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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 January 2009 (08.01.2009)

PCT

(10) International Publication Number
WO 2009/005437 A1

(51) International Patent Classification:
H04L 9/14 (2006.01) *H04L 9/08* (2006.01)
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/SE2008/000417

(22) International Filing Date: 27 June 2008 (27.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0701596-9 29 June 2007 (29.06.2007) SE
60/960,559 3 October 2007 (03.10.2007) US

(71) Applicant *(for all designated States except US)*: **ONITEO AB** [SE/SE]; Danmarksgatan 46, S-164 40 Kista (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **THORSEN, Hans** [SE/SE]; Korsfararvägen 18, S-181 40 Lidingö (SE).

(74) Agent: **IPQ IP SPECIALISTS AB**; Mailbox 550, S-114 11 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) **Title:** METHOD AND SYSTEM FOR SECURE HARDWARE PROVISIONING

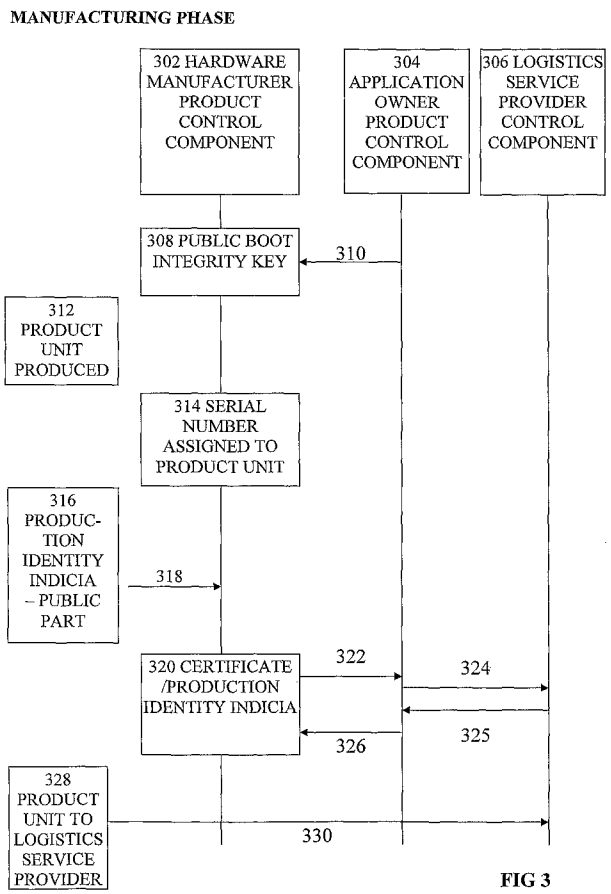

FIG 3

(57) **Abstract:** Provisioning a computer related product, comprising manufacturing a product at a product manufacturing entity; maintaining a product control database at product authenticity responsible entity; assigning a first identifier to the product for the purpose of establishing a boot integrity identity of the product, said first identifier being an asymmetric private-public encryption key pair stored in the product control database; storing a copy of the public part of said first identifier (public boot integrity key) in a memory of the product; assigning a second identifier to the product for the purpose of establishing a logistics identity of the product, said second identifier comprising manufacturing information such as a serial number for the product; storing said second identifier indicating the logistics identity in the product control database; assigning a third identifier for the product for the purpose of establishing a production identity of the product, said third identifier being an asymmetric private-public encryption key pair generated by activating an encryption key generator chip provided in the product; extracting and storing a copy of the public part of said third identifier indicating a production identity in the product control database; maintaining the private part of said third identifier indicating a production identity in a storage means of the product.

WO 2009/005437 A1

Method and system for secure hardware provisioning

Field of the Invention

The present invention relates generally to the provisioning of computer related hardware to end consumers. More particularly, the invention relates to a method and a system for provisioning computer related hardware products in a secure manner including authentication of the products in a manufacturing and delivery chain.

Background

In the current development of global economy, product suppliers by necessity tend to involve other parties to provide specialized services in the production and delivery of products to end consumers. Typically, such specialized services would for example include the manufacturing of products in a factory as well as logistics services for storing and transporting products from the factory to the end consumer. A consequence of this is that the product supplier does not have full physical control over the product in its journey from manufacture to the end consumer.

Product suppliers have a large responsibility for their products, sometimes over the whole product life cycle. This is particularly true for products that have a safety or security critical function. Other kinds of products may have important business functions and therefore be associated with great economic values. In general, it is a property for virtually all products that they carry the trademark and the good name of the product supplier and also for this reason the product suppliers are usually anxious to see to their products also after purchase.

Products that comprise hardware and software, i.e. computerized or other computer related products, are particularly sensitive to tampering and it is important that the product cannot be manipulated by a third party. Furthermore, with such products it is often important to update software and for natural

reasons of economy it is preferred to update the software via a data communications network such as the Internet or by means of some other distributed method. In the updating procedure it is important to know that the product is authentic, i.e. that it is a product for which the product supplier has a responsibility.

While there are a number of known methods for authentication, there is still a need for improvements with regard to the balance between security and convenience in operation. The latter concept also includes the concept of availability, which is used herein to refer to the ability to distribute and give service to a large number of computer related hardware units in an efficient and cost effective manner.

Related art

US20020023217 presents a method for uniquely identifying each manufactured device, in which each device is designated with its own public-private key pair. The public key is extracted from the devices. This method seeks to minimize the risk of misuse of the device.

US2006005253 shows a method for manufacturing trusted devices, in which a licensing authority provides unique keys to the hardware manufacturer(s). The trusted devices generate unique public and private key pairs.

US20060230271 discloses a method for distributing software keys to manufactures after placed order. A trusted party provides certificates, which are forwarded to the manufacturer and the device.

US20040139329 describes a method for assuring that correct handling of a device. Each manufacturer stores the serial numbers and public keys from every produced device. An enrollment authority maintains this data for later processes, e.g. backup or recovery processes.

US7099477 describes a method and a system for backing up trusted devices, in which the device's and the manufacturer's keys are used for assuring the identity of the device. If the authorization process approves the key combination the device is restored.

US6185678 describes a secure and reliable bootstrap architecture. The basic principle is sequencing the bootstrap process as a chain of progressively higher levels of abstraction, and requiring each layer to check a digital signature of the next layer before control is passed to it.

WO 0127770 describes a security device for a personal computer that interrupts the normal boot sequence to execute a secure operating system. The security device performs a number of integrity and security checks before initiating a non-secure operating system.

Object of the invention

The object of the present invention is to provide a method and a system for provisioning computer related products that enable the product supplier to maintain control over its products in all the phases of the product life cycle.

Summary of the invention

The solution is based on the establishment of a plurality of identifiers associated with an individual computer related product unit and generated in different phases of the manufacturing and provisioning chain of the product. The identifiers are cryptographically protected by means of asymmetric cryptography and are embedded in an identification entity, also called an ID bundle. An identifier is preferably generated in an encryption generator chip within the product, whereupon a public part of the identifier is extracted from the product whereas a private part of the identifier is stored and maintained within the product itself. An escrow key generated by a trusted escrow key

manager is further comprised in the identification entity for the purpose of encrypting data that is generated during execution of application software in a data processing system associated with the product. In case of product failure, data can be recovered by means of the escrow key obtained from the escrow key manager.

According to a first aspect of the invention, a method of provisioning a computer related product, comprises the steps of:
manufacturing a product at a product manufacturing entity;
maintaining a product control database at product authenticity responsible entity;
assigning a first identifier to the product for the purpose of establishing a boot integrity identity of the product, said first identifier being an asymmetric private-public encryption key pair stored in the product control database;
storing a copy of the public part of said first identifier (public boot integrity key) in a memory of the product;
assigning a second identifier to the product for the purpose of establishing a logistics identity of the product, said second identifier comprising manufacturing information such as a serial number for the product;
storing said second identifier indicating the logistics identity in the product control database;
assigning a third identifier for the product for the purpose of establishing a production identity of the product, said third identifier being an asymmetric private-public encryption key pair generated by activating an encryption key generator chip provided in the product;
extracting and storing a copy of the public part of said third identifier indicating a production identity in the product control database;
maintaining the private part of said third identifier indicating a production identity in a storage means of the product.

According to further aspects of the invention, the method is configured such that:

The first identifier indicating the boot integrity identity is generated by the product authenticity responsible entity.

The second identifier indicating the logistics identity is assigned to the product by the product manufacturing entity.

The encryption key generator chip is provided in the product by the product manufacturing entity as a part of the product manufacturing process.

A copy of the public part of the first identifier indicating the boot integrity identity is communicated comprised in a certificate in a signed message from the product authenticity responsible entity to the product manufacturing entity.

A copy of the second identifier indicating the logistics identity and a copy of the public part of the third identifier indicating a production identity are communicated comprised in a certificate in a signed message from the product authenticity responsible entity to the product manufacturing entity.

The method further comprises the steps of:

generating an escrow key at an escrow entity for the purposes of encrypting application data and having a data recovery emergency key in case of product hardware failure;

generating a fourth identifier for the product for the purpose of establishing an operational identity of the product, said first identifier being an asymmetric private-public encryption key pair;

generating an identification entity (ID bundle) comprising elements dependent on a selection of the first identifier indicating the boot integrity identity, the second identifier indicating logistics identity, the third identifier indicating a production identity, the fourth identifier indicating the operational identity and the escrow key,

storing the identification entity (ID bundle) in a product control database.

The method further comprises the steps of:
providing installer application software signed with the private part of the first identifier (private boot integrity key);
verifying the installer application software against the public part of the first identifier (public boot integrity key) stored in the product;
installing, if said verification is positive, operational software on a data processing system associated with the product;
providing a copy of the identification entity (ID bundle) and loading it into the product;
decrypting the content of the identification entity (ID bundle) by means of the private part of the third identifier indicating a production identity that is stored in the product;
distributing the decrypted content of the identification entity (ID bundle) in a file system of the data processing system associated with the product.

The method further comprises the steps of:
executing operational software and generate data by means of the product;
encrypting and storing generated data dependent on the escrow key of the identification entity.

The method further comprises the steps of:
substituting a failed product with a substituting product;
installing operational software and encrypted data into substituting product;
associating the identifiers of the failed product and the substituting product;
obtaining the escrow key associated with the failed product and inputting it to the substituting product;
decrypting and restoring the data within the substituting product by means of said escrow key.

The invention further comprises a system for provisioning a computer related product, the system comprising:

first product control components of a product authenticity responsible entity, having an encryption key generator, an identification entity generator and a database configured for storing encryption keys and identity indicia associated with product identities;

second product control components of a product manufacturing entity, having a manufacturing information manager and a certificate generator;

third product control components of a logistics responsible entity, having a database configured for storing identification entities associated with product identities;

fourth product control components of an escrow key responsible entity, having an escrow key generator and a secured database configured for secure storage of escrow keys associated with product identities.

A system for provisioning a computer related product comprising:

first product control components of a product authenticity responsible entity, having an encryption key generator, an identification entity generator and a database configured for storing encryption keys and identity indicia associated with product identities, said first product control components being adapted to assign a first identifier for the purpose of establishing a boot integrity identity for said computer related product;

second product control components of a product manufacturing entity, having a manufacturing information manager and a certificate generator, said second product control components being adapted to assign a second identifier for the purpose of establishing a logistics identity for said computer related product, and to assign a third identifier for the purpose of establishing a production identity for said computer related product.

Other aspects of the system, further comprises a selection of:

third product control components of a logistics responsible entity, having a database configured for storing identification entities associated with product identities.

fourth product control components of an escrow key responsible entity, having an escrow key generator and a secured database configured for secure storage of escrow keys associated with product identities.

The invention also comprises a computer program product for provisioning a computer related product, having an identification entity comprising identifier elements dependent on a boot integrity identity, a production identity and an escrow key.

More specific aspects of the invention are realized as a computer program product for provisioning a computer related product, adapted to realize an identification entity (ID bundle) comprising:
a first identifier element dependent on a boot integrity identity of the computer related product;
a fourth identifier element dependent on an operational identity of the computer related product;
an escrow key element of an escrow key.

Aspects of the computer program product are such that the identification entity (ID bundle) further comprises selections of:
a second identifier element dependent on a logistics identity of the computer related product;
a third identifier element dependent on a production identity of the computer related product.

According to an aspect of the invention, the computer program product is adapted to providing a copy of the identification entity (ID bundle) and loading it into the computer related product; distributing the content of the identification entity (ID bundle) in a file system of the data processing system associated with the computer related product.

The invention is further realized as a computer related product having data storage means and an encryption key generator chip, comprising :
a public part of a first identifier (public boot integrity key) stored in said data storage means of the product, said first identifier being an asymmetric private-public encryption key pair being assigned to the product for the purpose of establishing a boot integrity identity of the product;
a private part of a third identifier indicating a production identity in said storage means of the product, said third identifier being an asymmetric private-public encryption key pair generated by activating said encryption key generator chip provided in the product and being assigned for the product for the purpose of establishing a production identity of the product.

Further aspects of the computer related product are further being assigned a selection of:
a second identifier indicating the logistics identity by the product manufacturing entity, said second identifier being stored in a product control database;
an escrow key generated at an escrow entity for the purposes of encrypting application data and having a data recovery emergency key in case of product hardware failure;
a fourth identifier generated for the product for the purpose of establishing an operational identity of the product, said first identifier being an asymmetric private-public encryption key pair;
an identification entity (ID bundle) generated to comprise elements dependent on a selection of the first identifier indicating the boot integrity identity, the second identifier indicating logistics identity, the third identifier indicating a production identity, the fourth identifier indicating the operational identity and the escrow key,
the identification entity (ID bundle) being stored in a product control database.

The computer related product claim, further comprises:
installer application software signed with the private part of the first identifier (private boot integrity key);
and is adapted for:
verifying the installer application software against the public part of the first identifier (public boot integrity key) stored in the product;
installing, if said verification is positive, operational software on a data processing system associated with the product;
obtaining a copy of the identification entity (ID bundle) and loading it into the product;
decrypting the content of the identification entity (ID bundle) by means of the private part of the third identifier indicating a production identity that is stored in the product;
distributing the decrypted content of the identification entity (ID bundle) in a file system of a data processing system associated with the product.

The computer related product is optionally further adapted for:
executing operational software and generate data by means of the product;
encrypting and storing generated data dependent on the escrow key of the identification entity.

Brief Description of Drawings

The present invention will be further explained with reference to the accompanying drawings, in which:
FIG 1 shows an overview of actors in an embodiment of the provisioning architecture of the invention.
FIG 2 shows an overview of phases in an embodiment of the provisioning chain of the invention.
FIG 3 shows an overview of communications in an embodiment of the manufacturing phase of the invention.

FIG 4 shows an overview of communications in an embodiment of the delivery phase of the invention.

FIG 5 shows an example of an ID bundle according to an embodiment of the invention.

Detailed Description of Preferred Embodiments

Overview

The present invention comprises architecture for provisioning and assuring the identity of a computer related or a computerized product throughout the whole lifecycle of the product. The terms computer related product and computerized product is in this context intended to mean a hardware product comprising a data processing system or a product devised for association with a data processing system, such as a data carrier or data memory, an I/O unit or a peripheral device.

The lifecycle of a computer related product comprises a number of different phases that includes a manufacturing phase and a delivery phase comprised in a provisioning chain as well as an operational phase in the hands of an end consumer. Typically, and according to an embodiment exemplified herein, the product supplier, here also called the Application owner, buys specialized services from different actors that are responsible for the product in the respective phases of the provisioning chain. The specialized services may also, as in another embodiment, be implemented within a single actor but all having their respective responsibilities.

An identification entity preferably in the shape of an ID bundle is generated for each product unit. The ID bundle comprises identification indicia preferably constituted by encrypted certificates originating from or comprising elements from different actors and phases in the provisioning chain.

The identification entity is used in different situations in the operational phase to establish the identity and authenticity of the product unit. The identification indicia are protected by encryption keys that are known and used by different actors. A backup system with encryption keys kept in escrow is provided for the case of complete product failure and replacement of the product in order to recover data also when the product itself must be changed.

The invention comprises product control components of a product control system comprised in the invention. The different product control components are housed and used by each of the different actors, and are devised for generating identification indicia and for communication with other actors and their respective product control components. The different actors that are thus responsible for the different phases of the provisioning chain and the product lifecycle are connected or connectable preferably by means of these product control components to exchange signed messages regarding the individual product units.

In one embodiment, each individual product unit is provided with a security enhanced BIOS as described in the co-pending patent applications SE0600416-2 and PCT/SE2007/000169, the contents of which are hereby incorporated by reference.

In a preferred embodiment, each product unit comprises, thus optionally but not necessarily, a tamper proof encryption key generator chip. This encryption key generator chip is for example an RSA chip, by means of which production identity indicia constituted by a first pair of a private and a public encryption key are generated in the final stage of the manufacturing procedure.

At one stage in the provisioning chain, for example when an end consumer has been designated for a specific product unit, an ID Bundle is generated comprising indicia that are dependent on the public encryption key of the

production identity indicia. The ID Bundle is preferably further provided to comprise operational identity indicia dependent on a another pair of a private encryption key and a public encryption key.

The operational identity indicia of the ID Bundle are in this case encrypted against the public encryption key of the product identity indicia and a public part of at least one escrow key. The escrow key is used to enable recovery of data that has been encrypted by the product unit itself, in case the encryption key has been lost. The escrow key is obtainable from an independent Escrow partner, which is one of the actors in the provisioning chain.

The result is that the identity of the individual product unit is assured during the whole life cycle of the product. This solution enables secure transfer of sensitive data generated in the product unit to another unit that is deployed with an ID Bundle in a corresponding manner. Secure transfer includes for example secure message passing, backup and restore even in a hostile environment where the units are disconnected from a supervising system.

In one embodiment, the product unit is a computerized product wherein for example a motherboard of a data processing system is provided with an encryption key generator chip. The identification entity is generated and maintained for a computerized product based on this motherboard. The identity and the authenticity are in this case directly coupled to the motherboard itself.

In another embodiment, the product unit is a computer related product in the shape of a data carrier, e.g. a USB storage device, that is provided with an encryption key generator chip and preferably a read only memory sector. In this case, the identification entity is thus generated and maintained for the data carrier. In an application of this embodiment the data carrier is provided with boot software and installation image software stored in the read only memory sector. In a case where the application owner is responsible for a computerized

system comprising for example a standard PC or a PC motherboard, the computerized system can be manufactured, assembled and delivered to the end customer in an unsafe manner. The data carrier is also distributed to the end consumer, who couples the data carrier to the computerized system and boots the computerized system from the data carrier. In a current practical implementation, the data carrier is a USB stick and the computerized system comprises a standard PC computer that has the capability to boot from a data carrier connected to a USB port. The installation image software on the data carrier is then executed and trusted operating system software is installed on the computerized system under the identity and the authenticity of the data carrier. The effect is that the computerized system with the trusted operating system software is associated with the identity and authenticity of the data carrier, and thus in a sense inherits the quality and the capability of being identified and authenticated from the data carrier.

Actors

Fig 1 shows schematically the basic actors in a provisioning chain or a product supply chain according to an embodiment of the invention, which comprises:

1. An application owner 1 (the product supplier).
2. An escrow key manager 2, i.e. a trusted party where escrow keys are generated and deposited. The escrow key manager should preferably be an authority or some other organization without any commercial interests and should be equipped with specific rules for delivering or handing over escrow keys for example to an application owner or to an end consumer.
3. A hardware manufacturer 3 engaged by the application owner to manufacture the hardware of products. Thus a co-actor of the application owner.

4. A logistics service provider 4 engaged by the application owner to carry out the transport of the products from the hardware manufacturer to an end consumer. Thus a co-actor of the application owner
5. An End consumer 5 buying the product from the application owner.

The provisioning chain may also, as shown in Fig 1, comprise a software partner 6 engaged by the application owner to provide the service to develop and manufacture software, as well as a software deployment partner 7 similarly engaged by the application owner to distribute and deploy the software to the hardware product and the end consumer.

Product control components

Different actors of the provisioning chain in a system for provisioning a computer related or a computerized product are provided with product control components of a product control system devised to support the generation and communication of product identity indicia.

A product control system of the provisioning system according to an embodiment of the invention comprises:

1. Application owner product control components comprising: an operational encryption key generator; an ID Bundle generator; a production key generator preferably in the shape of a CA server, a database for storing encryption keys associated with specific product units and a connectivity server devised to associate the product identity information with communication identity.
2. Escrow key manager product control components comprising: a CA server devised to generate escrow keys, and a secured database for secure storage of the private part of the escrow keys.
3. Hardware manufacturer product control components comprising: means devised to initiate generation of the production identity indicia preferably by means of a tamper proof RSA chip and extraction of the public encryption key of said production identity indicia; a manufacturing information manager

devised to handle assignment and communication of serial numbers for the manufactured product units; a certificate generator devised to generate a certificate associating the public encryption key of said production identity indicia with said manufacturing information. These functional components may be integrated in a factory server.

4. Logistics service provider product control components comprising a logistics server devised to store ID Bundles and to provide installation support.

The product control components are devised to exchange signed and/or encrypted messages.

Method for secure provisioning

A method for provisioning and product control according to an embodiment of the invention comprises the following phases and steps. Fig 2 shows schematically an overview of the main phases of the method.

1. A setup phase 201, comprising the steps wherein:
   a. A trusted relationship is established between the application owner and his co-actors, more specifically the escrow key manager, the hardware manufacturer, and the logistics service provider, respectively.
   b. The application owner establishes product control routines with its co-actors.
   c. The application owner installs product control components at the sites of its co-actors and provides said product control components with certificates in a trusted PKI domain. The trusted relationship (see a. above) between the Application owner and his co-actors is embodied and maintained by means of the product control components, which are used for secure communication between the actors.

2. A manufacturing phase 202, shown in more detail in Fig 3, comprising the steps wherein:

a. The hardware manufacturer product control component 302 receives a public boot integrity key 308 in a signed message 310 from the application owner product control component 304. The public boot integrity key 308 has thus been generated and established in advance by the application owner as the public part of an encryption key pair.

b. A product unit 312 is produced, for example a data processor unit motherboard or a data carrier in the shape of a USB data storage device.

c. The product unit 312 is provided with an encryption key generator chip in the shape of an RSA chip.

d. A logistics identity indicia comprising manufacturing information, e.g. serial number, is assigned to the product unit 314.

e. Production identity indicia 316 are generated by activating the RSA chip and thereby generating an asymmetric key pair comprising a private and a public encryption key. The private key stays inside the RSA chip.

f. The public key of the production identity indicia is extracted from the RSA chip.

g. A copy of the public boot integrity key is stored in a memory of the product unit. In the exemplifying case where the product unit is a data processing unit motherboard, the public boot integrity key is stored in a parameter memory, and in the case with the data carrier the public boot integrity key is stored in a read only devised memory section.

h. A factory certificate comprising the public encryption key of the production identity indicia and the logistics identity indicia with the manufacturing information is generated 320.

i. A signed message 322,326 with the certificate comprising the public encryption key of the production identity indicia and the manufacturing information is sent, on-line or off-line, from the hardware manufacturer 302 to the Application owner 304.

j. The Application owner 304 verifies the authenticity of the factory message and stores 324,325 the certificate and its content in the logistics server database 306.

k. The product unit 312,328 is handed over 330 to the logistics service provider 306.

3. A delivery phase 203, shown in more detail in Fig 4, comprising the steps wherein:
   a. An end costumer 402 places an order 404 for a product unit with the Application owner via a business adapter 406 of the application owner product control components.
   b. The Application owner sends 407 an order 408 for delivery of a product unit to a Logistics module 410 of the Logistics service provider product control components.
   c. The Logistics service provider selects 412 a product unit to deliver and sends 409 the logistics identity indicia (comprising manufacturing information) of the selected product unit to the Application owner production control component 406.
   d. An escrow certificate 414 for the product unit is generated 413,415 by means of a CA server 416 of the Escrow actor.
   e. A factory certificate 416, i.e. a certificate comprising the production identity indicia and the logistics identity indicia is retrieved (Get BOOT_CERT) 417,419 from a logistics server 418.
   f. Operational identity indicia (for step 420) in the shape an asymmetric private-public encryption key pair is generated 421,422 by means of a CA server 416 of the Application owner.
   g. An ID Bundle 420 is created based on the operational identity indicia keys.
   h. The public part of the operational identity indicia 424 (Store Certificate) is stored 423,425 in a connectivity server 426 of the Application owner.
   i. The ID Bundle associated with the factory certificate is stored 428, 430 in the logistics server 418.
   j. The product unit is delivered to the end consumer ready for installation and operation.

4. An operational phase 204, comprising an installation procedure 205, an operational procedure 206 and a recovery procedure 207 according to the following:

An installation procedure 205 comprising the steps wherein:

a. The End consumer is provided with installer application software from the Application owner. The installer application software is signed with the private boot integrity key that corresponds to the public boot integrity key stored in the product unit. In an embodiment where the product unit is a data carrier, the installer application software is preferably stored on the data carrier but may also be downloaded or distributed in other manners.

b. The installer application software is verified against the public key stored in the memory of the product unit, and if the verification is positive the product unit grants access for execution to the installer application software, else (i.e. if the verification is negative) the product unit rejects execution of said software and the installation procedure ends.

c. If thus granted access for execution, the installer application software prepares media and installs operational software on a data processing system of or associated with the product unit.

d. The ID Bundle that corresponds to the specific product unit and the public part of the production identity indicia are obtained from the Application owner, for example delivered by the logistics service provider or obtained by the product itself by means of functions in the installer application software.

e. The ID Bundle is loaded into the product unit and is decrypted using the production private key stored in the tamper proof RSA chip of the product unit.

f. The decrypted content, i.e. the private and public parts of the operational identity indicia, of the ID Bundle is distributed in the file system of the

product unit. At the same time the installer application software provides the product with the certificate of the connectivity server of the Application owner.

g. The product now has its own operational identity and the identity of a trusted communication path given by the certificate of the connectivity server.

An operational procedure 206, comprising the steps wherein:

h. The product unit executes the operational software and generates data.

i. Data generated by the product unit is encrypted dependent on the escrow encryption key of the ID bundle and stored outside the product unit as a part of a backup storage process.

A Recovery procedure 207 for substituting failed hardware of a product unit, comprising the steps wherein:

j. A second product unit to substitute the failed product unit is installed as in the above installation procedure.

k. Data recovery application software is installed on said second product unit together with the encrypted backup data from the first product unit.

l. The End consumer requests data recovery assistance from the Application owner with the logistics identity indicia of the failed product unit and the second, substituting product unit as input.

m. The Application owner requests the escrow key for the logistics identity indicia of the failed product unit from the Escrow key manager.

n. The Application owner obtains the public key of the operational identity indicia based on the logistics identity indicia of the substituting product unit from the connectivity server.

o. The Application owner encrypts the private part of the escrow key with the public part of the operational key of the substituting product unit.

p. The application owner transfers the encrypted private part of the escrow key to the recovery application software of the substituting product unit.

q. The private part of the escrow key is decrypted with the private part of the operational key of the substituting product unit.
r. The backup information is decrypted with the private part of the escrow key and is restored in the substituting product unit.
s. The substituting product unit goes into an operational procedure as above.

In a case where the identity and the authenticity is carried by the data carrier and the associated data processing system hardware fails, only the data processing system hardware needs be substituted and the installation procedure be repeated. Thereby the identity and the authenticity of the data carrier are associated with the new hardware. The encrypted data is then recovered by means of the encryption keys comprised in the ID bundle stored in the data carrier.

Identification entity

The identification entity is in a preferred embodiment, as has been described above, compiled and realized as an ID Bundle comprising a plurality of elements associated with different phases of the provisioning chain.

In an embodiment of the invention, the ID Bundle comprises a selection of:

1. The private encryption key of the operational identity indicia.
2. The public encryption key of the operational identity indicia embedded in for example an X509 certificate that associates the public key with manufacturing information, wherein the certificate is signed by the application owner (product supplier).
3. A first copy of a temporary session key used to symmetrically encrypt said private encryption key of the operational identity indicia and said certificate that embeds the public encryption key of the operational identity indicia, wherein said temporary session key is encrypted against the public encryption key of the production identity indicia.

4. A second copy of said temporary session key encrypted against an escrow key (at least one).

Fig 5 shows another example of an ID bundle 502 according to an embodiment of the invention and comprising an escrow certificate 504 encrypted with a session key, a boot certificate 506 encrypted with the session key and an identity certificate 508 for the product unit encrypted with the session key.

The different aspects of the invention have been described by means of specific examples. The invention may however be realized in a variety of manners within the scope of the accompanying claims.

Claims

1. A method of provisioning a computer related product, comprising the steps of:

manufacturing a product at a product manufacturing entity;

maintaining a product control database at product authenticity responsible entity;

assigning a first identifier to the product for the purpose of establishing a boot integrity identity of the product, said first identifier being an asymmetric private-public encryption key pair stored in the product control database;

storing a copy of the public part of said first identifier (public boot integrity key) in a memory of the product;

assigning a second identifier to the product for the purpose of establishing a logistics identity of the product, said second identifier comprising manufacturing information such as a serial number for the product;

storing said second identifier indicating the logistics identity in the product control database;

assigning a third identifier for the product for the purpose of establishing a production identity of the product, said third identifier being an asymmetric private-public encryption key pair generated by activating an encryption key generator chip provided in the product;

extracting and storing a copy of the public part of said third identifier indicating a production identity in the product control database;

maintaining the private part of said third identifier indicating a production identity in a storage means of the product.

2. The method of claim 1, wherein said first identifier indicating the boot integrity identity is generated by the product authenticity responsible

entity.

3. The method of any of the preceding claims, wherein said second identifier indicating the logistics identity is assigned to the product by the product manufacturing entity.

4. The method of any of the preceding claims, wherein the encryption key generator chip is provided in the product by the product manufacturing entity as a part of the product manufacturing process.

5. The method of any of the preceding claims, wherein a copy of the public part of the first identifier indicating the boot integrity identity is communicated comprised in a certificate in a signed message from the product authenticity responsible entity to the product manufacturing entity.

6. The method of any of the preceding claims, wherein a copy of the second identifier indicating the logistics identity and a copy of the public part of the third identifier indicating a production identity are communicated comprised in a certificate in a signed message from the product authenticity responsible entity to the product manufacturing entity.

7. The method of any of the preceding claims, further comprising the steps of:

generating an escrow key at an escrow entity for the purposes of encrypting application data and having a data recovery emergency key in case of product hardware failure;

generating a fourth identifier for the product for the purpose of establishing an operational identity of the product, said fourth identifier being an asymmetric private-public encryption key pair;

generating an identification entity (ID bundle) comprising elements dependent on a selection of the first identifier indicating the boot integrity identity, the second identifier indicating logistics identity, the third identifier indicating a production identity, the fourth identifier indicating the operational identity and the escrow key,

storing the identification entity (ID bundle) in a product control database.

8. The method of the preceding claim, further comprising the steps of:

providing installer application software signed with the private part of the first identifier (private boot integrity key);

verifying the installer application software against the public part of the first identifier (public boot integrity key) stored in the product;

installing, if said verification is positive, operational software on a data processing system associated with the product;

providing a copy of the identification entity (ID bundle) and loading it into the product;

decrypting the content of the identification entity (ID bundle) by means of the private part of the third identifier indicating a production identity that is stored in the product;

distributing the decrypted content of the identification entity (ID bundle) in a file system of the data processing system associated with the product.

9. The method of the preceding claim, further comprising the steps of:

executing operational software and generate data by means of the product;

encrypting and storing generated data dependent on the escrow key of the identification entity.

10. The method of the preceding claim, further comprising the steps of:

substituting a failed product with a substituting product;

installing operational software and encrypted data into substituting product;

associating the identifiers of the failed product and the substituting product;

obtaining the escrow key associated with the failed product and inputting it to the substituting product;

decrypting and restoring the data within the substituting product by means of said escrow key.

11. A system for provisioning a computer related product comprising:

first product control components of a product authenticity responsible entity, having an encryption key generator, an identification entity generator and a database configured for storing encryption keys and identity indicia associated with product identities, said first product control components being adapted to assign a first identifier for the purpose of establishing a boot integrity identity for said computer related product;

second product control components of a product manufacturing entity, having a manufacturing information manager and a certificate generator, said second product control components being adapted to assign a second identifier for the purpose of establishing a logistics identity for said computer related product, and to assign a third identifier for the purpose of establishing a production identity for said computer related product.

12. The system of claim 11, further comprising

third product control components of a logistics responsible entity, having a database configured for storing identification entities

associated with product identities.

13. The system of claim 11, further comprising

fourth product control components of an escrow key responsible entity, having an escrow key generator and a secured database configured for secure storage of escrow keys associated with product identities.

14. A computer program product for provisioning a computer related product, adapted to realize an identification entity (ID bundle) comprising:

a first identifier element dependent on a boot integrity identity of the computer related product;

a fourth identifier element dependent on an operational identity of the computer related product;

an escrow key element of an escrow key.

15. The computer program product of claim 14, wherein the identification entity (ID bundle) further comprises:

a second identifier element dependent on a logistics identity of the computer related product.

16. The computer program product of claim 14, wherein the identification entity (ID bundle) further comprises:

a third identifier element dependent on a production identity of the computer related product.

17. The computer program product of claim 14, further being adapted to

providing a copy of the identification entity (ID bundle) and loading it into the computer related product;

distributing the content of the identification entity (ID bundle) in a

file system of the data processing system associated with the computer related product.

18. A computer related product having data storage means and an encryption key generator chip, comprising :

a public part of a first identifier (public boot integrity key) stored in said data storage means of the product, said first identifier being an asymmetric private-public encryption key pair being assigned to the product for the purpose of establishing a boot integrity identity of the product;

a private part of a third identifier indicating a production identity in said storage means of the product, said third identifier being an asymmetric private-public encryption key pair generated by activating said encryption key generator chip provided in the product and being assigned for the product for the purpose of establishing a production identity of the product.

19. The computer related product of claim 14, further being assigned a second identifier indicating the logistics identity by the product manufacturing entity, said second identifier being stored in a product control database.

20. The computer related product of claim 14, further being assigned:

an escrow key generated at an escrow entity for the purposes of encrypting application data and having a data recovery emergency key in case of product hardware failure;

a fourth identifier generated for the product for the purpose of establishing an operational identity of the product, said first identifier being an asymmetric private-public encryption key pair;

an identification entity (ID bundle) generated to comprise elements dependent on a selection of the first identifier indicating the

boot integrity identity, the second identifier indicating logistics identity, the third identifier indicating a production identity, the fourth identifier indicating the operational identity and the escrow key,

the identification entity (ID bundle) being stored in a product control database.

21. The computer related product of the preceding claim, further comprising:

installer application software signed with the private part of the first identifier (private boot integrity key);

and being adapted for:

verifying the installer application software against the public part of the first identifier (public boot integrity key) stored in the product;

installing, if said verification is positive, operational software on a data processing system associated with the product;

obtaining a copy of the identification entity (ID bundle) and loading it into the product;

decrypting the content of the identification entity (ID bundle) by means of the private part of the third identifier indicating a production identity that is stored in the product;

distributing the decrypted content of the identification entity (ID bundle) in a file system of a data processing system associated with the product.

22. The computer related product of the preceding claim, further being adapted for:

executing operational software and generate data by means of the product;

encrypting and storing generated data dependent on the escrow key of the identification entity.

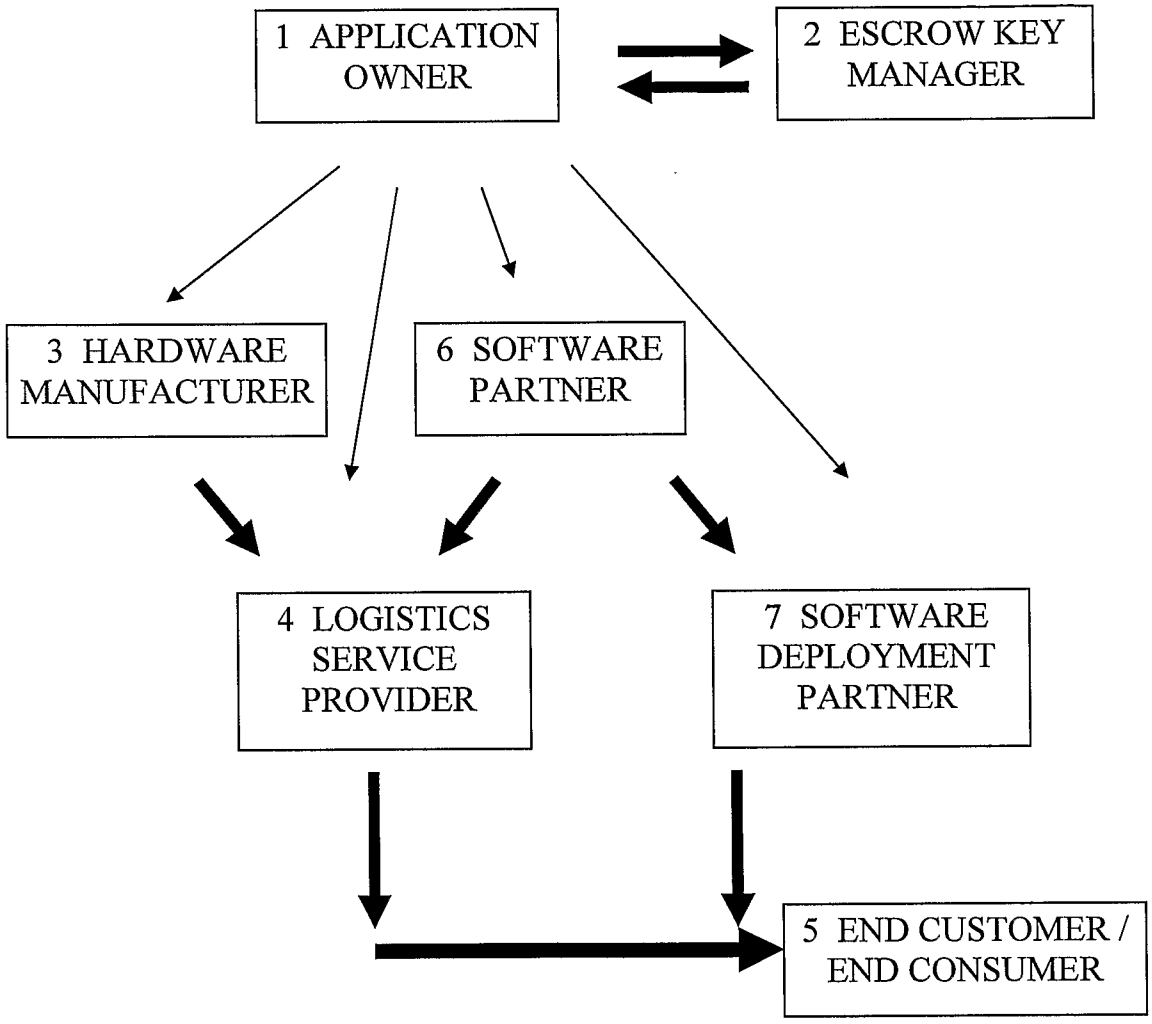
1 APPLICATION OWNER
2 ESCROW KEY MANAGER
3 HARDWARE MANUFACTURER
6 SOFTWARE PARTNER
4 LOGISTICS SERVICE PROVIDER
7 SOFTWARE DEPLOYMENT PARTNER
5 END CUSTOMER / END CONSUMER

FIG 1

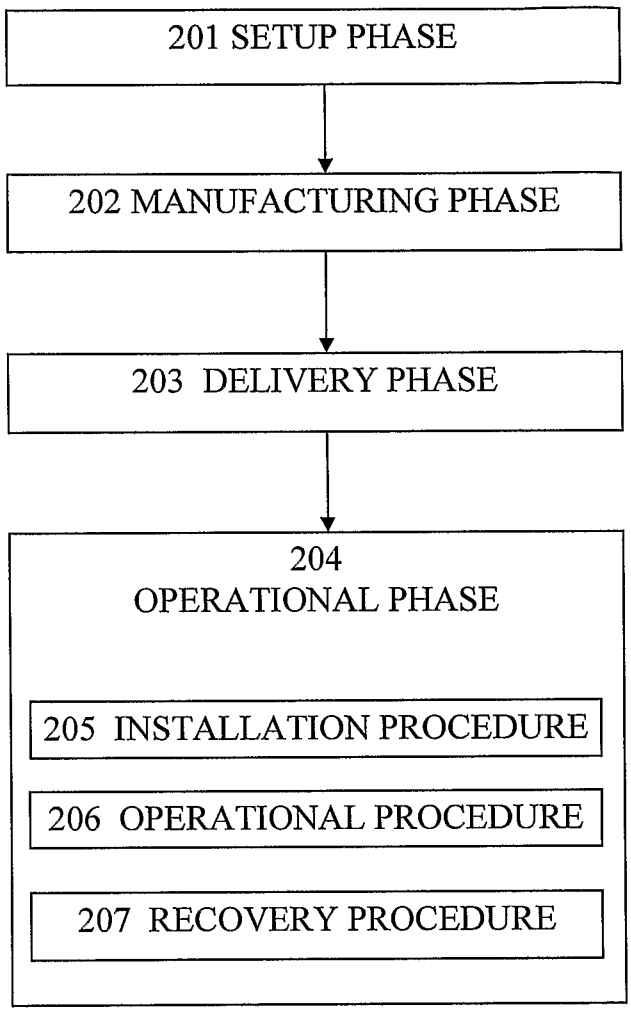
201 SETUP PHASE
202 MANUFACTURING PHASE
203 DELIVERY PHASE
204
OPERATIONAL PHASE
205 INSTALLATION PROCEDURE
206 OPERATIONAL PROCEDURE
207 RECOVERY PROCEDURE

FIG 2

MANUFACTURING PHASE

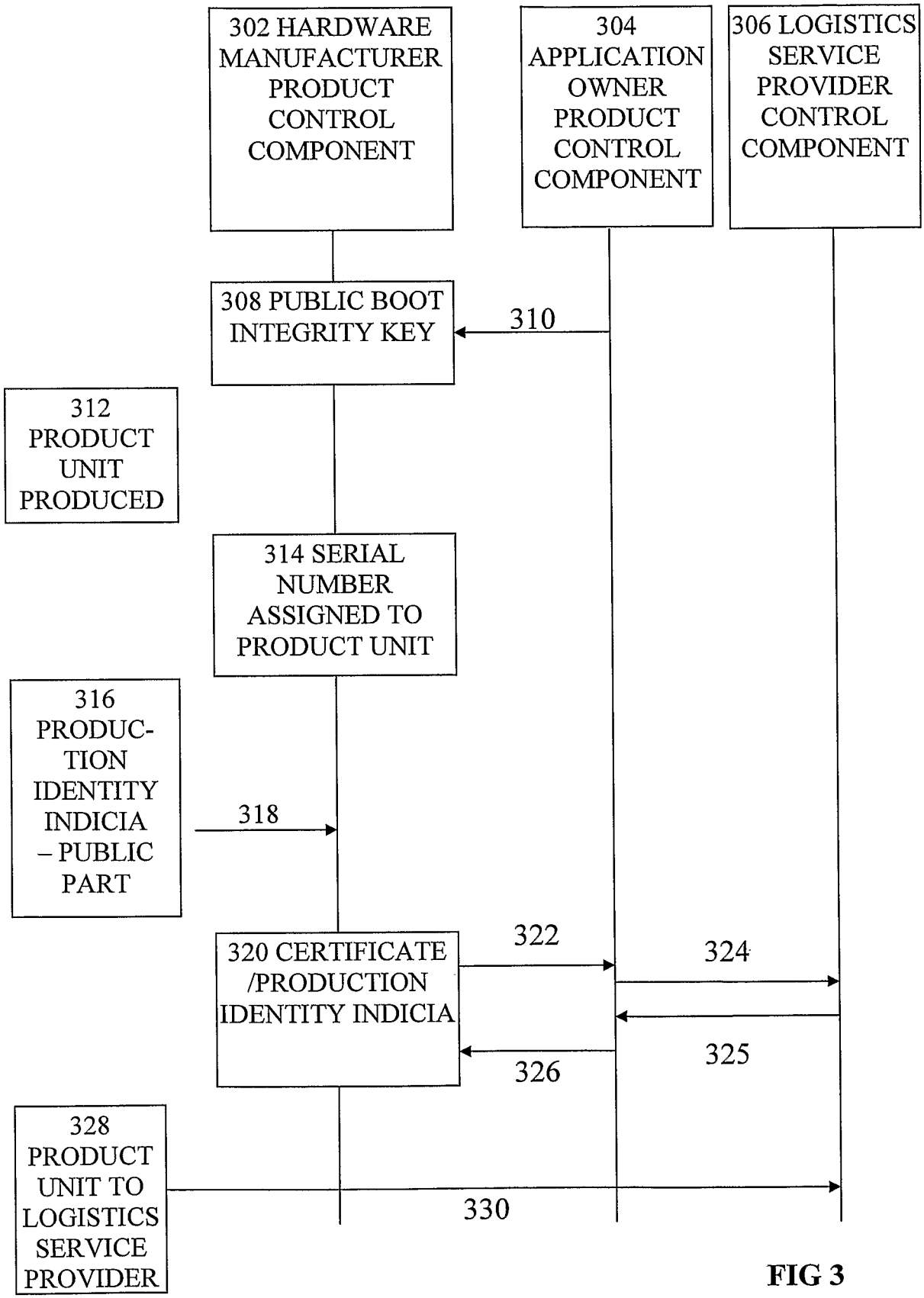

FIG 3

DELIVERY PHASE

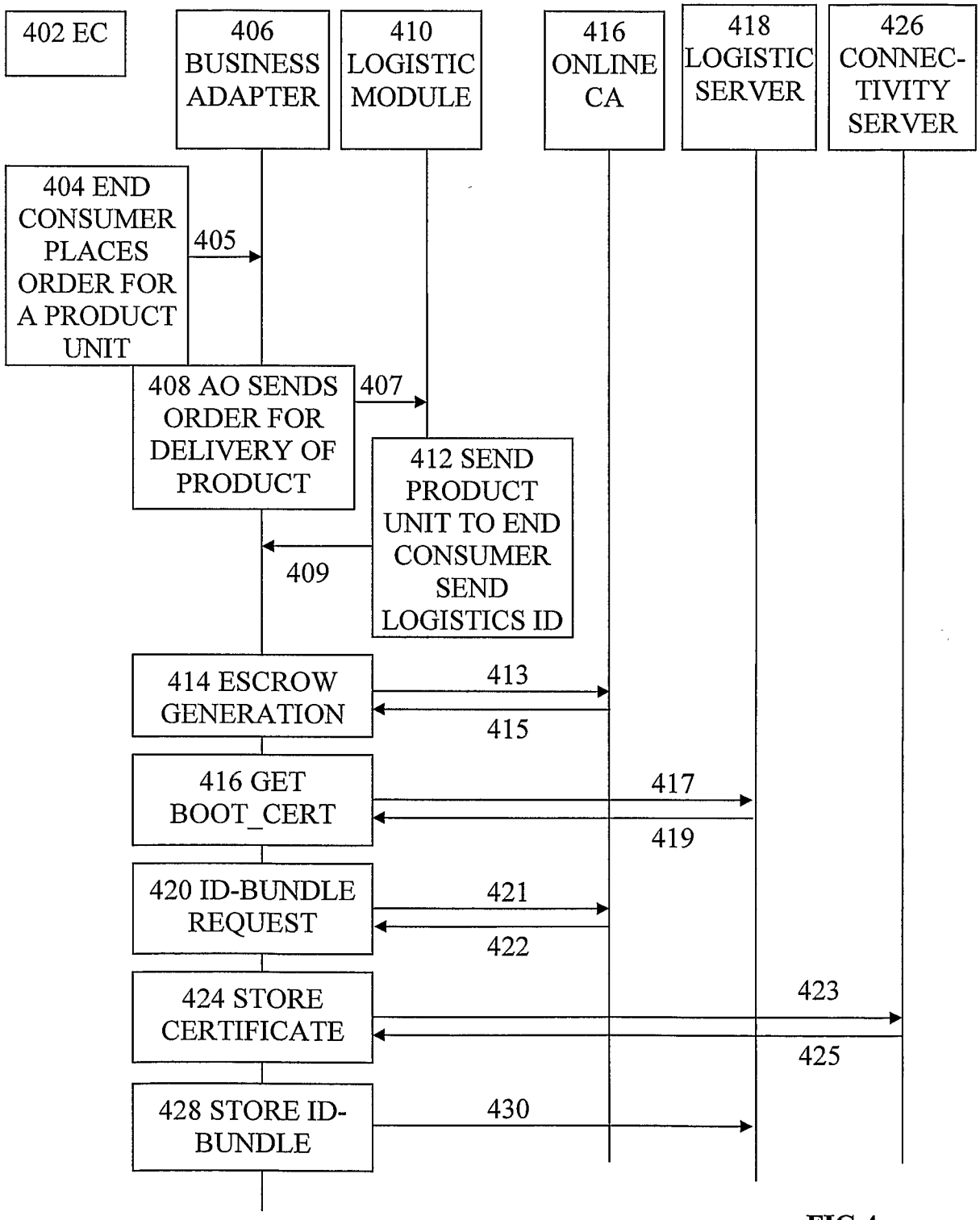

FIG 4

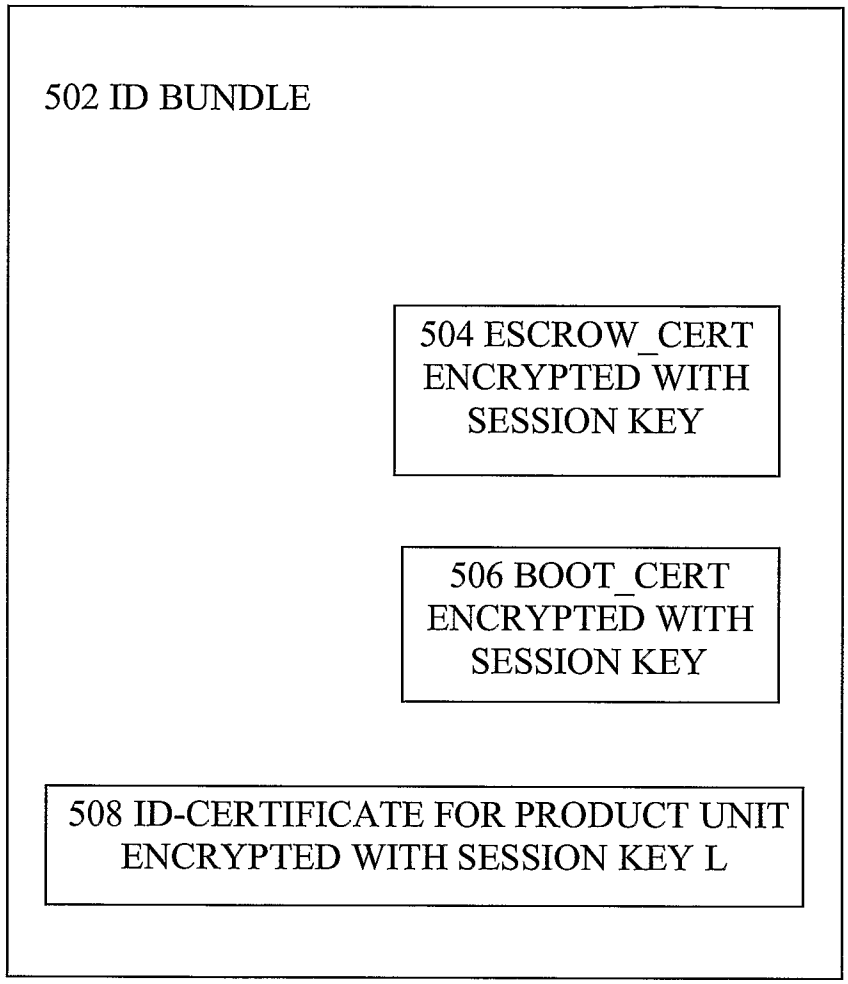
502 ID BUNDLE
504 ESCROW_CERT ENCRYPTED WITH SESSION KEY
506 BOOT_CERT ENCRYPTED WITH SESSION KEY
508 ID-CERTIFICATE FOR PRODUCT UNIT ENCRYPTED WITH SESSION KEY L

FIG 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000417

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: G06F, G06Q, H04L

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, INSPEC, COMPDX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20040030901 A1 (WHEELER, L H ET AL), 12 February 2004 (12.02.2004), claims 1-2, abstract ---	1-22
A	US 5841865 A1 (SUDIA, F W), 24 November 1998 (24.11.1998), column 15, line 50 - line 59; column 16, line 60 - column 17, line 27, claim 1, abstract ---	1-22
A	US 20040205362 A1 (CATHERMAN, R C ET AL), 14 October 2004 (14.10.2004), paragraph [0013] ---	1-22

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 October 2008	07-10-2008
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 Frida Holmberg/PR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000417

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5563950 A1 (EASTER, R J ET AL), 8 October 1996 (08.10.1996), claims 1-12, abstract ---	1-22
A	WO 2004054208 A1 (AUSTRALIA AND NEW ZEALAND BANKING GROUP LIMITED), 24 June 2004 (24.06.2004), claims 1-10, abstract ---	1-22
A	US 20060053025 A1 (MERTENS, R), 9 March 2006 (09.03.2006), paragraphs [0008],[0019]-[0021] ---	1-22
A	US 20030221107 A1 (KANG, C-U), 27 November 2003 (27.11.2003), abstract --- --------	1-22

International patent classification (IPC)
H04L 9/14 (2006.01)
G06F 21/02 (2006.01)
H04L 9/08 (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 **CWYIHOUFFU**.

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.