PC), laptop, pager, television, or the like, or one or more electronic devices operating on a motor vehicle, after a user has purchased the device and taken it away for use. In particular, exemplary embodiments provide a scripting tool that can be used to create a policy update script, or resource application or file, that describes the desired modifications to an electronic device security policy. Exemplary embodiments further provide an OSGi resource processor, referred to as a Policy Update Resource Processor, that is located on the electronic device and is configured to carry out the security policy modifications outlined in the policy update script. In particular, in one exemplary embodiment, the modifications may be those necessary to provide a new software component, with which the script corresponds, the requisite permissions to access other software components and resources available on the electronic device. The script may also describe how the security policy should be modified, in turn, to provide the other software components access to the services of the new software component.

In accordance with one aspect, a method is provided of updating a security policy associated with an electronic device. In one exemplary embodiment, the method includes: (1) receiving a policy update script comprising one or more modifications to the security policy; and (2) processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.

According to another aspect, an electronic device is provided that is capable of updating a security policy associated with the electronic device. In one exemplary embodiment the electronic device includes an OSGi policy update resource processor that is configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy.

According to yet another aspect, an apparatus is provided that is capable of updating a security policy associated with an electronic device. In one exemplary embodiment, the apparatus includes a processor and a memory in communication with the processor that stores an application executable by the processor, wherein
5 the application is configured, upon execution, to: (1) generate a policy update script comprising one or more modifications to the security policy, wherein the policy update script is capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and (2) transmit the policy update script.

10 In accordance with another aspect, a system is provided for updating a security policy associated with an electronic device. In one exemplary embodiment, the system includes: (1) a network entity configured to generate a policy update script comprising one or more modifications to the security policy and to transmit the policy update script; and (2) an electronic device configured to
15 receive the policy update script, wherein the electronic device comprises an OSGi policy update resource processor that is configured to process the policy update script received in order to effect the modifications to the security policy.

In accordance with yet another aspect, a computer program product is provided for updating a security policy associated with an electronic device. The
20 computer program product contains at least one computer-readable storage medium having computer-readable program code portions stored therein. The computer-readable program code portions of one exemplary embodiment include: (1) a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and (2) a second executable portion for
25 processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

Having thus described exemplary embodiments of the invention in general
30 terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

Figure 1 is a flow chart illustrating the steps which may be taken in order to update an electronic device security policy in accordance with exemplary embodiments of the present invention;

Figure 2 is a block diagram of one type of system that would benefit from exemplary embodiments of the present invention;

Figure 3 is a schematic block diagram of an entity capable of operating as a device associated with a software developer and/or an authorized policy administrator in accordance with exemplary embodiments of the present invention;

Figure 4 is a schematic block diagram of an electronic device capable of operating in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION

Exemplary embodiments of the present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the inventions are shown. Indeed, these inventions may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like numbers refer to like elements throughout.

Method of Updating Electronic Device Security Policy

Reference is now made to Figure 1, which illustrates the steps which may be taken in order to update the security policy associated with a particular electronic device (e.g., cellular telephone, PDA, PC, laptop, pager, television, or one or more electronic devices operating on a motor vehicle.). As shown, in one exemplary embodiment, the process may begin when a party, such as a software developer, creates or develops a software component or application to be installed on the electronic device. (Step 101). As discussed above, software components are applications operating on an electronic device that may provide services to other components on the device and are likewise capable of dynamically discovering and using services of those other software components and applications. As is discussed in more detail below, Step 101 is optional. In other words exemplary embodiments of the present invention are not limited to instances where new software components are being developed for deployment on electronic devices.

Once the software component has been developed, in Step 102, a policy update script is generated that describes the modifications that must be made to the electronic device security policy in order to enable the new software component to access other services and resources of the electronic device, and vice versa (i.e., the modifications grant the appropriate permissions to the various components). The policy update script may, for example, be in the form of an Extensible Markup Language (XML) file, or the like.

The developed software component and the corresponding policy update script are then combined, in Step 103 into a deployment (or installation) package for deployment on the device. The deployer (or party responsible for creating the deployment package and providing it to the electronic device, which may or may not be the software developer), in Step 104 signs the package (i.e., incorporates a digital signature, such as a private key, with the package). The signature will be used to verify whether and to what extent the signer (i.e., the deployer) is authorized to modify the electronic device security policy; thus providing increased security to the policy updating process. In one exemplary embodiment, different parties may be provided with different levels of authorization. For example, where one party may have authorization to make wholesale modifications to the existing security policy, other parties may have only restricted access.

The deployment or installation package, including the software component, the policy update script and the signature, is then provided to the device in Step 105. In one exemplary embodiment, this step is performed where the user of the electronic device initiates the download of the software component over a network, such as a wide area network (WAN), or the like. Alternatively, the software component may be pushed to the electronic device. As one of ordinary skill in the art will recognize, the software component may be transmitted via any number of mechanisms, including, for example, over Bluetooth, a USB cable, infrared, or even a multimedia card (MMC), without departing from the spirit and scope of exemplary embodiments of the present invention.

Regardless of how the deployment package is received by the electronic device (in Step 106), upon receipt, installation of the deployment package begins (Step 107). In one exemplary embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment

package is in fact authorized to modify the existing security policy of the mobile device (Step 108). Assuming the signature is verified and that the deployer is authorized (based on the existing electronic device security policy), in Step 109, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script.

In particular, according to the OSGi specification, a deployment service exists on the electronic device that is configured to process deployment or installation packages received by the electronic device. This deployment service comprises one or more plug-ins called resource processors, wherein different resource processors are capable of processing different installation packages. In particular, resource processors, or software components that may be located on the device itself or within the deployment package to be installed, handle the lifecycle of specific resource types by processing the resource to create artifacts that are then removed when the resource is dropped. The use of a plug-in architecture for the deployment service is beneficial since it enables the use of multiple types of resources in the installation package (i.e., for each new type of resource a new resource processor, or plug-in, can be added where necessary).

According to exemplary embodiments of the present invention, a new plug-in or OSGi resource processor, referred to as the Policy Update Resource Processor is included in the deployment service. The Policy Update Resource Processor is configured to recognize the policy update script and to conduct the necessary security policy update according to the script. In one exemplary embodiment, usage of the Policy Update Resource Processor is protected by a new Java 2 permission, such that only deployment packages assigned this new permission can run this new processor. The assignment of the Java 2 permission is carried out based on the signature information of the deployment package. In other words, verifying the signature incorporated with the package in order to determine whether, and to what extent, the signer is authorized to modify the security policy, in essence verifies that the party signing the package has been given the new permission.

As mentioned briefly above, exemplary embodiments of the present invention are not limited to situations where a new software component is to be installed on the electronic device. In contrast, the policy update script may be used any time a party desires to modify the existing security policy and is authorized to

do so. In one exemplary embodiment, rather than including the policy update script in a deployment package for a new software component, a manufacturer or operator may create an "empty" deployment or installation package containing only the policy update script (thus eliminating Step 101). The manufacturer or operator could then provide the package to the appropriate parties, such as the software developer. Using this technique, manufacturers and operators would no longer be required to run the actual installation or remote policy management themselves. The below exemplary use case provides an example of where an empty deployment package may be used.

10

Exemplary Use Case:

The following describes a scenario in which exemplary embodiments of the present invention would be particularly useful. As discussed above, downloadable applications and software components are executed under the control of the electronic device security policy and the OSGi service platform. In particular, software components have limited capabilities (e.g., in terms of what services or resources they can access, and vice versa), which are often granted based on the digital signatures authenticating the application code and the electronic device security policy.

15

At the time of development of these applications, however, developers need special access to the device (i.e., they may require special capabilities for their applications). Developer permissions may, therefore, be granted for particular devices, which may be identified by the device's International Mobile Equipment Identification (IMEI). Granting these permissions is a complex and expensive process and only a few authorized parties are authorized to do so.

20

25

For example, one method of granting the requisite permissions is based on the creation of different developer platforms, wherein a special developer certificate may be locked to the IMEIs of one or more specific devices. Developers use private keys corresponding to these certificates when signing their applications. The applications can then be executed on the devices with the listed IMEIs. One drawback to this method, however, is that it assumes that the root certificates that can be used for signing the developer certificates have been provided to the one or more devices at the time of manufacture. In addition, a

30

special mechanism is required that can recognize that the developer certificate is locked to particular IMEI numbers and act accordingly.

Exemplary embodiments of the present invention provide a better solution to the issue of providing developers with special permissions (i.e., one that
5 overcomes at least the above-referenced drawbacks) by combining the conditional permission framework of the OSGi Service Platform with the policy update scripts described above. In particular, the OSGi Service Platform Release 4 is extending the standard Java 2 security system with a conditional permission framework that would allow granting permissions based on different conditions. OSGi policies,
10 therefore, comprise a list of conditions, wherein if those conditions are met, then a certain permission is granted. One such condition, referred to as the IMEICondition, ties the granting of certain permission to the IMEI of the device. This allows certain permissions to be granted on certain categories of devices, or on only single devices.

15 Exemplary embodiments of the present invention combine the IMEICondition with the use of a policy update script in order to create terminal-specific scripts that can be used to update the security policies of only specific electronic devices (e.g., devices on which software developers wish to test their software – i.e., devices the developer wishes to turn into developer devices).

20 In particular, according to exemplary embodiments of the present invention, a developer may provide the IMEIs of the devices they would like to use as developer devices to an authorized policy administrator of those devices (i.e., to a party with authorization to create policy update scripts that will be read by a Policy Update Resource Processor on the device in order to modify the existing
25 security policy). The authorized policy administrator, in turn, creates a policy update script granting the requisite permissions (e.g., AllPermission) to the developers and includes the IMEICondition in the script. In other words, the permission is granted conditionally only for those devices identified by their IMEI. The authorized policy administrator puts the script into a deployment package (i.e.,
30 the standard installation scripts of the OSGi platform), signs the package with his private key and then returns the signed package to the developer. Upon receipt of the package, the developer can execute the package on the device, which, in turn, executes the policy update script. The execution of the deployment package is authorized, based on the authorized policy administrator's signature, to perform the

policy update script. From that point on, the developer will have all of the rights described in the policy update script, with respect to the device(s) identified by their IMEIs. If the deployment package were to be executed with respect to a device not identified in the IMEICondition, the device's security policy would not be affected, since the condition would not be met and, therefore, the permission would not be granted.

The foregoing solution is beneficial because it enables parties having rights to update an electronic device security policy (e.g., the device manufacturer) to delegate that right to, for example, a network operator that can then create developer devices in their developer community. It further eliminates the need to create developer certificates and lock those certificates to the IMEIs of various devices. Permissions can be granted selectively, providing the policy administrator with more fine-grained control than in the case of developer certificates.

15 Overall System and Mobile Device:

Referring to Figure 2, an illustration of one type of system that would benefit from exemplary embodiments of the present invention is provided. As shown in Figure 2, the system can include one or more mobile stations 10, each having an antenna 12 for transmitting signals to and for receiving signals from one or more base stations (BS's) 14. The base station is a part of one or more cellular or mobile networks that each includes elements required to operate the network, such as one or more mobile switching centers (MSC) 16. As well known to those skilled in the art, the mobile network may also be referred to as a Base Station/MSC/Interworking function (BMI). In operation, the MSC is capable of routing calls, data or the like to and from mobile stations when those mobile stations are making and receiving calls, data or the like. The MSC can also provide a connection to landline trunks when mobile stations are involved in a call.

The MSC 16 can be coupled to a data network, such as a local area network (LAN), a metropolitan area network (MAN), and/or a wide area network (WAN). The MSC can be directly coupled to the data network. In one typical embodiment, however, the MSC is coupled to a Packet Control Function (PCF) 18, and the PCF is coupled to a Packet Data Serving Node (PDSN) 19, which is in turn coupled to a WAN, such as the Internet 20. In turn, devices such as processing elements (e.g., personal computers, server computers or the like) can be coupled to the mobile

station 10 via the Internet. For example, the processing elements can include devices corresponding with an Authorized Policy Administrator 22 (i.e., a party having authorization to create policy update scripts that will be read by a Policy Update Resource Processor on the mobile station in order to modify the existing security policy) and/or a Software Developer 24, discussed above. As will be appreciated, the processing elements can comprise any of a number of processing devices, systems or the like capable of operating in accordance with embodiments of the invention.

The BS 14 can also be coupled to a signaling GPRS (General Packet Radio Service) support node (SGSN) 30. As known to those skilled in the art, the SGSN is typically capable of performing functions similar to the MSC 16 for packet switched services. The SGSN, like the MSC, can be coupled to a data network, such as the Internet 20. The SGSN can be directly coupled to the data network. In a more typical embodiment, however, the SGSN is coupled to a packet-switched core network, such as a GPRS core network 32. The packet-switched core network is then coupled to another GTW, such as a GTW GPRS support node (GGSN) 34, and the GGSN is coupled to the Internet.

Although not every element of every possible network is shown and described herein, it should be appreciated that the mobile station 10 may be coupled to one or more of any of a number of different networks. In this regard, mobile network(s) can be capable of supporting communication in accordance with any one or more of a number of first-generation (1G), second-generation (2G), 2.5G and/or third-generation (3G) mobile communication protocols or the like. More particularly, one or more mobile stations may be coupled to one or more networks capable of supporting communication in accordance with 2G wireless communication protocols IS-136 (TDMA), GSM, and IS-95 (CDMA). Also, for example, one or more of the network(s) can be capable of supporting communication in accordance with 2.5G wireless communication protocols GPRS, Enhanced Data GSM Environment (EDGE), or the like. In addition, for example, one or more of the network(s) can be capable of supporting communication in accordance with 3G wireless communication protocols such as Universal Mobile Telephone System (UMTS) network employing Wideband Code Division Multiple Access (WCDMA) radio access technology. Some narrow-band AMPS (NAMPS), as well as TACS, network(s) may also benefit from embodiments of the

invention, as should dual or higher mode mobile stations (e.g., digital/analog or TDMA/CDMA/analog phones).

One or more mobile stations 10 (as well as one or more processing elements, although not shown as such in Figure 2) can further be coupled to one or more wireless access points (APs) 36. The AP's can be configured to communicate with the mobile station in accordance with techniques such as, for example, radio frequency (RF), Bluetooth (BT), infrared (IrDA) or any of a number of different wireless networking techniques, including WLAN techniques. The APs may be coupled to the Internet 20. Like with the MSC 16, the AP's can be directly coupled to the Internet. In one embodiment, however, the APs are indirectly coupled to the Internet via a GTW 28. As will be appreciated, by directly or indirectly connecting the mobile stations and the processing elements (e.g., devices associated with the Authorized Policy Administrator 22 and/or Software Developer 24) and/or any of a number of other devices to the Internet, whether via the AP's or the mobile network(s), the mobile stations and processing elements can communicate with one another to thereby carry out various functions of the respective entities, such as to transmit and/or receive data, content or the like. As used herein, the terms "data," "content," "information," and similar terms may be used interchangeably to refer to data capable of being transmitted, received and/or stored in accordance with embodiments of the invention. Thus, use of any such terms should not be taken to limit the spirit and scope of embodiments of the invention.

Although not shown in Figure 2, in addition to or in lieu of coupling the mobile stations 10 to one or more processing elements (e.g., devices associated with an Authorized Policy Administrator 22 and/or Software Developer 24) across the Internet 20, one or more such entities may be directly coupled to one another. As such, one or more network entities may communicate with one another in accordance with, for example, RF, BT, IrDA or any of a number of different wireline or wireless communication techniques, including LAN and/or WLAN techniques. Further, the mobile station 10 and the processing elements can be coupled to one or more electronic devices, such as printers, digital projectors and/or other multimedia capturing, producing and/or storing devices (e.g., other terminals).

Referring now to Figure 3, a block diagram of an entity capable of operating as a device associated with an Authorized Policy Processor 22 and/or a Software Developer 24 is shown in accordance with one embodiment of the invention. The entity capable of operating as a device associated with an Authorized Policy Processor 22 and/or a Software Developer 24 includes various means for performing one or more functions in accordance with exemplary embodiments of the invention, including those more particularly shown and described herein. In particular, the entity capable of operating as the device associated with either or both the Authorization Policy Processor 22 or the Software Developer 24 may include means for performing one or more of Steps 101-105 of Figure 1 discussed above. It should be understood, however, that one or more of the entities may include alternative means for performing one or more like functions, without departing from the spirit and scope of embodiments of the invention. As shown, the entity capable of operating as a device associated with an Authorized Policy Processor 22 and/or a Software Developer 24 can generally include means, such as a processor 210 connected to a memory 220, for performing or controlling the various functions of the entity. The memory can comprise volatile and/or non-volatile memory, and typically stores content, data or the like. For example, the memory typically stores content transmitted from, and/or received by, the entity. Also for example, the memory typically stores software applications, instructions or the like for the processor to perform steps associated with operation of the entity in accordance with embodiments of the invention. For example, the memory of the entity capable of operating as the device associated with the Authorized Policy Processor 22 may store computer program code for generating a policy update script and signing a deployment or installation package including the generated script prior to transmitting it to, for example, the entity capable of operating as the device associated with the Software Generator 24.

In addition to the memory 220, the processor 210 can also be connected to at least one interface or other means for displaying, transmitting and/or receiving data, content or the like (e.g., for transmitting and/or receiving a generated software component, policy update script and/or signature). In this regard, the interface(s) can include at least one communication interface 230 or other means for transmitting and/or receiving data, content or the like, as well as at least one

user interface that can include a display 240 and/or a user input interface 250. The user input interface, in turn, can comprise any of a number of devices allowing the entity to receive data from a user, such as a keypad, a touch display, a joystick or other input device.

5 Reference is now made to Figure 4, which illustrates one type of electronic device that would benefit from embodiments of the invention. As shown, the electronic device may be a mobile station 10, and, in particular, a cellular telephone. It should be understood, however, that the mobile station illustrated and hereinafter described is merely illustrative of one type of electronic device that
10 would benefit from embodiments of the invention and, therefore, should not be taken to limit the scope of embodiments of the invention. While several embodiments of the mobile station 10 are illustrated and will be hereinafter described for purposes of example, other types of mobile stations, such as personal digital assistants (PDAs), pagers, laptop computers, as well as other types of
15 electronic systems including both mobile, wireless devices and fixed, wireline devices, can readily employ embodiments of the invention.

 The mobile station includes various means for performing one or more functions in accordance with exemplary embodiments of the invention, including those more particularly shown and described herein. It should be understood,
20 however, that one or more of the entities may include alternative means for performing one or more like functions, without departing from the spirit and scope of embodiments of the invention. More particularly, for example, as shown in Figure 3, in addition to an antenna 302, the mobile station 10 includes a transmitter 304, a receiver 306, and means, such as a processing device 308, e.g., a processor,
25 controller or the like, that provides signals to and receives signals from the transmitter 304 and receiver 306, respectively. These signals include signaling information in accordance with the air interface standard of the applicable cellular system and also user speech and/or user generated data. In this regard, the mobile station can be capable of operating with one or more air interface standards,
30 communication protocols, modulation types, and access types. More particularly, the mobile station can be capable of operating in accordance with any of a number of second-generation (2G), 2.5G and/or third-generation (3G) communication protocols or the like. Further, for example, the mobile station can be capable of operating in accordance with any of a number of different wireless networking

techniques, including Bluetooth, IEEE 802.11 WLAN (or Wi-Fi®), IEEE 802.16 WiMAX, ultra wideband (UWB), and the like.

It is understood that the processing device 308, such as a processor, controller or other computing device, includes the circuitry required for implementing the video, audio, and logic functions of the mobile station and is capable of executing application programs for implementing the functionality discussed herein. For example, the processing device may be comprised of various means including a digital signal processor device, a microprocessor device, and various analog to digital converters, digital to analog converters, and other support circuits. The control and signal processing functions of the mobile device are allocated between these devices according to their respective capabilities. The processing device 308 thus also includes the functionality to convolutionally encode and interleave message and data prior to modulation and transmission. The processing device can additionally include an internal voice coder (VC) 308A, and may include an internal data modem (DM) 308B. Further, the processing device 308 may include the functionality to operate one or more software applications, which may be stored in memory. For example, the controller may be capable of operating a connectivity program, such as a conventional Web browser. The connectivity program may then allow the mobile station to transmit and receive Web content, such as according to HTTP and/or the Wireless Application Protocol (WAP), for example.

The mobile station may also comprise means such as a user interface including, for example, a conventional earphone or speaker 310, a ringer 312, a microphone 314, a display 316, all of which are coupled to the controller 308. The user input interface, which allows the mobile device to receive data, can comprise any of a number of devices allowing the mobile device to receive data, such as a keypad 318, a touch display (not shown), a microphone 314, or other input device. In embodiments including a keypad, the keypad can include the conventional numeric (0-9) and related keys (#, *), and other keys used for operating the mobile station and may include a full set of alphanumeric keys or set of keys that may be activated to provide a full set of alphanumeric keys. Although not shown, the mobile station may include a battery, such as a vibrating battery pack, for powering the various circuits that are required to operate the mobile station, as well as optionally providing mechanical vibration as a detectable output.

The mobile station can also include means, such as memory including, for example, a subscriber identity module (SIM) 320, a removable user identity module (R-UIM) (not shown), or the like, which typically stores information elements related to a mobile subscriber. In addition to the SIM, the mobile device
5 can include other memory. In this regard, the mobile station can include volatile memory 322, as well as other non-volatile memory 324, which can be embedded and/or may be removable. For example, the other non-volatile memory may be embedded or removable multimedia memory cards (MMCs), Memory Sticks as manufactured by Sony Corporation, EEPROM, flash memory, hard disk, or the
10 like. The memory can store any of a number of pieces or amount of information and data used by the mobile device to implement the functions of the mobile station. For example, the memory can store an identifier, such as an international mobile equipment identification (IMEI) code, international mobile subscriber identification (IMSI) code, mobile device integrated services digital network (MSISDN) code, or the like, capable of uniquely identifying the mobile device.
15 The memory can also store content. The memory may, for example, store computer program code for an application and other computer programs. For example, in one embodiment of the invention, the memory may store computer program code for performing any combination of Steps 106-109 of Figure 1
20 discussed above. In particular, the memory may store computer program code for receiving a policy update script including one or more modifications to the security policy and for processing the policy update script using an OSGi policy update resource processor 317, also included in the electronic device, in order to effect the modifications to the security policy. In general, the OSGi policy update resource
25 processor 317 is a software component that is capable of handling the life cycle of a particular resource type by processing the resource to create artifacts that are then removed when the resource is dropped.

The system, method, electronic device, network entity and computer program product of exemplary embodiments of the invention are primarily
30 described in conjunction with mobile communications applications. It should be understood, however, that the system, method, electronic device, network entity and computer program product of embodiments of the invention can be utilized in conjunction with a variety of other applications, both in the mobile communications industries and outside of the mobile communications industries.

For example, the system, method, electronic device, network entity and computer program product of exemplary embodiments of the invention can be utilized in conjunction with wireline and/or wireless network (e.g., Internet) applications.

5 Conclusion:

As described above and as will be appreciated by one skilled in the art, embodiments of the invention may be configured as a system, method, electronic device, network entity and computer program product. Accordingly, embodiments of the invention may be comprised of various means including entirely of
10 hardware, entirely of software, or any combination of software and hardware. Furthermore, embodiments of the invention may take the form of a computer program product on a computer-readable storage medium having computer-readable program instructions (e.g., computer software) embodied in the storage medium. Any suitable computer-readable storage medium may be utilized
15 including hard disks, CD-ROMs, optical storage devices, or magnetic storage devices.

Exemplary embodiments of the invention have been described above with reference to block diagrams and flowchart illustrations of methods, apparatuses (i.e., systems) and computer program products. It will be understood that each
20 block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by various means including computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to
25 produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create a means for implementing the functions specified in the flowchart block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data
30 processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including computer-readable instructions for implementing the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause

a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions that execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

- 5 Accordingly, blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that each block of the block diagrams and flowchart illustrations, and
- 10 combinations of blocks in the block diagrams and flowchart illustrations, can be implemented by special purpose hardware-based computer systems that perform the specified functions or steps, or combinations of special purpose hardware and computer instructions.

- 15 Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these exemplary embodiments of the invention pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that exemplary embodiments of the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments
- 20 are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

THAT WHICH IS CLAIMED:

1. A method of updating a security policy associated with an electronic device, said method comprising:
 - 5 receiving a policy update script comprising one or more modifications to the security policy; and
 - processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.
- 10 2. The method of Claim 1, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received.
3. The method of Claim 2 further comprising:
 - 15 verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy.
4. The method of Claim 1 further comprising:
 - receiving a new software component associated with the policy update
 - 20 script; and
 - installing the new software component.
5. The method of Claim 4, wherein the modifications to the security policy grant the new software component permission to access one or more existing
- 25 software applications installed on the electronic device.
6. The method of Claim 5, wherein the modifications further grant one or more existing software components permission to access the new software component.
- 30 7. An electronic device capable of updating a security policy associated with the electronic device, said electronic device comprising:
 - an OSGi policy update resource processor configured to receive a policy update script comprising one or more modifications to the security policy and to

process the policy update script received in order to effect the modifications to the security policy.

8. The electronic device of Claim 7, wherein the policy update script further
5 comprises a signature corresponding with a transmitting party from whom the policy update script is received.

9. The electronic device of Claim 8, wherein the resource processor is further
10 configured to verify the signature in order to determine whether the transmitting party is authorized to modify the security policy.

10. The electronic device of Claim 9, wherein the resource processor is further
configured to determine, based at least in part on the signature, an extent to which
the transmitting party is authorized to modify the security policy.

15

11. The electronic device of Claim 7 further comprising:
a means to receive a new software component associated with the policy
update script; and
a means to install the new software component on the electronic device.

20

12. The electronic device of Claim 10, wherein the modifications to the
security policy grant the new software component permission to access one or
more existing software applications installed on the electronic device, and wherein
the modifications further grant one or more existing software components
25 permission to access the new software component.

13. An apparatus capable of updating a security policy associated with an
electronic device, said apparatus comprising:

a processor; and
30 a memory in communication with the processor, said memory storing an
application executable by the processor, wherein the application is configured,
upon execution, to:

generate a policy update script comprising one or more
modifications to the security policy, said policy update script capable of being

processed by an OSGi policy update resource processor in order to effect the modifications; and

transmit the policy update script.

- 5 14. The apparatus of Claim 13, wherein the application is further configured, upon execution, to associate a signature with the policy update script, said signature capable of being verified in order to determine whether a party associated with the apparatus is authorized to modify the security policy.
- 10 15. The apparatus of Claim 13, wherein the application is further configured, upon execution, to combine the policy update script with a new software component to be installed on the electronic device, said application further configured, upon execution, to transmit the new software component to the electronic device with the policy update script.
- 15 16. The apparatus of Claim 15, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device.
- 20 17. The apparatus of Claim 16, wherein the modifications further grant one or more existing software components permission to access the new software component.
18. The apparatus of Claim 15, wherein the application is further configured, 25 upon execution, to generate the new software component.
19. A system for updating a security policy associated with an electronic device, said system comprising:
- 30 an apparatus configured to generate a policy update script comprising one or more modifications to the security policy, said apparatus further configured to transmit the policy update script; and
- an electronic device configured to receive the policy update script, said electronic device comprising an OSGi policy update resource processor configured

to process the policy update script received in order to effect the modifications to the security policy.

20. The system of Claim 19, wherein the apparatus is further configured to
5 associate a signature with the policy update script, such that transmitting the policy update script comprises transmitting the policy update script and the associated signature.

21. The system of Claim 20, wherein the electronic device is further configured
10 to verify the signature in order to determine whether a party associated with the apparatus is authorized to modify the security policy.

22. The system of Claim 19, wherein the apparatus is further configured to
15 combine the policy update script with a new software component and to transmit the new software component with the policy update script to the electronic device.

23. The system of Claim 22, wherein the electronic device is further configured to receive the new software component and to install the software component.

20 24. The system of Claim 23, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device.

25. The system of Claim 24, wherein the modifications further grant one or
25 more existing software components permission to access the new software component.

26. The system of Claim 22, wherein the apparatus is further configured to
generate the new software component.

30

27. A computer program product for updating a security policy associated with an electronic device, wherein the computer program product comprises at least one computer-readable storage medium having computer-readable program code portions stored therein, said computer-readable program code portions comprising:

a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and

a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.

10

28. The computer program product of Claim 27, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received.

29. The computer program product of Claim 28, wherein the computer-readable program code portions further comprise:

a third executable portion for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy.

15

30. The computer program product of Claim 27, wherein the computer-readable program code portions further comprise:

a third executable portion for receiving a new software component associated with the policy update script; and

20

a fourth executable portion for installing the new software component.

31. The computer program product of Claim 30, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device.

25

32. The computer program product of Claim 31, wherein the modifications further grant one or more existing software components permission to access the new software component.

30

33. An apparatus for updating a security policy associated with an electronic device, said apparatus comprising:

a means for receiving a policy update script comprising one or more modifications to the security policy; and

a means for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.

- 5 34. The apparatus of Claim 33, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received, said apparatus further comprising:

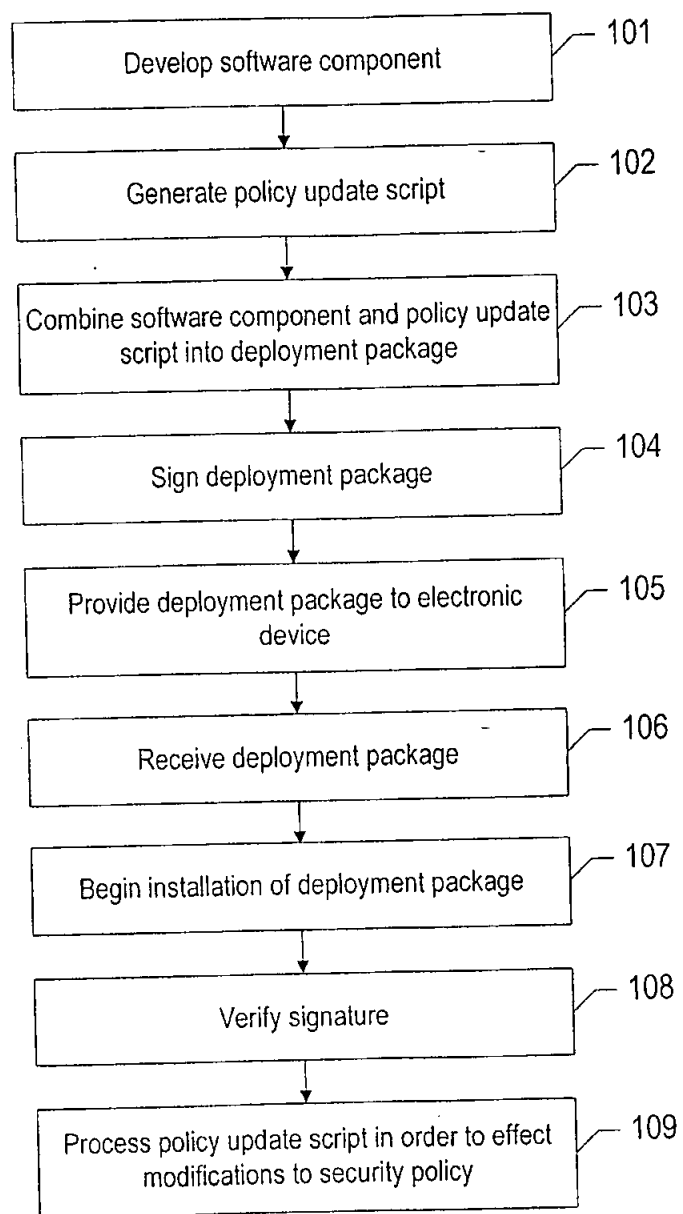
a means for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy.

10

35. The apparatus of Claim 33 further comprising:

a means for receiving a new software component associated with the policy update script; and

- 15 a means for installing the new software component, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device and one or more existing software components permission to access the new software component.

FIG. 1

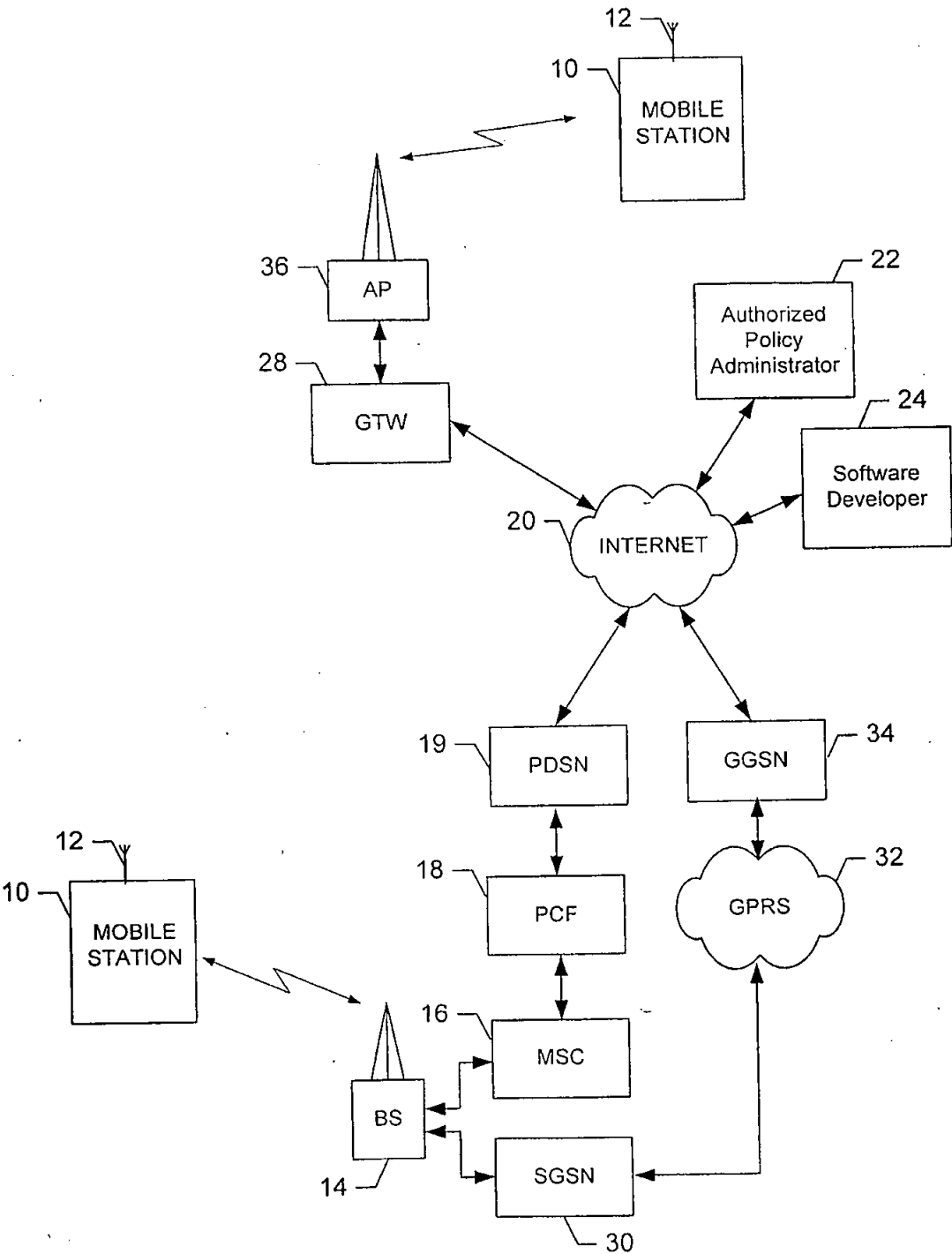
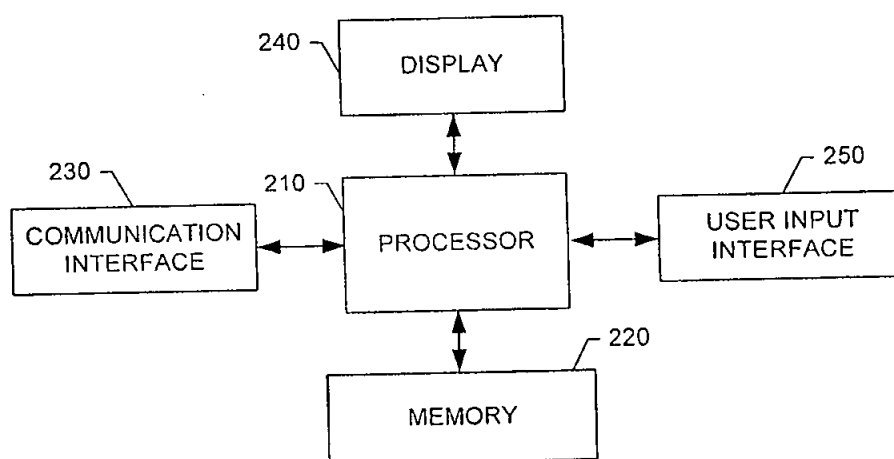


FIG. 2

FIG. 3

10

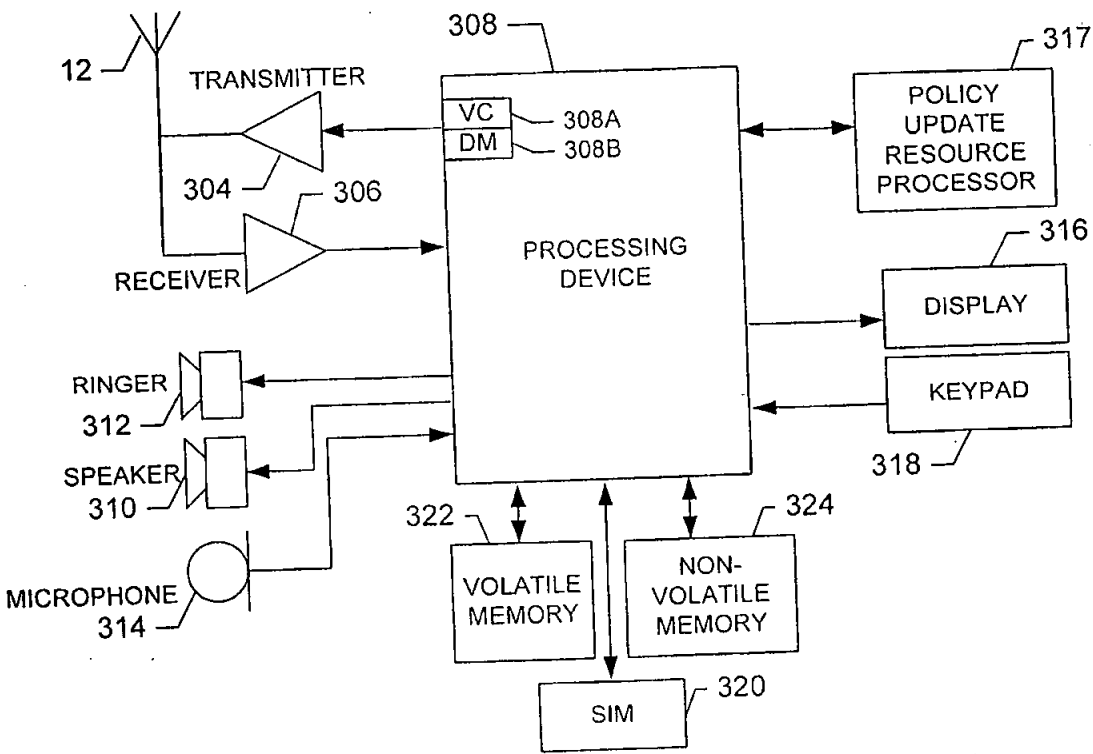


FIG. 4

From the INTERNATIONAL BUREAU

PCT**NOTIFICATION OF THE RECORDING
OF A CHANGE**(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

To:

MILLER, Jennifer, F.
Alston & Bird LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year)

03 December 2008 (03.12.2008)

Applicant's or agent's file reference

42933/329992

IMPORTANT NOTIFICATION

International application No.

PCT/IB2007/001557

International filing date (day/month/year)

08 June 2007 (08.06.2007)

1. The following indications appeared on record concerning:

☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative

Name and Address

NOKIA CORPORATION
Keilalahdentie 4
FIN-02150 Espoo
Finland

State of Nationality

FI

State of Residence

FI

Telephone No.

Facsimile No.

E-mail address

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☒ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence

Name and Address

NOKIA SIEMENS NETWORKS Oy
Karaportti 3
FIN-02610 Espoo
Finland

State of Nationality

FI

State of Residence

FI

Telephone No.

Facsimile No.

E-mail address

☐ Notifications by e-mail authorized

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☐ the receiving Office ☒ the designated Offices concerned
☐ the International Searching Authority ☐ the elected Offices concerned
☐ the International Preliminary Examining Authority ☐ other:The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Grolier David

e-mail ro.ib@wipo.int

Telephone No. +41 22 338 92 22

Facsimile No. +41 22 910 06 10

Form PCT/IB/306 (July 2008)

I/DVN00AQ30

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2007/001557

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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)

IPC: H04L, G06F

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, COMPD, INSP, XPI3E

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20050120219 A1 (MUNETOH, S ET AL), 2 June 2005 (02.06.2005), paragraph [0007], [0008], claims 1, 2 --	1-3,7-9, 13-14,19-21, 27-29,33-34
Y	WO 2004028070 A1 (CREDANT TECHNOLOGIES, INC.), 1 April 2004 (01.04.2004), page 3, line 26 - line 30; page 11, line 21 - line 26; page 18, line 13 - line 19, figure 8, claim 5 --	1-3,7-9, 13-14,19-21, 27-29,33-34
A	WO 095801 A1 (INTEL CORPORATION), 4 November 2004 (04.11.2004), paragraph [0011], [0012], [0029], claims 7, 12, 13 --	1-35

☒ 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

22 November 2007

Date of mailing of the international search report

23-11-2007

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Henrik Eriksson/CC

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001557

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 2006071338 A1 (MOTOROLA INC), 6 July 2006 (06.07.2006), paragraph [0024], [0069], figure 10, 12, claims 1-3, abstract -- -----	1-3,7-9, 13-14,19-21, 27-29,33-34

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001557

International patent classification (IPC)

H04L 9/32 (2006.01)
G06F 21/00 (2006.01)
H04L 29/00 (2006.01)

Download your patent documents at www.prv.se

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument(service in Swedish).

Use the application number as username.

The password is **GYXDTNEPFX**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/09/2007

International application No.
PCT/IB2007/001557

US	20050120219	A1	02/06/2005	CN	1625105 A	08/06/2005
				JP	2005167589 A	23/06/2005
WO	2004028070	A1	01/04/2004	AU	2003276898 A	08/04/2004
				EP	1547303 A	29/06/2005
				JP	2006500657 T	05/01/2006
				US	20060242685 A	26/10/2006
				US	20060147043 A	06/07/2006
				US	20060190984 A	24/08/2006
				US	20060236363 A	19/10/2006
WO	095801	A1	04/11/2004	NONE		
WO	2006071338	A1	06/07/2006	US	20060143179 A	29/06/2006

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference 42933/329992	FOR FURTHER ACTION		See item 4 below
International application No. PCT/IB2007/001557	International filing date (<i>day/month/year</i>) 08 June 2007 (08.06.2007)	Priority date (<i>day/month/year</i>) 09 June 2006 (09.06.2006)	
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237			
Applicant NOKIA SIEMENS NETWORKS Oy			

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 <i>bis</i>.1(a). 2. This REPORT consists of a total of 10 sheets, including this cover sheet. In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.																
3. This report contains indications relating to the following items: <table> <tr> <td>☒ Box No. I</td> <td>Basis of the report</td> </tr> <tr> <td>☒ Box No. II</td> <td>Priority</td> </tr> <tr> <td>☐ Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td>☐ Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td>☒ Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td>☒ Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td>☐ Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td>☐ Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table> 4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).	☒ Box No. I	Basis of the report	☒ Box No. II	Priority	☐ Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	☐ Box No. IV	Lack of unity of invention	☒ Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	☒ Box No. VI	Certain documents cited	☐ Box No. VII	Certain defects in the international application	☐ Box No. VIII	Certain observations on the international application
☒ Box No. I	Basis of the report															
☒ Box No. II	Priority															
☐ Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability															
☐ Box No. IV	Lack of unity of invention															
☒ Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement															
☒ Box No. VI	Certain documents cited															
☐ Box No. VII	Certain defects in the international application															
☐ Box No. VIII	Certain observations on the international application															

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Date of issuance of this report 10 December 2008 (10.12.2008)
	Authorized officer Cecile Chatel e-mail: ro.ib@wipo.int

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

Alston & Bird LLP
Miller Jennifer F
Bank of America Plaza
101 South Tryon Street, Suite
4000
28280-4000 Charlotte, NC
USA

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

23-11-2007

Applicant's or agent's file reference
42933/329992

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/IB2007/001557

International filing date (day/month/year)

08-06-2007

Priority date (day/month/year)

09-06-2006

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

See Supplemental Box

Applicant

Nokia Corporation et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☒ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further opinions, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/SE
Patent- och registreringsverket
Box 5055
S-102 42 STOCKHOLM

Facsimile No. +46 8 667 72 88

Authorized officer

Henrik Eriksson/CC

Telephone No. +46 8 782 25 00

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2007/001557

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Cover sheet

International patent classification (IPC)
H04L 9/32 (2006.01)
G06F 21/00 (2006.01)
H04L 29/00 (2006.01)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB2007/001557

Box No. I	Basis of this opinion
1.	With regard to the language, this opinion has been established on the basis of: ☒ the international application in the language in which it was filed ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.	☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3.	With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of: a. type of material ☐ a sequence listing ☐ table(s) related to the sequence listing b. format of material ☐ on paper ☐ in electronic form c. time of filing/furnishing ☐ contained in the international application as filed. ☐ filed together with the international application in electronic form. ☐ furnished subsequently to this Authority for the purposes of search.
4.	☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5.	Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2007/001557

Box No. II Priority

1. ☒ The validity of the priority claim has not been considered because the International Searching Authority does not have in its possession a copy of the earlier application whose priority has been claimed or, where required, a translation of that earlier application. This opinion has nevertheless been established on the assumption that the relevant date (Rules 43*bis*.1 and 64.1) is the claimed priority date.
2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.
3. Additional observations, if necessary:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2007/001557

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-35	YES
	Claims		NO
Inventive step (IS)	Claims	4-6, 10-12, 15-18, 22-26, 30-32, 35	YES
	Claims	1-3, 7-9, 13-14, 19-21, 27-29, 33-34	NO
Industrial applicability (IA)	Claims	1-35	YES
	Claims		NO

2. Citations and explanations:

The invention concerns a method, electronic device, apparatus, system and computer program product for updating an electronic device security policy. The invention solves the problem that parties, which are not the device manufacturer or network operator, are not able to modify the existing security policy of the electronic device after a user has taken possession of it.

The object of the invention is to provide a convenient and safe way to update the security policy associated with an electronic device after a user has purchased the device and taken it away for use.

Cited documents

D1: WO 2004028070 A1
D2: US 20050120219 A1
D3: WO 2004095801 A1

Document D1 is considered to represent the closest prior art. D1 describes a server, computer memory and method to support security policy maintenance and distribution. A method of updating policies and key materials is provided. An authentication of a user of a mobile computing device is done by receiving a password and the client is resident at the mobile computing device (page 3 rows 26-30). A policy service provides management of the role-based policies as well as creation of the policy files. Once the policies have been defined for a population of users, the administrator can select to publish the policies. The publication process is the act of forming the secure policy files and automatically pushing the policy files out to the individual shield application (page 11 rows 21-26).

.../...

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: BOX V

A method for distributing a modified security policy is illustrated in figure 8. A new policy is added by an administrator connected to the server and the server, in response to the administrator request, creates a new policy package. To distribute the policy package to the mobile computing device, the server authenticates a connection with the gatekeeper and upon successful authentication, sends the policy package to the gatekeeper (page 18 rows 13-19). Claim 5 describes a method of selectively providing a mobile computing device with access to a software application on a server depending on whether the mobile computing device has an installed security program.

Document D2 describes information processing apparatus, a server apparatus, a method of an information processing apparatus, a method of a server apparatus and an apparatus executable process. An information processing apparatus for obtaining services through a network is provided (claims 1 and 2). In server technology as well as network computer systems, other security policies with further flexibilities are requested, because the server may receive many different types of information processing apparatuses including computers, PDAs and sometimes cellular phones. It is required for the server to address the security requirement in more flexible and application independent policy [0007]. The OSGi specifies a framework designed for providing an environment for independent services and offers function of provision, administration and life-cycle managements of such services [0008].

Document D3 represents the general state of the art. D3 describes methods and systems for managing security policies. The security-enabled device can be a software application representing a logical device [0011]. Security policies define security processes, limitations, and/or logic to be enforced on one or more of the security-enabled devices of the network. The security policies can be represented in a variety of data formats. For example a security policy can be a script, written in an interpretive programming language, which is executed by a security-enabled device in order to enforce security limitations on the security-enabled device [0012].

.../...

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB2007/001557

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of BOX V

The security policies are dynamically installed and enforced on the security-enabled devices [0029]. Claim 7 describes a method comprising distributing security policies, enforcing a number of the security policies and updating the policy repository. Claim 12 and 13 describes that the repository push the security policy to the security-enabled device for enforcement.

The invention according to claims 1, 7, 13, 19, 27 and 33 differs from the server, computer memory and method in D1 in that it specifies that the policy update script is being processed using an OSGi policy update resource processor in order to effect the modifications to the security policy.

Due to these features, a way for the life cycle of the software components on a device to be managed from anywhere in the network is achieved.

Consequently, with the background of D1, the problem is to find a way for parties not limited to the device manufacturer or network operator to modify the existing security policy of an electronic device after a user has taken possession of the electronic device.

A solution to this problem is known from document D2, which discloses that an OSGi framework can be used for life-cycle managements.

It is therefore considered to be obvious for a person skilled in the art to use the teachings of D2 together with the prior-art as specified in D1 in order to achieve remotely management of the components according to the claimed invention.

Accordingly, the method, electronic device, apparatus, system and a computer program product for updating a security policy as claimed in claims 1, 7, 13, 19, 27 and 33 lacks an inventive step.

Furthermore, the method, electronic device, apparatus, system and a computer program product referred to in claims 2-3, 8-9, 14, 20-21, 28-29 and 34 are considered to lack inventive step in view of what is known from the cited documents (see especially D1 page 3 rows 26-30).

.../...

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB2007/001557

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of: BOX V

If it can be shown that some aspect covered by claims 2-3, 8-9, 14, 20-21, 28-29 and 34 provides unexpected effects and the claims are restricted accordingly, the judgement may be reconsidered. Until these conditions are met, claims 2-3, 8-9, 14, 20-21, 28-29 and 34 are not considered to involve an inventive step.

The invention defined in claims 4-6, 10-12, 15-18, 22-26, 30-32 and 35 is not disclosed by any of the documents cited in the International Search Report.

The cited prior art does not give any indication that would lead a person skilled in the art to the claimed method, electronic device, apparatus, system and a computer program product for updating a security policy where the policy update script is associated with a new software component and where the software component is to be received and installed in the device. Therefore, the claimed invention is not obvious to a person skilled in the art.

Accordingly, the invention defined in claims 4-6, 10-12, 15-18, 22-26, 30-32 and 35 is novel and is considered to involve an inventive step.

To sum up, the subject matter of claims 1-3, 7-9, 13-14, 19-21, 27-29 and 33-34 is novel, but is not considered to involve an inventive step. The subject matter of claims 4-6, 10-12, 15-18, 22-26, 30-32 and 35 is novel and is considered to involve an inventive step. The subject matter of all the claims is industrially applicable.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2007/001557

Box No. VI Certain documents cited

1. Certain published documents (Rules 43bis.1 and 70.10)

	Application No. Patent No.	Publication date (day/month/year)	Filing date (day/month/year)	Priority date (valid claim) (day/month/year)
P	WO 2006071338	6/7/2006	17/10/2005	29/12/2004

2. Non-written disclosures (Rules 43bis.1 and 70.9)

Kind of non-written disclosure	Date of non-written disclosure (day/month/year)	Date of written disclosure referring to non-written disclosure (day/month/year)

From the INTERNATIONAL BUREAU

PCT**NOTIFICATION OF THE RECORDING
OF A CHANGE**(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

To:

MILLER, Jennifer, F.
Alston & Bird LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year) 03 December 2008 (03.12.2008)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 42933/329992	
International application No. PCT/IB2007/001557	International filing date (day/month/year) 08 June 2007 (08.06.2007)

1. The following indications appeared on record concerning: ☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative		
Name and Address NOKIA CORPORATION Keilalahdentie 4 FIN-02150 Espoo Finland	State of Nationality FI	State of Residence FI
	Telephone No.	
	Facsimile No.	
	E-mail address	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: ☒ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence		
Name and Address NOKIA SIEMENS NETWORKS Oy Karaportti 3 FIN-02610 Espoo Finland	State of Nationality FI	State of Residence FI
	Telephone No.	
	Facsimile No.	
	E-mail address ☐ Notifications by e-mail authorized	
3. Further observations, if necessary:		
4. A copy of this notification has been sent to: ☐ the receiving Office ☒ the designated Offices concerned ☐ the International Searching Authority ☐ the elected Offices concerned ☐ the International Preliminary Examining Authority ☐ other:		

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 910 06 10	Authorized officer Grolier David e-mail ro.ib@wipo.int Telephone No. +41 22 338 92 22
---	--

**MÉTODO, DISPOSITIVO, APARATO, SISTEMA ELECTRÓNICO Y
PRODUCTO DE PROGRAMA DE COMPUTADORA PARA ACTUALIZAR
UN CRITERIO DE SEGURIDAD DE DISPOSITIVO ELECTRÓNICO
CAMPO**

5 Modalidades ejemplares de realización de la presente invención se refieren,
en forma general, a la actualización de un criterio de seguridad de dispositivo
electrónico y, en particular, a un Procesador de Recursos de Actualización de
Criterio OSGi que puede ser usado para efectuar las actualizaciones de criterio
después que un usuario ha tomado posesión del dispositivo para su uso personal.

10

FUNDAMENTOS

OSGi (Open Services Gateway initiative), o plataforma modular abierta de
servicios para múltiples aplicaciones y servicios, es una organización de
estándares abiertos que especifica una plataforma de servicios basados en Java
15 que puede ser administrada en forma remota. Más específicamente, la plataforma
modular abierta de servicios OSGi habilita los ciclos de vida de componentes de
software de un dispositivo, al cual se ha añadido la plataforma de servicios, para
ser administrados desde cualquier punto en la red. Los componentes de software,
los cuales pueden proveer servicios a otros componentes de software que operan
20 en el dispositivo electrónico, comprenden aplicaciones que son capaces de
descubrir en forma dinámica y usar otros componentes de software o aplicaciones.
Estos componentes pueden ser instalados, iniciados, detenidos, actualizados y
desinstalados en forma remota, sin requerir para ello una reiniciación o
interrupción de otro tipo de la operación del dispositivo.

25 La interacción de los diferentes componentes de software es controlada por
el criterio de seguridad asociado con el dispositivo electrónico en el cual están
instalados los componentes. En particular, el criterio de seguridad controla como

los componentes interactúan entre sí, que tipo de servicios respectivos pueden usar los componentes de software, qué tipo de servicios pueden proveer los respectivos componentes de software, y como los componentes de software pueden acceder a diferentes recursos del dispositivo electrónico.

5 Cada componente de software puede ser asociado con un respectivo permiso, en donde con la finalidad de acceder al servicio provisto por el componente de software, se deberán conceder los permisos correspondientes a otros componentes de software del dispositivo electrónico. Sin embargo, los permisos asociados con nuevos componentes de software que son instalados
10 después que el dispositivo electrónico ha sido entregado por el fabricante o el operador de red, no habrían sido conocidos a otros componentes del dispositivo electrónico. Dicho en otras palabras, el criterio de seguridad asociado con el dispositivo electrónico no incluiría cualquier tipo de referencia a los nuevos componentes de software o sus correspondientes permisos. Adicionalmente, los
15 nuevos servicios no habrían obtenido similarmente el(los) permiso(s) requerido(s) para acceder a servicios provistos por otros componentes de software del dispositivo electrónico.

 Como resultado, con la finalidad que otras aplicaciones y componentes del dispositivo electrónico puedan acceder al nuevo servicio, y viceversa, el criterio de
20 seguridad de dispositivo electrónico debe ser actualizado o ampliado para conceder los permisos requeridos a los componentes o aplicaciones apropiados.

 En forma similar, pueden existir otras situaciones en los cuales sería deseable para otras partes que no sean el fabricante u operador de red, que puedan modificar el criterio existente de seguridad del dispositivo electrónico (es
25 decir, en adición a donde debe ser introducido un nuevo componente de software). Por ejemplo, un desarrollador de programas puede desear cambiar el criterio de seguridad en uno o más dispositivos electrónicos para poder ensayar diferentes

aplicaciones que está desarrollando. Adicionalmente, las empresas que proveen a sus empleados con dispositivos móviles (por ejemplo teléfonos celulares y/o PDAs) pueden tener software específico que solamente puede ser operado en los dispositivos de la empresa y que requieren permisos especiales dentro del dispositivo. También puede ser deseable para la empresa poder instalar los derechos necesarios en el los dispositivos móviles al mismo tiempo que el software es instalado.

Actualmente, sin embargo, para poder modificar el criterio de seguridad de dispositivo electrónico, una parte debe tener AllPermission, un permiso basado en Java que concede permiso para acceder a todo programa en el dispositivo electrónico, o un permiso de igual o similar potencia. Sin embargo, los fabricantes y, en algunas instancias, los operadores de red, son generalmente las únicas partes con un permiso tan potente. Esto hace prácticamente imposible para cualquier otra parte que no sea el fabricante o el operador de red modificar el criterio existente de seguridad.

Por lo tanto, existe la necesidad de una manera para aquellas partes no limitadas al fabricante del dispositivo u operador de red, con la cual puedan modificar el criterio existente de seguridad de un dispositivo electrónico después que el usuario haya tomado posesión del dispositivo electrónico.

20

RESUMEN

En forma general, las modalidades ejemplares de realización de la presente invención proveen un perfeccionamiento con respecto al estado del arte conocido, proveyendo, entre otras, una manera conveniente y segura para actualizar el criterio de seguridad asociado con un dispositivo electrónico, tal como teléfono celular, asistente digital personal (PDA), computadora personal (PC), laptop, pager, televisión, o lo similar, o uno o más dispositivos electrónicos que operan en un vehículo automotor, después que el usuario ha adquirido el dispositivo y se lo

25

haya llevado para su uso. En particular, modalidades ejemplares de realización proveen una herramienta de programación que pueda ser usada para crear un bloque de instrucciones (script) de actualización de criterios, o aplicación de recurso o archivo, que describe las modificaciones deseadas a un criterio de seguridad de dispositivo electrónico. Las modalidades ejemplares de realización proveen además un procesador de recursos OSGi, referido como Procesador de Recursos de Actualización de Criterio, el cual está ubicado en el dispositivo electrónico y está configurado para llevar a cabo las modificaciones de criterio de seguridad definidas en el bloque de instrucciones de actualización de criterio. En particular, en una modalidad ejemplar de realización, las modificaciones pueden ser aquellas que son necesarias para proveer un nuevo componente de software, con el cual corresponde el bloque de instrucciones, los permisos requeridos para acceder a otros componentes del software y recursos disponibles en el dispositivo electrónico. El bloque de instrucciones también puede definir como deberá ser modificado el criterio de seguridad, a su vez, para proveer a los otros componentes del software acceso a los servicios del nuevo componente de software.

De acuerdo con un aspecto, se provee un método para actualizar un criterio de seguridad asociado con un dispositivo electrónico. En una modalidad ejemplar de realización, el método comprende: (1) recibir un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad; y (2) procesar el bloque de instrucciones de actualización de criterio usando un Procesador de Recursos de Actualización de criterio OSGi para efectuar las modificaciones al criterio de seguridad.

De acuerdo con otro aspecto, se provee un dispositivo electrónico que es capaz de actualizar un criterio de seguridad asociado con el dispositivo electrónico. En una modalidad ejemplar, el dispositivo electrónico incluye un

Procesador de Recursos de Actualización de criterio OSGi que está configurado para recibir un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad y procesar el bloque de instrucciones de actualización de criterio con la finalidad de efectuar las modificaciones al criterio de seguridad.

De acuerdo con otro aspecto, se ha previsto un aparato que es capaz de actualizar un criterio de seguridad asociado con un dispositivo electrónico. En una modalidad ejemplar de realización, el aparato incluye un procesador y una memoria en comunicación con el procesador que almacena una aplicación ejecutable por el procesador, estando la aplicación configurada, al ser ejecutada, para: (1) generar un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad, siendo el bloque de instrucciones de actualización de criterio capaz de ser procesado por un Procesador de Recursos de Actualización de criterio OSGi con la finalidad de efectuar las modificaciones; y (2) transmitir el bloque de instrucciones de actualización de criterio.

De acuerdo con otro aspecto, se provee un sistema para actualizar un criterio de seguridad asociado con el dispositivo electrónico. En una modalidad ejemplar de realización, el sistema incluye: (1) una entidad de red configurada para generar un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad y transmitir el bloque de instrucciones de actualización de criterio; y (2) un dispositivo electrónico configurado para recibir el bloque de instrucciones de actualización de criterio, comprendiendo el dispositivo electrónico un Procesador de Recursos de Actualización de criterio OSGi que está configurado para procesar el bloque de instrucciones de actualización de criterio para efectuar la modificaciones al criterio de seguridad.

De acuerdo con aun otro aspecto, se provee un producto de programa de computadora para actualizar el criterio de seguridad asociado con el dispositivo electrónico. El producto de programa de computadora contiene al menos un medio de almacenamiento legible por computadora que tiene almacenadas porciones de código de programa legibles por computadora. Las porciones de código de programa legibles por computadora de una modalidad ejemplar de realización incluyen: (1) una primera porción ejecutable para recibir un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad; y (2) una segunda porción ejecutable para procesar el bloque de instrucciones de actualización de criterio usando un Procesador de Recursos de Actualización de criterio OSGi con la finalidad de efectuar las modificaciones al criterio de seguridad.

DESCRIPCIÓN RESUMIDA DE DIFERENTES VISTAS DE LOS DIBUJOS

Habiendo sido descriptas modalidades ejemplares de realización de la invención en términos generales, se hará referencia a continuación a los dibujos adjuntos, los cuales no están necesariamente en escala, y en los cuales:

La figura 1 es un diagrama de flujo que ilustra las etapas que pueden ser llevadas a cabo con la finalidad de actualizar un criterio de seguridad de dispositivo electrónico de acuerdo con modalidades ejemplares de realización de la presente invención.

La figura 2 es un diagrama de bloques de un tipo de sistema que se beneficiaría de las modalidades ejemplares de realización de la presente invención.

La figura 3 es un diagrama esquemático de bloques de una entidad capaz de operar como dispositivo asignado a un desarrollador de software y/o un administrador de criterio autorizado de acuerdo con modalidades ejemplares de

realización de la presente invención.

La figura 4 es un diagrama esquemático de bloques de un dispositivo electrónico capaz de operar de acuerdo con una modalidad ejemplar de realización de la presente invención.

5

DESCRIPCIÓN DETALLADA

Modalidades ejemplares de realización de la presente invención serán descritas a continuación en forma más detallada con referencia a los dibujos adjuntos, en los cuales algunas, pero no todas las modalidades de realización
10 están ilustradas. Por cierto, estas invenciones pueden ser materializadas de diferentes maneras y no deberán ser consideradas como limitativas de las modalidades de realización descritas en la presente; por el contrario, estas modalidades de realización están provistas de manera que esta descripción satisfaga los requerimientos legales. Números similares de referencias se refieren
15 a elementos similares en todo respecto.

Método para actualizar la política de seguridad de dispositivo electrónico

Se hace referencia ahora a la figura 1, la cual ilustra las etapas que pueden ser llevadas a cabo con la finalidad de actualizar el criterio de seguridad asociado
20 con un dispositivo electrónico particular (por ejemplo, teléfono celular, PDA, PC, laptop, pager, televisión, o uno o más dispositivos electrónicos que operan en un vehículo automotor). Como se ilustra, en una modalidad ejemplar de realización, el proceso puede comenzar cuando una parte interesada, tal como un desarrollador de software, crea o desarrolla un componente de software o aplicación a ser
25 instalado en el dispositivo electrónico. (Etapas 101). Como se ha discutido más arriba, los componentes de software son aplicaciones que operan en un dispositivo electrónico que puede proveer servicios a otros componentes en el

dispositivo y son capaces asimismo de descubrir dinámicamente y usar los servicios de aquellos otros componentes de software y aplicaciones. Como será discutido en mayor detalle más abajo, la Etapa 101 es opcional. En otras palabras, modalidades ejemplares de realización de la presente invención no están limitadas a instancias en las cuales son desarrollados nuevos componentes de software para ser aplicados en dispositivos electrónicos.

Una vez que el componente de software ha sido desarrollado, se genera en la Etapa 102 un bloque de instrucciones (script) de actualización de criterio que describe las modificaciones que deben ser realizadas en el criterio de seguridad del dispositivo electrónico para posibilitar al nuevo componente de software acceso a otros servicios y recursos del dispositivo electrónico, y viceversa (es decir, las modificaciones conceden los permisos apropiados a los diferentes componentes). El bloque de instrucciones de actualización de criterio, por ejemplo, puede estar presente en forma de un archivo de Lenguaje de Marca Extensible (Extensible Markup Language (XML)), o lo similar.

El componente de software desarrollado y el correspondiente bloque de instrucciones de actualización de criterio son a continuación combinados en la Etapa 103 en un paquete de aplicación (o instalación) para ser aplicado en el dispositivo. El aplicador (o parte responsable de la creación del paquete de aplicación y proveerlo al dispositivo electrónico, el cual puede o no ser el desarrollador de software), en la Etapa 104 firma el paquete (es decir, incorpora una firma digital, como ser una clave privada, en el paquete). La firma será usada para verificar si y en qué medida el firmante (es decir, el aplicador) está autorizado a modificar el criterio de seguridad del dispositivo electrónico; proveyendo de esta manera una seguridad incrementada al proceso de actualización de criterio. En una modalidad ejemplar de realización, las diferentes partes pueden ser provistas con diferentes niveles de autorización. Por ejemplo, en el caso donde una parte

puede tener autorización para realizar modificaciones totales al criterio existente de seguridad, otras partes pueden tener solamente acceso restringido.

El paquete de aplicación o instalación, incluyendo el componente de software, bloque de instrucciones de actualización de criterio y la firma, es a
5 continuación suministrado al dispositivo en la Etapa 105. En una modalidad de realización ejemplar, esta etapa es realizada cuando el usuario del dispositivo electrónico inicia la descarga del componente de software a través de una red, tal como una red de área extensa (WAN) o lo similar. Alternativamente, el componente de software puede ser alimentado mediante un medio físico al
10 dispositivo electrónico. Como podrá reconocer una persona entendida en la materia, el componente de software puede ser transmitido a través de una cantidad cualesquiera de mecanismos, incluyendo, por ejemplo, Bluetooth, un cable USB, infrarrojo, o aun una tarjeta multimedia (MMC), sin apartarse del espíritu y alcance de las modalidades ejemplares de realización de la presente
15 invención.

Sin considerar cómo el paquete de aplicación es recibido por el dispositivo electrónico (en la Etapa 106), después de la recepción comienza la instalación del paquete de aplicación (Etapa 107). En una modalidad ejemplar de realización, al iniciar el proceso de instalación, se verifica la firma del programador para
20 determinar, como indicado anteriormente, si y en que medida la parte que transmite el paquete de aplicación está en realidad autorizado a modificar el criterio existente de seguridad del dispositivo móvil (Etapa 108). Asumiendo que la firma ha sido verificada y que el desarrollador está autorizado (basado en el criterio existente de seguridad del dispositivo electrónico), en la Etapa 109, se
25 procesa el bloque de instrucciones de actualización de criterio con la finalidad de efectuar modificaciones al criterio de seguridad que está descripta por o incluida en el bloque de instrucciones de actualización de criterio.

En particular, según la especificación OSGi, un servicio de aplicación existe en el dispositivo electrónico que está siendo configurado para procesar paquetes de aplicación o de instalación recibidos por el dispositivo electrónico. Este servicio de aplicación comprende uno o más procesadores de recurso llamados enchufables (plug-ins), en los cuales diferentes procesadores de recursos son capaces de procesar diferentes paquetes de instalación. En particular, los procesadores de recurso, o componentes de software que pueden estar ubicados en el mismo dispositivo o dentro del paquete de aplicación a ser instalado, manipulean el ciclo de vida de tipos específicos de recurso mediante el procesamiento del recurso para crear artefactos que son posteriormente removidos cuando el recurso es dejado caer. El uso de una arquitectura enchufable (plug-in) para los servicios de aplicación es beneficioso ya que permite el uso de múltiples tipos de recursos en el paquete de instalación (es decir, para cada tipo nuevo de recurso un nuevo procesador de recurso, o enchufable (plug-in), puede ser añadido donde sea necesario).

De acuerdo con modalidades ejemplares de realización de la presente invención, un nuevo medio enchufable o procesador de recurso OSGi, referido como Procesador de Recursos de Actualización de Criterio, es incluido en el servicio de aplicación. El Procesador de Recursos de Actualización de Criterio está configurado para reconocer el bloque de instrucciones de actualización de criterio y para realizar la actualización necesaria de política de seguridad de acuerdo con este bloque de instrucciones. En una modalidad de realización ejemplar, el uso del Procesador de Recursos de Actualización de Criterio está protegido por un nuevo permiso Java 2, de manera que solamente paquetes de aplicación que tienen asignado este nuevo permiso pueden correr este nuevo procesador. La asignación del permiso Java 2 es realizada basado en la información de firma del paquete de aplicación. En otras palabras, el hecho de

verificar la firma incorporada en el paquete para determinar si y en que medida el firmante está autorizado a modificar el criterio de seguridad, verifica en esencia que la parte que firma el paquete ha recibido el nuevo permiso.

Como se ha mencionado en forma resumida más arriba, las modalidades
5 ejemplares de realización de la presente invención no están limitadas a situaciones en las cuales un nuevo componente de software debe ser instalado en el dispositivo electrónico. Por el contrario, el bloque de instrucciones de actualización de criterio puede ser usado cada vez que una parte desea modificar el criterio existente de seguridad y está autorizada para hacerlo. En una modalidad
10 ejemplar de realización, en lugar de incluir el bloque de instrucciones de actualización de criterio en el paquete de aplicación para un nuevo componente de software, un fabricante u operador puede crear un paquete "vacío" de aplicación o instalación que contiene solamente el bloque de instrucciones de actualización de criterio (siendo eliminada de esta manera la Etapa 101). El fabricante u operador
15 podría, en consecuencia, proveer el paquete a las partes apropiadas, como ser un desarrollador de software. Mediante el uso de esta técnica, los fabricantes y operadores ya no están obligados a ejecutar por sí mismos la instalación o administración remota del criterio. El caso ejemplar de uso indicado más abajo provee un ejemplo en el cual puede ser usado un paquete vacío de aplicación.

20

Caso ejemplar de uso

A continuación se describe un escenario en el cual modalidades ejemplares de realización de la presente invención serán particularmente útiles. Como se ha discutido anteriormente, aplicaciones y componentes de software descargables,
25 son ejecutados bajo el control del criterio de seguridad del dispositivo electrónico y la plataforma de servicios OSGi. En particular, los componentes de software tienen capacidades limitadas (por ejemplo, en términos en cuanto a servicios o recursos

a los cuales pueden acceder, y viceversa), los cuales son concedidos frecuentemente basados en firmas digitales que autentican el código de aplicación y el criterio de seguridad del dispositivo electrónico.

Sin embargo, en el momento del desarrollo de estas aplicaciones, los desarrolladores necesitan acceso especial al dispositivo (es decir, los mismos pueden requerir aptitudes especiales para sus aplicaciones). En consecuencia, los permisos de desarrollador pueden ser concedidos para dispositivos particulares, los cuales pueden ser identificados por la Identificación de Equipo Móvil Internacional (IMEI) del dispositivo. El hecho de conceder estos permisos es un proceso complejo y costoso y solamente unas pocas partes autorizadas están autorizadas para realizarlo.

Por ejemplo, un método de conceder los permisos requeridos está basado en la creación de diferentes plataformas de desarrollador, donde un certificado especial de desarrollador puede estar ligado a las Identificaciones de Equipo Móvil Internacional (IMEI) de uno o más dispositivos específicos. Los desarrolladores usan claves privadas que corresponden a estos certificados cuando firman sus aplicaciones. Las aplicaciones pueden luego ser ejecutadas en los dispositivos con las Identificaciones de Equipo Móvil Internacional (IMEI) que se encuentran en la lista. Sin embargo, una desventaja de este método es que el mismo asume que los certificados principales que pueden ser usados para firmar los certificados de desarrollador han sido provistos a uno o más dispositivos en el momento de su fabricación. Adicionalmente, se requiere un mecanismo especial que pueda reconocer que el certificado de desarrollador está ligado a números particulares IMEI y actuar en forma correspondiente.

Modalidades ejemplares de realización de la presente invención proveen una mejor solución al problema de proveer a los desarrolladores con permisos especiales (es decir, uno que pueda superar al menos las desventajas indicadas

más arriba) combinando la estructura básica de permiso condicional de la Plataforma Modular Abierta de Servicios OSGi con el bloque de instrucciones de actualización de criterio descrito más arriba. En particular, la autorización de Plataforma Modular Abierta de Servicios OSGi 4 consiste en ampliar el sistema de seguridad estándar Java 2 con una estructura básica de permiso condicional que permitiría conceder permisos basados en diferentes condiciones. En consecuencia, los criterios OSGi comprenden una lista de condiciones, en la cual si estas condiciones son satisfechas, se concede un determinado permiso. Una de tales condiciones, referida como condición IMEI, liga la concesión de determinado permiso al IMEI del dispositivo. Esta medida permite que sean concedidos ciertos permisos en ciertas categorías de dispositivos, o solamente en dispositivos individuales.

Modalidades ejemplares de realización de la presente invención combinan la Condición IMEI con el uso de un bloque de instrucciones de actualización de criterio para crear bloques de instrucciones específicos de terminal que pueden ser usados para actualizar los criterios de seguridad de ciertos dispositivos electrónicos específicos (por ejemplo, dispositivos en los cuales los desarrolladores de software desean ensayar su software – es decir, dispositivos que el desarrollador desea convertir en dispositivos del desarrollador).

En particular, según modalidades ejemplares de realización de la presente invención, un desarrollador puede proveer las Identificaciones IMEI de los dispositivos que desearían usar como dispositivos de desarrollador a un administrador autorizado de criterio de dichos dispositivos (es decir, a una parte con autorización para crear bloques de instrucciones de actualización de criterio que serán leídos por un Procesador de Recursos de Actualización de Criterio en el dispositivo para modificar el criterio existente de seguridad). El administrador autorizado de criterio, a su vez, crea un bloque de instrucciones de actualización

de criterio concediendo los permisos requeridos (por ejemplo, AllPermission) a los desarrolladores e incluye la Condición IMEI en el bloque de instrucciones. En otras palabras, el permiso es concedido condicionalmente solo para aquellos dispositivos identificados por su identificación IMEI. El administrador autorizado de criterio coloca el bloque de instrucciones en un paquete de aplicación (es decir, los bloques de instrucciones de aplicación estándar de la plataforma OSGi), firma el paquete con su clave privada y devuelve el paquete firmado al desarrollador. Al recibir el paquete, el desarrollador puede ejecutar el paquete en el dispositivo, el cual, a su vez, ejecuta el bloque de instrucciones de actualización de criterio. La ejecución del paquete de aplicación es autorizada, basada en la firma del administrador autorizado de criterio, para llevar a cabo el bloque de instrucciones de actualización de criterio. A partir de ese punto, el desarrollador tendrá todos los derechos descritos en el bloque de instrucciones de actualización de criterio, con respecto al (a los) dispositivo(s) identificado(s) por su identificación IMEI. Si el paquete de aplicación debe ser ejecutado con respecto a un dispositivo no identificado en la Condición IMEI, el criterio de seguridad del dispositivo no se vería afectado, puesto que esta condición no sería satisfecha y, en consecuencia, no se concedería el permiso.

La solución anterior es beneficiosa debido al hecho que permite a las partes que tienen derechos para actualizar un criterio de seguridad de dispositivo electrónico (por ejemplo, el fabricante del dispositivo) delegar este derecho a, por ejemplo, un operador de red que puede entonces crear dispositivos de desarrollador en su comunidad de desarrolladores. Además, elimina la necesidad de crear certificados de desarrollador y ligar estos certificados a las identificaciones IMEI de diferentes dispositivos. Los permisos pueden ser concedidos selectivamente, proveyendo al administrador de criterio con un control más estricto que en los casos de certificados de desarrollador.

Sistema general y dispositivo móvil

Con referencia a la figura 2, se provee una ilustración de un tipo de sistema que se beneficiaría de las modalidades ejemplares de realización de la presente invención. Como se ilustra en la figura 2, el sistema puede incluir una o más estaciones móviles 10, cada una con una antena 12 para transmitir señales hacia y recibir señales desde una o más estaciones base (BS) 14. La estación base es parte de una o más redes celulares o móviles que comprenden, en cada caso, elementos requeridos para operar la red, tales como una o más centrales de conmutación móviles (MSC) 16. Como es bien conocido para aquellos entendidos en estas artes, la red móvil puede ser referida como Estación Base /MSC/función de adaptación entre dos sistemas (BMI). En funcionamiento, la central MSC es capaz de enrutar llamadas, datos o lo similar hacia y desde estaciones móviles cuando estas estaciones móviles están realizando y recibido llamadas, datos o lo similar. Las centrales MSC pueden también proveer una conexión a troncos de líneas fijas cuando las estaciones móviles están involucradas en una llamada.

Las centrales MSC 16 pueden ser conectadas a una red de datos, tal como una red de área local (LAN), una red de área metropolitana (MAN), y/o una red de área extensa (WAN). Las centrales MSC pueden ser conectadas directamente a una red de datos. En una modalidad típica de realización, sin embargo, la central MSC está conectada a una Función de Control de Paquete (PCF) 18, y esta función PCF está conectada a un Nodo de Servicios de Datos de Paquete (PDSN) 19, el cual a su vez está conectado a una red WAN, tal como Internet 20. A su vez, los dispositivos tales como elementos de procesamiento (por ejemplo, computadores personales, servidores de computadora o lo similar) pueden ser conectados a la estación móvil 10 a través de Internet. Por ejemplo, los elementos de procesamiento pueden incluir dispositivos que correspondan con un

Administrador Autorizado de Criterio 22 (es decir, una parte que tienen autorización para crear bloques de instrucciones de actualización de criterio que serán leídos por un Procesador de Recursos de Actualización de Criterio en la estación móvil para modificar el criterio existente de seguridad) y/o un
5 Desarrollador de Software 24, discutido más arriba. Como se podrá apreciar, los elementos de procesamiento pueden comprender cualquier número de dispositivos de procesamiento, sistemas o lo similar capaces de operar de acuerdo con las modalidades de realización de esta invención.

La estación base BS 14 también puede estar conectada a un nodo de
10 soporte de señalización GPRS (General Packet Radio Service – Servicio de Radio Genérico de Datos por Paquetes) 30. Como es conocido por aquellos entendidos en estas artes, el nodo SGSN es capaz típicamente de realizar funciones similares a aquellas de la central de conmutación móvil MSC 16 para servicios de conmutación de paquetes. El nodo SGSN, al igual que la central MSC, puede
15 estar conectado a una red de datos, tal como Internet 20. El nodo SGSN puede estar conectado directamente a la red de datos. Sin embargo, en una modalidad de realización más típica, el nodo SGSN está conectado a una red básica de conmutación de paquetes, tal como una red básica GPRS 32. La red básica de conmutación de paquetes es luego conectada a otra pasarela (Gateway GTW), tal
20 como un nodo de soporte GTW GPRS (GGSN) 34, y el nodo de soporte GGSN está conectado a Internet.

A pesar que no todos los elementos de cualquier red posible están ilustrados y descriptos en la presente, se debe apreciar que la estación móvil 10 puede estar conectada a una o más de cualquiera de una pluralidad de redes
25 diferentes. A este respecto, la(s) red(es) móvil(es) pueden ser capaces de soportar comunicaciones de acuerdo con uno o más de un número de protocolos de comunicación móviles de primera generación (1G), de segunda generación (2G),

2,5G y/o de tercera generación (3G) o lo similar. Más particularmente, una o más estaciones móviles pueden estar conectadas a una o más redes capaces de soportar comunicaciones de acuerdo con los protocolos de comunicación inalámbrica 2G IS-136 (TDMA), GSM, y IS-95 (CDMA). Asimismo, por ejemplo, una o más redes pueden ser capaces de soportar comunicaciones de acuerdo con los protocolos de comunicación inalámbrica 2,5G GPRS, tecnología que mejora el estándar GSM (Enhanced Data GSM Environment – EDGE), o lo similar. Adicionalmente, por ejemplo, una o más redes pueden ser capaces de soportar comunicaciones de acuerdo con los protocolos de comunicación inalámbrica 3G tales como la red UMTS (Universal Mobile Telephone System) que emplea tecnología de acceso por radio WCDMA (Wideband Code Division Multiple Access). Algunas redes de banda estrecha AMPS (NAMPS), como también TACS, pueden beneficiarse de las modalidades de realización de la presente invención, lo mismo que estaciones móviles de modo dual o mayor (por ejemplo, teléfonos digital/analógico o TDMA/CDMA/analógicos).

Una o más estaciones móviles 10 (como también uno o más elementos de procesamiento, aunque no están ilustrados en la figura 2) pueden estar adicionalmente conectados a uno o más puntos de acceso inalámbrico (AP) 36. Los puntos de acceso AP pueden estar configurados para comunicar con estaciones móviles de acuerdo con técnicas tales como ser, por ejemplo, radio frecuencia (RF), Bluetooth (BT), infrarrojo (IrDA) o cualquiera de un número de técnicas de red inalámbrica diferentes, incluyendo técnicas WLAN. Los puntos de acceso AP pueden estar conectados a Internet 20. En forma similar a las centrales de comunicación móviles MSC 16, los puntos de acceso AP pueden estar conectados directamente a Internet. Sin embargo, en una modalidad de realización, los puntos de acceso AP están conectados indirectamente a Internet a través de una pasarela GTW 28. Como podrá apreciarse, conectando directa o

indirectamente las estaciones móviles y los elementos de procesamiento (por ejemplo dispositivos asociados con el Administrados Autorizado de Criterio 22 y/o Desarrollador de Software 24) y/o cualquiera de un número de otros dispositivos a Internet, ya sea a través de los puntos de acceso AP o la(s) red(es) móvil(es), las

5 estaciones móviles y los elementos de procesamiento pueden comunicarse entre sí con la finalidad de llevar a cabo diferentes funciones en las respectivas entidades, tales como transmitir y/o recibir datos, contenidos y lo similar. Como se usan en la presente, los términos "datos", "contenido", "información", y términos similares pueden ser usados en forma intercambiable para referirse a datos

10 capaces de ser transmitidos, recibidos y/o almacenados de acuerdo con las modalidades de realización de la presente invención. En consecuencia, el uso de cualquiera de estos términos no debe ser considerado como limitativo del espíritu y alcance de las modalidades de realización de la invención.

Aunque no se ilustra en la figura 2, además o en lugar del acoplamiento de

15 las estaciones móviles 10 a uno o más elementos de procesamiento (por ejemplo dispositivos asociados con el Administrador Autorizado de Criterio 22 y/o Desarrollador de Software 24) a través de Internet 20, una o más de dichas entidades pueden estar conectada directamente una con otra. Como tal, una o más entidades de red pueden comunicarse entre sí de acuerdo con, por ejemplo,

20 RF, BT, IrDA o cualquiera de un número de diferentes técnicas de comunicación alámbricas o inalámbricas, incluyendo LAN y/o WLAN. Adicionalmente, la estación móvil 10 y los elementos de procesamiento pueden estar conectados con uno o más dispositivos electrónicos, tales como impresoras, proyectores digitales y/u otros dispositivos de multimedia que capturan, producen y/o almacenan (por

25 ejemplo, otras terminales).

Con referencia ahora a la figura 3, se ilustra un diagrama de bloques de una entidad capaz de operar como un dispositivo asociado con un Administrador

Autorizado de Criterio 22 y/o un Desarrollador de Software 24, de acuerdo con una modalidad de realización de la presente invención. La entidad capaz de operar como dispositivo asociado con un Administrador Autorizado de Criterio 22 y/o un Desarrollador de Software 24 incluye diferentes medios para llevar a cabo una o

5 más funciones de acuerdo con modalidades ejemplares de realización de la presente invención, incluyendo aquellas ilustradas y descriptas en forma más particular en la presente. En particular, la entidad capaz de operar como dispositivo asociado con cualquiera o ambos el Administrador Autorizado de Criterio 22 o el Desarrollador de Software 24 puede incluir medios para ejecutar

10 una o más Etapas 105-105 de la figura 1 descripta más arriba. Se deberá entender, sin embargo, que una o más entidades pueden incluir medios alternativos para llevar a cabo una o más funciones similares, sin por ello alejarse del espíritu y alcance de las modalidades de realización de la presente invención. Como se ilustra, la entidad capaz de operar como dispositivo asociado con un

15 Administrador Autorizado de Criterio 22 y/o un Desarrollador de Software 24 puede comprender generalmente medios, tales como un procesador 210 conectado a una memoria 220, para llevar a cabo o controlar las diferentes funciones de la entidad. La memoria puede comprender una memoria volátil y/o una memoria no volátil, y almacena típicamente contenidos, datos o lo similar. Por

20 ejemplo, la memoria almacena típicamente contenidos transmitidos típicamente desde y/o recibidos por la entidad. También, por ejemplo, la memoria almacena típicamente aplicaciones de software, instrucciones o lo similar para el procesador que puede llevar a cabo etapas asociadas con la operación de la entidad de acuerdo con modalidades de realización de la presente invención. Por ejemplo, la

25 memoria de la entidad capaz de operar como dispositivo asociado con el Administrador Autorizado de Criterio 22 puede almacenar códigos de programa de computadora para generar un bloque de instrucciones de actualización de criterio

y firmar un paquete de aplicación o de instalación, incluyendo el bloque de instrucciones generado antes de la transmisión del mismo, por ejemplo hacia la entidad capaz de operar como dispositivo asociado con el Desarrollador de Software 24.

5 Además de la memoria 220, el procesador 210 también puede estar conectado a al menos una interfase u otros medios para visualizar en pantalla, transmitir y/o recibir datos, contenidos o lo similar (por ejemplo para transmitir y/o recibir un componente generado de software, bloque de instrucciones de actualización de criterio y/o firma). Al respecto, la(s) interfase(s) puede(n) incluir al

10 menos una interfase de comunicación 230 u otros medios para transmitir y/o recibir datos, contenidos y lo similar, así como al menos una interfase de usuario que puede incluir un elemento de visualización (display) 240 y/o una interfase de entrada de usuario 250. La interfase de entrada de usuario, a su vez, puede comprender cualquiera de un número de dispositivos que permiten a la entidad

15 recibir datos por parte de un usuario, tal como un teclado, un display táctil, palanca de mando (joystick) u otro dispositivo de entrada.

A continuación se hace referencia a la figura 4, la cual ilustra un tipo de dispositivo electrónico que se beneficiaría de las modalidades de realización de la presente invención. Como se ilustra, el dispositivo electrónico puede ser una

20 estación móvil 10, y, en particular, un teléfono celular. Se deberá entender, sin embargo, que la estación móvil ilustrada y descrita a continuación es meramente ilustrativa de un tipo de dispositivo electrónico que se beneficiaría de las modalidades de realización de la presente invención y, en consecuencia, no debería tomarse como limitativo del alcance de las modalidades de realización de

25 la invención. Aunque diferentes modalidades de realización de la estación móvil 10 están ilustradas y serán descritas a continuación para fines de ejemplificación, otros tipos de estaciones móviles, tales como asistentes personales digitales

(PDA), pagers, computadoras tipo laptop, así como otros tipos de sistemas electrónicos, incluyendo tanto dispositivos móviles, inalámbricos, como dispositivos de línea fija, pueden hacer uso fácilmente de modalidades de realización de la invención.

5 La estación móvil incluye diferentes medios para llevar a cabo una o más funciones de acuerdo con modalidades ejemplares de realización de la presente invención, incluyendo aquellas ilustradas y descritas en forma más particular en la presente. Se deberá entender, sin embargo, que una o más de las entidades puede incluir medios alternativos para llevar a cabo una o más funciones similares, 10 sin apartarse del espíritu y alcance de las modalidades de realización de la presente invención. Más particularmente, por ejemplo, como se ilustra en la figura 3, además de una antena 302, la estación móvil 10 puede incluir un transmisor 304, un receptor 306, y medios, como un dispositivo de procesamiento 308, por ejemplo un procesador, controlador o lo similar, que suministra señales hacia y 15 recibe señales desde el transmisor 304 y el receptor 306, respectivamente. Estas señales incluyen información de señalización de acuerdo con el estándar de interfase de aire del sistema celular aplicable y también voz de usuario y/o datos generados por el usuario. Al respecto, la estación móvil puede ser capaz de operar con uno o más estándar de interfase de aire, protocolos de comunicación, tipos de 20 modulación, y tipos de acceso. Más particularmente, la estación móvil puede ser capaz de operar de acuerdo con cualquiera de un número de protocolos de comunicación de segunda generación (2G), 2,5G y/o tercera generación (3G) o lo similar. Más aun, por ejemplo, la estación móvil puede ser capaz de operar de acuerdo con cualquiera de un número de diferentes técnicas de red inalámbrica, 25 incluyendo Bluetooth, IEEE 802.11 WLAN (o Wi-Fi[®]), IEEE 802.16 WiMAX, banda ultra ancha (UWB) y lo similar.

Se entiende que el dispositivo de procesamiento 308, tal como un

procesador, controlador u otro dispositivo de computación, incluye los circuitos requeridos para implementar las funciones de video, de audio y lógicas de la estación móvil y es capaz de ejecutar programas de aplicación para implementar la funcionalidad discutida en la presente. Por ejemplo, el dispositivo de procesamiento puede estar constituido de varios medios que incluyen un dispositivo procesador de señales digitales, un dispositivo microprocesador y varios convertidores análogo a digital, convertidores digital a análogo y otros circuitos de soporte. Las funciones de procesamiento de señal y de control del dispositivo móvil están ubicadas entre estos dispositivos de acuerdo con sus respectivas capacidades. El dispositivo procesador 308 incluye, por lo tanto, también la funcionalidad para codificar en forma convolucionada y para entrelazamiento de mensajes y datos previo a la modulación y transmisión. El dispositivo de procesamiento puede incluir adicionalmente un codificador interno de voz (VC) 308A, y también puede incluir modem de datos internos (DM) 308B. Más aun, el dispositivo de procesamiento 308 puede incluir la funcionalidad de operar una o más aplicaciones de software, las cuales pueden estar almacenadas en la memoria. Por ejemplo, el controlador puede ser capaz de operar un programa de conectividad, tal como un buscador (browser) convencional en red. El programa de conectividad puede a continuación permitir que la estación móvil transmita y reciba contenidos de red, tales como de acuerdo al protocolo de transferencia de hipertexto http y/o el protocolo de aplicación inalámbrica (WAP), por ejemplo.

La estación móvil puede comprender también medios tales como una interfase de usuario que incluye, por ejemplo, un auricular o parlante convencional 310, una campanilla 312, un micrófono 314, una pantalla de visualización (display) 316, estando todos conectados al controlador 308. La interfase de entrada de usuario, la cual permite al dispositivo móvil recibir datos, puede comprender

cualquiera de un número de dispositivos que permiten al dispositivo móvil recibir datos, tales como un teclado 318, una pantalla táctil (no ilustrada), un micrófono 314, u otro dispositivo de entrada. En las modalidades de realización que incluyen un teclado, éste puede incluir teclas numéricas (0-9) y teclas relacionadas (#, *)
5 convencionales, y otras teclas usadas para operar la estación móvil, y puede incluir también un juego completo de teclas alfanuméricas o juego de teclas que pueden ser activadas para proveer un juego completo de teclas alfanuméricas. A pesar que no se ha ilustrado, la estación móvil también puede incluir una batería, tal como un paquete vibratorio de baterías, para alimentar los diferentes circuitos
10 que son requeridos para operar la estación móvil, como también proveer opcionalmente vibraciones mecánicas como una salida detectable.

La estación móvil también puede incluir medios, tales como una memoria que comprende, por ejemplo, un módulo de identificación de abonado (subscriber identity module – SIM) 320, un módulo de identificación de abonado removible (R-
15 UIM) (no ilustrado) o lo similar, que almacena típicamente elementos de información relacionados con el abonado de telefonía móvil. Adicionalmente al módulo de identificación de abonado (SIM), el dispositivo de telefonía móvil puede incluir otra memoria. Al respecto, la estación móvil puede incluir una memoria volátil 322, así como otra memoria no volátil 324, la cual puede estar incorporada
20 y/o puede ser removible. Por ejemplo, la otra memoria no volátil puede estar constituida por tarjetas de memoria multimedia (MMC) incorporadas o removibles, medios de almacenamiento (Memory Sticks) como los fabricados por Sony Corporation, EEPROM, memoria flash, disco rígido o lo similar. La memoria puede almacenar cualquier número de piezas o cantidad de información y de datos
25 usadas por el dispositivo móvil para implementar las funciones de la estación móvil. Por ejemplo, la memoria puede almacenar un identificador, tal como un código de identificación de equipo móvil internacional (IMEI), código de

identificación de abonado de teléfono móvil internacional (IMSI), código de red digital de servicios integrados de dispositivo móvil (MSISDN), o lo similar, capaces de identificar en forma unívoca el dispositivo móvil. La memoria también almacenar contenidos. La memoria puede, por ejemplo, almacenar un código de programa de computadora para una aplicación y otros programas de computadora. Por ejemplo, en una modalidad de realización de la presente invención, la memoria puede almacenar un código de programa de computadora para realizar cualquier combinación de las Etapas 106-109 de la figura 1 discutida más arriba. En particular, la memoria puede almacenar códigos de programa de computadora para recibir un bloque de instrucciones de actualización de criterio que incluye una o más modificaciones al criterio de seguridad y para procesar el bloque de instrucciones de actualización de criterio que usa un Procesador de Recursos de Actualización de criterio OSGi 317, también incluido en el dispositivo electrónico, para efectuar las modificaciones en el criterio de seguridad. En general, el Procesador de Recursos de Actualización de criterio OSGi 317 es un componente de software capaz de manipular los ciclos de vida útil de un tipo particular de recurso, procesando el recurso para crear artefactos que son a continuación removidos cuando el recurso se abandona.

El sistema, método, dispositivo electrónico, entidad de red y producto de programa de computadora de las modalidades ejemplares de realización de la presente invención son descriptos en primer lugar conjuntamente con aplicaciones de comunicaciones móviles. Se debe entender, sin embargo, que el sistema, método, dispositivo electrónico, entidad de red y producto de programa de computadora de las modalidades de realización de la presente invención pueden ser utilizados en conjunción con una variedad de aplicaciones, tanto en la industria de comunicaciones móviles y fuera de la industria de comunicaciones móviles. Por ejemplo, el sistema, método, dispositivo electrónico, entidad de red y producto de

programa de computadora de las modalidades ejemplares de realización de la presente invención pueden ser utilizados en conjunción con aplicaciones de redes alámbricas o inalámbricas (por ejemplo, Internet).

5 Conclusión

Como se ha descrito más arriba y será apreciado por aquellos entendidos en estas artes, las modalidades de realización de la presente invención pueden ser configuradas como un sistema, método, dispositivo electrónico, entidad de red o producto de programa de computadora. En consecuencia, las modalidades de realización de la presente invención pueden estar constituidas por varios medios, incluyendo estar constituidas totalmente por componentes físicos (hardware), totalmente por software, o cualquier combinación de software y de componentes físicos (hardware). Adicionalmente, modalidades de realización de la presente invención pueden tomar la forma de un producto de programa de computadora o un medio de almacenamiento legible por computadora que tiene instrucciones de programas legibles por computadora (por ejemplo software de computadora) materializado en el medio de almacenamiento. Puede ser utilizado cualquier medio adecuado de almacenamiento legible por computadora, incluyendo discos rígidos, CD-ROM, dispositivos de almacenamiento óptico o dispositivos de almacenamiento magnéticos.

Modalidades ejemplares de realización de la presente invención han sido descritas más arriba con referencias a diagramas de bloques e ilustraciones de diagramas de flujo de métodos, aparatos (es decir sistemas) y productos de programa de computadora. Se entenderá que cada bloque de los diagramas de bloques e ilustraciones de los diagramas de flujo, y combinaciones de bloques en los diagramas de bloques e ilustraciones de diagramas de flujo, respectivamente, pueden ser implementados por varios medios que incluyen instrucciones de

programa de computadora. Estas instrucciones de programa de computadora pueden ser cargadas en una computadora universal, computadora de aplicación especial, o aparato programable de procesamiento de datos para producir una máquina, tal que las instrucciones que son ejecutadas en la computadora o en el
5 aparato programable de procesamiento de datos creen un medio para implementar las funciones especificadas en el bloque o bloques del diagrama de flujo.

Estas instrucciones del programa de computadora también pueden estar almacenadas en una memoria legible por computadora que pueden controlar una
10 computadora u otro aparato programable de procesamiento de datos para que funcione en una manera particular, de manera que las instrucciones almacenadas en la memoria legible por computadora produzcan un artículo de fabricación que incluye instrucciones legibles por computadora para implementar la función especificada en el bloque o bloques del diagrama de flujo. Las instrucciones del
15 programa de computadora también pueden ser cargadas en una computadora u otro aparato programable de procesamiento de datos para inducir una serie de etapas operativas a ser realizadas en la computadora u otro aparato programable para producir un proceso implementado por computadora tal que las instrucciones que son ejecutadas en la computadora u otro aparato programable provean etapas
20 para implementar las funciones especificadas en el bloque o bloques de diagrama de flujo.

En consecuencia, los bloques del diagrama de bloques e ilustraciones del diagrama de flujo soportan combinaciones de medios para llevar a cabo funciones específicas, combinaciones de etapas para llevar a cabo las funciones
25 especificadas y medios de instrucción de programa para llevar a cabo funciones específicas. También se entenderá que cada bloque de los diagramas de bloques e ilustraciones de los diagramas de flujo, y combinaciones de bloques en los

diagramas de bloques e ilustraciones de diagrama de flujo pueden ser implementados por sistemas de computadora basados en componentes físicos de propósito especial que realizan las funciones o etapas especificadas, o combinaciones de componentes físicos de propósito especial e instrucciones de
5 computadora.

Numerosas modificaciones y otras modalidades de realización de la presente invención descriptos en la presente vendrán a la mente a aquellos entendidos en estas artes a las cuales pertenecen las modalidades ejemplares de realización de la presente invención teniendo el beneficio de las enseñanzas
10 presentadas en las descripciones anteriores y dibujos asociados. En consecuencia, se entenderá que las modalidades ejemplares de realización de la presente invención no deberán ser limitadas a los ejemplos específicos de realización descriptos y que éstas tienen por propósito ser incluidas dentro del alcance de las reivindicaciones adjuntas. A pesar que en la presente se emplean
15 términos específicos, los mismos son usados solamente en un sentido genérico y descriptivo y no con propósito de limitación.

LO REIVINDICADO ES:

1.- Un método de actualización de un criterio de seguridad asociado con un dispositivo electrónico, comprendiendo dicho método:

recibir un bloque de instrucciones (script) de actualización de criterio que
5 comprende una o más modificaciones al criterio de seguridad; y

procesar el bloque de instrucciones de actualización de criterio usando un Procesador de Recursos de Actualización de criterios OSGi con la finalidad de efectuar las modificaciones al criterio de seguridad.

2.- El método según la reivindicación 1, en el cual el bloque de instrucciones
10 de actualización de criterio comprende además una firma que corresponde con una parte transmisora de la cual se recibe el bloque de instrucciones de actualización de criterio.

3.- El método según la reivindicación 2, el cual comprende además:
verificar la firma para determinar si la parte transmisora está autorizada a
15 modificar el criterio de seguridad.

4.- El método según la reivindicación 1, el cual comprende además:
recibir un nuevo componente de software asociado con el bloque de
instrucciones de actualización de criterio; e
instalar el nuevo componente de software.

20 5.- El método según la reivindicación 4, en el cual las modificaciones al criterio de seguridad conceden al nuevo componente de software permiso para acceder a una o más aplicaciones de software existentes instaladas en el dispositivo electrónico.

6.- El método según la reivindicación 5, en el cual las modificaciones
25 conceden adicionalmente a uno o más componentes de software existentes permiso para acceder al nuevo componente de software.

7.- Un dispositivo electrónico capaz de actualizar un criterio de seguridad

asociado con el dispositivo electrónico, comprendiendo dicho dispositivo electrónico:

un Procesador de Recursos de Actualización de Criterio OSGi configurado para recibir un bloque de instrucciones de actualización de criterio que comprende
5 una o más modificaciones al criterio de seguridad y para procesar el bloque de instrucciones de actualización de criterio recibido con la finalidad de efectuar las modificaciones al criterio de seguridad.

8.- El dispositivo electrónico según la reivindicación 7, en el cual el bloque de instrucciones de actualización de criterio de seguridad comprende además una
10 firma que corresponde con una parte transmisora de la cual se recibe el bloque de instrucciones de actualización de criterio.

9.- El dispositivo electrónico según la reivindicación 8, en el cual el procesador de recursos está configurado además para verificar la firma con la finalidad de determinar si la parte transmisora está autorizada a modificar el
15 criterio de seguridad.

10.- El dispositivo electrónico según la reivindicación 9, en el cual el procesador de recursos está además configurado para determinar, basado al menos en parte en la firma, la extensión en la cual la parte transmisora está autorizada a modificar el criterio de seguridad.

20 11.- El dispositivo electrónico según la reivindicación 7, el cual comprende además:

un medio para recibir un nuevo componente de software asociado con el bloque de instrucciones de actualización de criterio; y

un medio para instalar el nuevo componente de software en el dispositivo
25 electrónico.

12.- El dispositivo electrónico según la reivindicación 10, en el cual las modificaciones al criterio de seguridad conceden al nuevo componente de

software permiso para acceder a una o más aplicaciones de software instaladas en el dispositivo electrónico, y en el cual las modificaciones conceden además a uno o más componentes existentes de software permiso para acceder al nuevo componente de software.

- 5 13.- Un aparato capaz de actualizar un criterio de seguridad asociado con un dispositivo electrónico, comprendiendo dicho aparato:

un procesador;

- una memoria en comunicación con el procesador, almacenando dicha memoria una aplicación ejecutable por el procesador, en donde la aplicación está
10 configurada, en el momento de su ejecución, para:

- generar un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad, siendo dicho bloque de instrucciones de actualización de criterio capaz de ser procesado por un Procesador de Recursos de Actualización de criterio OSGi con la finalidad de
15 efectuar las modificaciones; y

transmitir el bloque de instrucciones de actualización de criterio.

- 14.- El aparato según la reivindicación 13, en el cual la aplicación está configurada además, al ser ejecutada, para asociar una firma con el bloque de instrucciones de actualización de criterio, pudiendo dicha firma ser verificada para
20 determinar si una parte asociada con el aparato está autorizada a modificar el criterio de seguridad.

- 15.- El aparato según la reivindicación 13, en el cual la aplicación está configurada además, al ser ejecutada, para combinar el bloque de instrucciones de actualización de criterio con un nuevo componente de software a ser instalado
25 en el dispositivo electrónico, siendo dicha aplicación configurada además, al ser ejecutada, para transmitir el nuevo componente de software al dispositivo electrónico con el bloque de instrucciones de actualización de criterio.

16.- El aparato según la reivindicación 15, en el cual las modificaciones al criterio de seguridad conceden al nuevo componente de software permiso para acceder a una o más aplicaciones existentes de software instaladas en el dispositivo electrónico.

5 17.- El aparato según la reivindicación 16, en el cual las modificaciones conceden además a uno o más componentes existentes de software permiso para acceder al nuevo componente de software.

10 18.- El aparato según la reivindicación 15, en el cual la aplicación está configurada además, al ser ejecutada, para generar el nuevo componente de software.

19.- Un sistema para actualizar un criterio de seguridad asociado con un dispositivo electrónico, comprendiendo dicho sistema:

15 un aparato configurado para generar un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad, estando dicho aparato configurado además para transmitir el bloque de instrucciones de actualización de criterio: y

20 un dispositivo electrónico configurado para recibir el bloque de instrucciones de actualización de criterio, comprendiendo dicho dispositivo electrónico un Procesador de Recursos de Actualización de criterio OSGi configurado para procesar el bloque de instrucciones de actualización de criterio recibido con la finalidad de efectuar las modificaciones al criterio de seguridad.

25 20.- El sistema según la reivindicación 19, en el cual el aparato está configurado además para asociar una firma con el bloque de instrucciones de actualización de criterio, de manera que la transmisión del bloque de instrucciones de actualización de criterio comprende transmitir el bloque de instrucciones de actualización de criterio y la firma asociada.

21.- El sistema según la reivindicación 20, en el cual el dispositivo

electrónico está configurado además para verificar la firma con la finalidad de determinar si una parte asociada con el aparato está autorizada a modificar el criterio de seguridad.

22.- El sistema según la reivindicación 19, en el cual el aparato está
5 configurado además para combinar el bloque de instrucciones de actualización de criterio con un nuevo componente de software y para transmitir el nuevo componente de software con el bloque de instrucciones de actualización de criterio al dispositivo electrónico.

23.- El sistema según la reivindicación 22, en el cual el dispositivo
10 electrónico está configurado además para recibir el nuevo componente de software e instalar el componente de software.

24.- El sistema según la reivindicación 23, en el cual las modificaciones al criterio de seguridad conceden al nuevo componente de software permiso para acceder a una o más aplicaciones existentes de software instaladas en el
15 dispositivo electrónico.

25.- El sistema según la reivindicación 24, en el cual las modificaciones conceden además a uno o más componentes de software permiso para acceder al nuevo componente de software.

26.- El sistema según la reivindicación 22, en el cual el aparato está
20 configurado además para generar el nuevo componente de software.

27.- Un producto de programa de computadora para actualizar un criterio de seguridad asociado con un dispositivo electrónico, en el cual el producto de programa de computadora comprende al menos un medio de almacenamiento legible por computadora que tiene porciones de código de programa legibles por
25 computadora almacenadas en éste, comprendiendo dichas porciones de código de programa legibles por computadora:

una primera porción ejecutable para recibir un bloque de instrucciones de

actualización de criterio que comprende una o más modificaciones al criterio de seguridad; y

una segunda porción ejecutable para procesar el bloque de instrucciones de actualización de criterio usando un Procesador de Recursos de Actualización de criterio OSGi con la finalidad de efectuar las modificaciones al criterio de seguridad.

28.- El producto de programa de computadora según la reivindicación 27, en el cual el bloque de instrucciones de actualización de criterio comprende además una firma que corresponde con una parte transmisora de la cual se recibe el bloque de instrucciones de actualización de criterio.

29.- El producto de programa de computadora según la reivindicación 28, en el cual las porciones de código de programa legibles por computadora comprenden además:

una tercera porción ejecutable para verificar la firma con la finalidad de determinar si la parte transmisora está autorizada a modificar el criterio de seguridad.

30.- El producto de programa de computadora según la reivindicación 27, en el cual las porciones de código de programa legibles por computadora comprenden además:

una tercera porción ejecutable para recibir un nuevo componente de software asociado con el bloque de instrucciones de actualización de criterio; y

una cuarta porción ejecutable para instalar el nuevo componente de software.

31.- El producto de programa de computadora según la reivindicación 30, en el cual las modificaciones al criterio de seguridad conceden al nuevo componente de software permiso para acceder a una o más aplicaciones existentes de software instaladas en el dispositivo electrónico.

32.- El producto de programa de computadora según la reivindicación 31, en el cual las modificaciones conceden además a uno o más componentes existentes de software permiso para acceder al nuevo componente de software.

33.- Un aparato para actualizar un criterio de seguridad asociado con un dispositivo electrónico, comprendiendo dicho aparato:

un medio para recibir un bloque de instrucciones de actualización de criterio que comprende una o más modificaciones al criterio de seguridad; y

un medio para procesar el bloque de instrucciones de actualización de criterio usando un Procesador de Recursos de Actualización de criterios OSGi con la finalidad de efectuar las modificaciones al criterio de seguridad.

34.- El aparato según la reivindicación 33, en el cual el bloque de instrucciones de actualización de criterio comprende además una firma que corresponde con una parte transmisora de la cual se recibe el bloque de instrucciones de actualización de criterio, comprendido dicho aparato además:

un medio para verificar la firma para determinar si la parte transmisora está autorizada para modificar el criterio de seguridad.

35.- El aparato según la reivindicación 33, el cual comprende además:

un medio para recibir un nuevo componente de software asociado con el bloque de instrucciones de actualización de criterio; y

un medio para instalar el nuevo componente de software, en donde las modificaciones al criterio de seguridad conceden al nuevo componente de software permiso para acceder a una o más aplicaciones existentes de software instaladas en el dispositivo electrónico y a uno o más componentes existentes de software permiso para acceder al nuevo componente de software.

Resumen (para carátula Publicación WO)

(57) Una manera de proceder conveniente y segura es provista para actualizar el criterio de seguridad asociado con un dispositivo electrónico después que el usuario haya comprado el dispositivo y llevado el mismo para usarlo. En particular se provee una herramienta de generación de bloque de instrucciones que puede ser usada para crear un bloque de instrucciones de actualización de criterio que describe las modificaciones deseadas al criterio de seguridad del dispositivo electrónico. Adicionalmente se ha provisto un procesador de recursos OSGi, referido como procesador de recursos de actualización de criterio, estando el procesador de recursos de actualización de criterio dispuesto en el dispositivo electrónico y configurado para llevar a cabo las modificaciones al criterio de seguridad definido en el bloque de instrucciones de actualización de criterio.

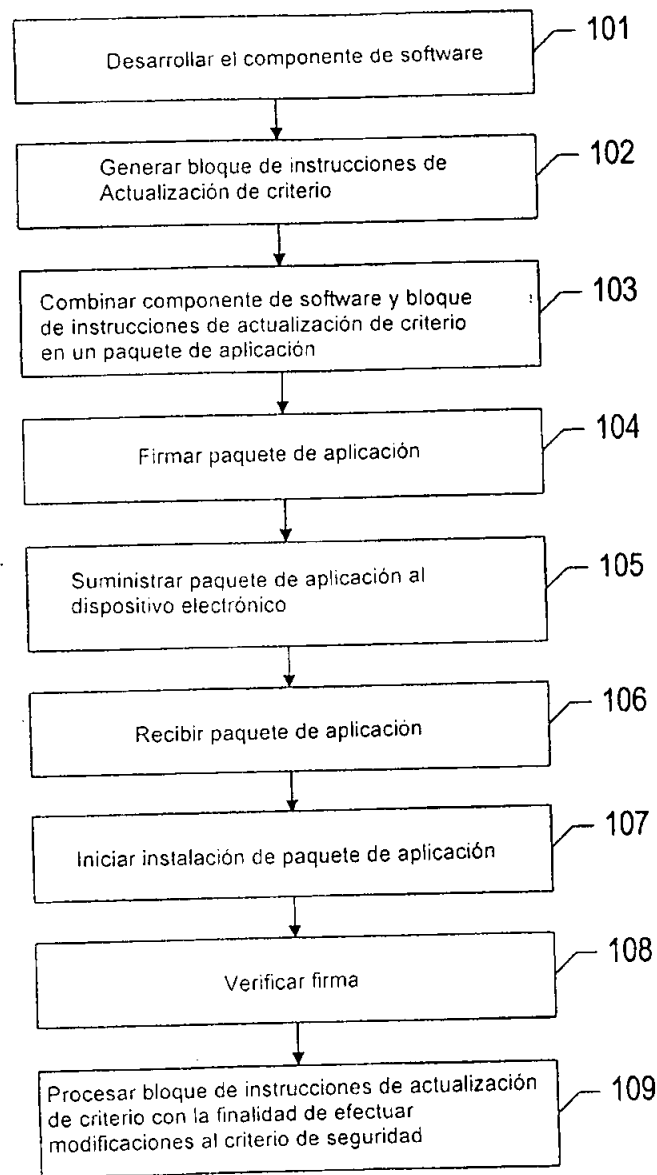


FIG. 1

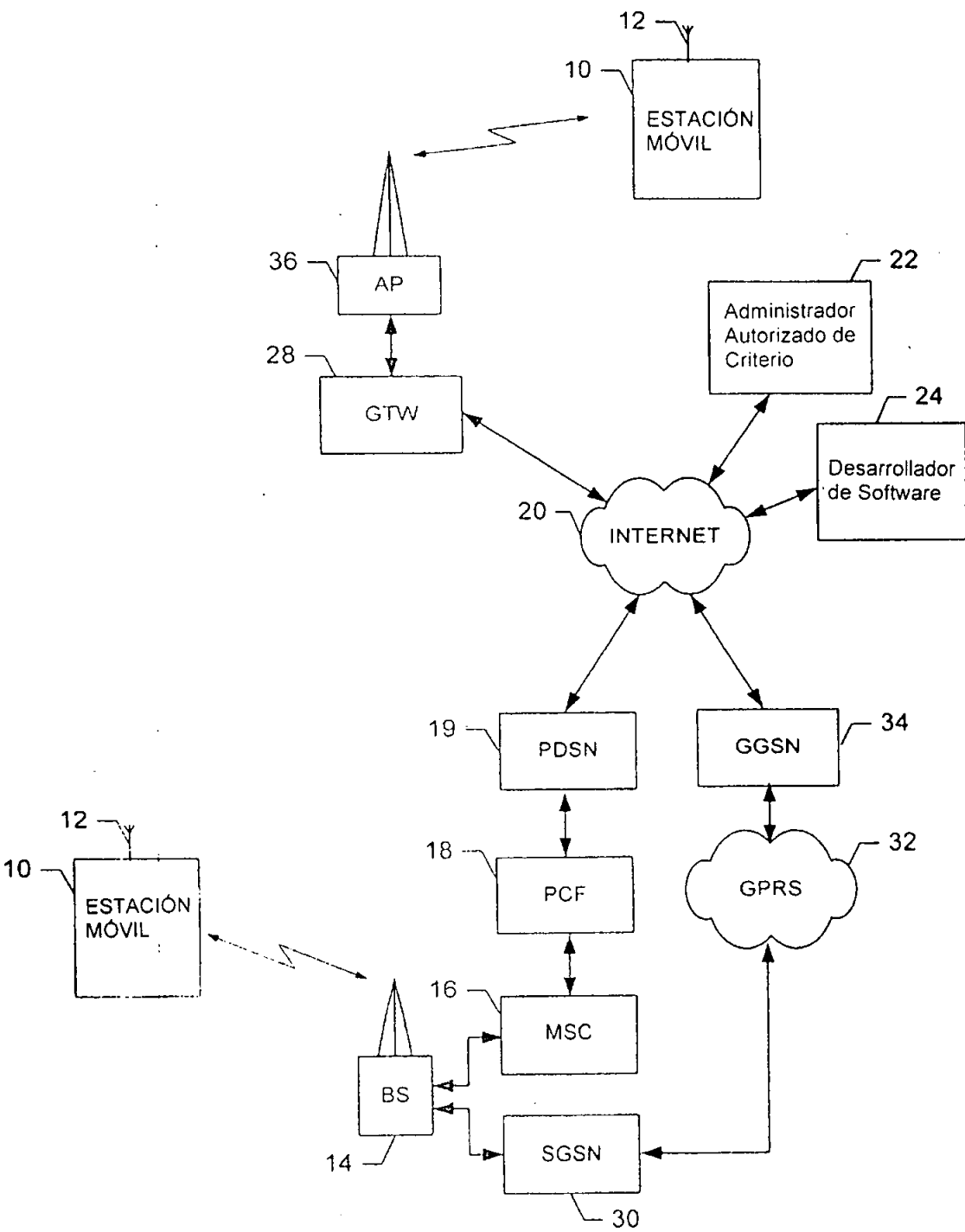


FIG. 2

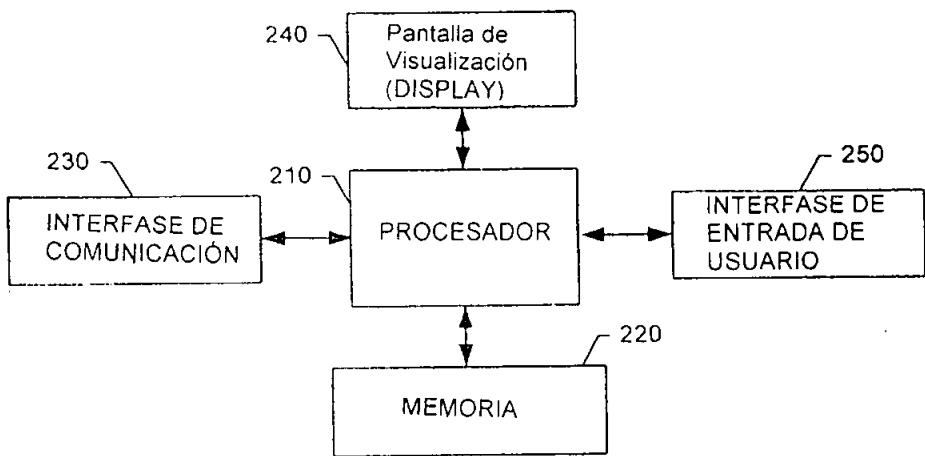


FIG. 3

10

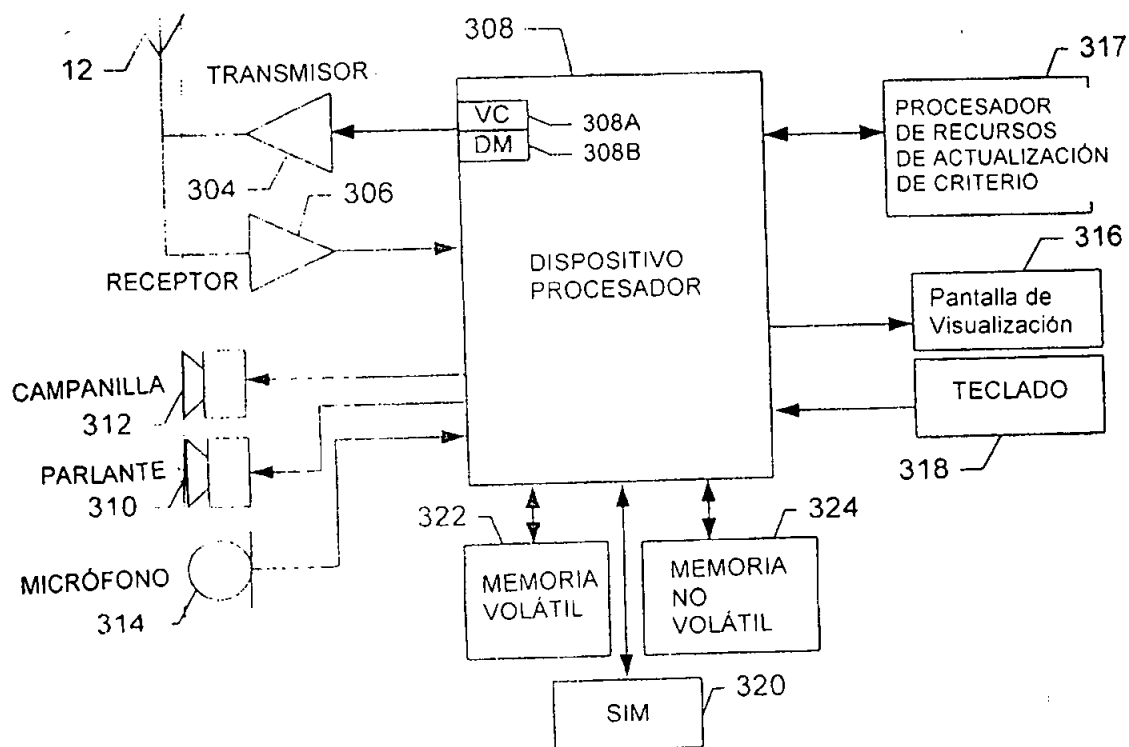


FIG. 4

Se. rectuz folio 99
Trujeta de Archivus.



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-001348- -00000-0000

Fecha: 2009-01-08 14:00:38 Dep. 2020 NUECREACION
Tra. 11 PATENTEYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 92

Delegatura de Propiedad Industrial
División de Nuevas Creaciones

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION
DEL TRÁMITE

	USUARIO	RADICADOR
PATENTE DE INVENCION (X) MODELO DE UTILIDAD ()	(X)	()
- Indicación de que se solicita la concesión de una patente	(X)	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	(X)	()
- Descripción de la invención	(X)	()
- Dibujos de ser estos pertinentes	(X)	()
- Comprobante de pago de las tasas establecidas	(X)	()

COMPLETA (X) INCOMPLETA ()

DISEÑO INDUSTRIAL ()

- Indicación de que se solicita el registro de Diseño Industrial	()	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
- Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño	()	()
- Comprobante de pago de las tasas establecidas	()	()

COMPLETA () INCOMPLETA ()

EZQUEMA DE TRAZADO ()

- Indicación de que se solicita el registro de Diseño Industrial	()	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
- Representación gráfica del Esquema de Trazado	()	()
- Comprobante de pago de las tasas establecidas	()	()

COMPLETA () INCOMPLETA ()

Firma responsable: Sandro Rodríguez

Fecha: Enco - 8-08