

(19)



(11)

EP 1 161 716 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
27.11.2013 Bulletin 2013/48

(51) Int Cl.:
G06F 21/57 (2013.01)

(21) Application number: **00903844.9**

(86) International application number:
PCT/GB2000/000528

(22) Date of filing: **15.02.2000**

(87) International publication number:
WO 2000/048063 (17.08.2000 Gazette 2000/33)

(54) **TRUSTED COMPUTING PLATFORM**

GESICHERTE COMPUTERPLATTFORM

PLATE-FORME INFORMATIQUE SECURISEE

(84) Designated Contracting States:
DE FR GB

(30) Priority: **15.02.1999 EP 99301100**
05.03.1999 GB 9905056

(43) Date of publication of application:
12.12.2001 Bulletin 2001/50

(73) Proprietor: **Hewlett-Packard Development
Company, L.P.**
Houston, TX 77070 (US)

(72) Inventors:
• **PROUDLER, Graeme, John**
Stoke Gifford,
Bristol BS34 8XQ (GB)
• **GUPTA, Dipankar**
Mountain View, CA 94040 (US)
• **CHEN, Liqun**
Bradley Stoke
Bristol BS32 9DQ (GB)

- **PEARSON, Siani, Lynne**
Westbury on Trym
Bristol BS9 3PZ (GB)
- **BALACHEFF, Boris**
St Michael's Hill
Bristol BS2 8DG (GB)
- **VAN WILDER, Bruno, Edgard**
B-9300 Aalst (BE)
- **CHAN, David**
Monte Sereno, CA 95030 (US)

(74) Representative: **Lawman, Matthew John Mitchell**
et al
EIP
Fairfax House
15 Fulwood Place
London, WC1V 6HU (GB)

(56) References cited:
EP-A- 0 510 244 EP-A- 0 849 657
WO-A-95/24696 WO-A-98/15082
US-A- 5 680 547

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 161 716 B1

Description

Technical Field

[0001] The present invention generally relates to trusted devices, trusted computing platforms, trusted transactions and methods of operating the same.

Background Art

[0002] For commercial applications, a client computing platform typically operates in an environment where its behaviour is vulnerable to modification by local or remote entities. This potential insecurity of the platform is a limitation on its use by local parties who might otherwise be willing to use the platform, or remote parties who might otherwise communicate with the platform; for example, for the purposes of E-commerce. For the present purposes, both local parties and remote parties will be referred to as "users" unless otherwise stated.

[0003] Existing security applications, for example virus detection software, execute on computing platforms under the assumption that the platform will operate as intended and that the platform will not subvert processes and applications. This is a valid assumption provided that the intended software state has not become unstable or has not been damaged by other software such as viruses. Users, therefore, typically restrict the use of such platforms to non-critical applications, and weigh the convenience of using the platforms against the risk to sensitive or business critical data.

[0004] EP 0849657 A describes computing apparatus adapted to be secure. This computing apparatus contains a security ASIC which holds cryptographic keys for components of the computing apparatus (including both the BIOS and plug-in components). When booting, the security ASIC determines whether each such component has a valid key before the relevant stage of the boot completes.

[0005] Increasing the level of trust in platforms therefore enables greater user confidence in existing security applications (such as the 'Secure Sockets Layer' or 'IPSec') or remote management applications. This enables greater reliance on those applications and hence reduced 'cost of ownership'. Greater trust also enables new electronic methods of business, since there is greater confidence in the correct operation of both local and remote computing platforms.

[0006] In this document, the word 'trust' is used in the sense that something can be 'trusted' if it always behaves in the expected manner for the intended purpose.

Disclosure of the Invention

[0007] The present inventors have appreciated that it is desirable to use a physical device in a computing platform to verify and possibly enforce trust in that platform. Typically, the device provides trusted measurement and

reporting of attributes of the associated platform, which indicate the integrity of the platform. Also, most preferably, the device is tamper-resistant.

[0008] In accordance with a first aspect, the present invention provides computing apparatus comprising main processing means and main memory means, each being mounted on an assembly and connected for communication with one or more other components on the assembly, wherein: the computing apparatus further comprises a trusted device mounted on the assembly and being connected for communications with one or more other components on the assembly, the trusted device comprising device memory means and device processing means; the device processing means is programmed to acquire a value of an integrity metric that provides an indication of whether the computing apparatus will operate as intended; and the device memory means stores the private key of a public/private key pair and the device processing means is operable to respond to an integrity challenge from a local or remote user of the computer apparatus by using the private key in a cryptographic process to authenticate the trusted device to the local or remote user and to sign the acquired value of the integrity metric, the trusted device being operable to output the signed integrity metric for reporting to the local or remote user in response to the challenge.

[0009] As used herein for reasons of simplicity of description, the term "device" also encompasses plural devices having equivalent function, or equivalent functionality integrated into one or more existing platform devices or assemblies. Additionally, the term 'true' as used herein implies that the value is that which correctly reflects the state of the computing apparatus. This may be ensured if the measurement method is substantially un-modifiable other than by the trusted device.

[0010] In accordance with a second aspect, the present invention provides a method of operating a system comprising trusted computing apparatus and a local or remote user, the trusted computing apparatus incorporating a trusted device comprising device memory means and device processing means, wherein the device memory means stores the private key of a public/private key pair and the device processing means is arranged to acquire a value of an integrity metric of the trusted computing apparatus, wherein the integrity metric provides an indication of whether trusted computing apparatus will operate as intended, the method comprising the steps of: the trusted device acquiring the value of the integrity metric of the trusted computing apparatus; the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus; the trusted computing apparatus receiving the challenge, and in response the device processing means of the trusted device using the private key stored in the device memory means in a cryptographic process to authenticate the trusted device to the user and to sign the acquired value of the integrity metric, the trusted device outputting the

signed integrity metric for reporting to the user in a response to the challenge; and the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party.

[0011] In accordance with a third aspect, the present invention provides a method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus, the method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus using the above method, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

[0012] In accordance with a fourth embodiment, the present invention provides a method of verifying that trusted computing apparatus is trustworthy for use by a user for processing a particular application, the method including the step of the user verifying the integrity of the trusted computing apparatus using the above method, and the user using the trusted computing apparatus to process the particular application in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

[0013] Other aspects and embodiments of the present invention will become apparent from the following description and claims.

Brief Description of the Drawings

[0014] A preferred embodiment of the present invention will now be described by way of example only with reference to the accompanying drawings in which:

Figure 1 is a diagram that illustrates a system capable of implementing embodiments of the present invention;

Figure 2 is a diagram which illustrates a motherboard including a trusted device arranged to communicate with a smart card via a smart card reader and with a group of modules;

Figure 3 is a diagram that illustrates the trusted device in more detail;

Figure 4 is a flow diagram which illustrates the steps involved in acquiring an integrity metric of the computing apparatus;

Figure 5 is a flow diagram which illustrates the steps involved in establishing communications between a trusted computing platform and a remote platform including the trusted platform verifying its integrity; and

Figure 6 is a flow diagram which illustrates the steps involved in verification of a trusted computing platform by a potential user of that platform by means of a smart card.

Best Mode For Carrying Out the Invention. & Industrial Applicability

[0015] The present exemplary embodiment generally provides the incorporation into a computing platform of a physical trusted device whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform. The identity and the integrity metric are compared with expected values provided by a trusted party (TP) that is prepared to vouch for the trustworthiness of the platform. If there is a match, the implication is that at least part of the platform is operating correctly, depending on the scope of the integrity metric.

[0016] A user verifies the correct operation of the platform before exchanging other data with the platform. A user does this by requesting the trusted device to provide its identity and an integrity metric. (Optionally the trusted device will refuse to provide evidence of identity if it itself was unable to verify correct operation of the platform.) The user receives the proof of identity and the identity metric, and compares them against values which it believes to be true. Those proper values are provided by the TP or another entity that is trusted by the user. If data reported by the trusted device is the same as that provided by the TP, the user trusts the platform. This is because the user trusts the entity. The entity trusts the platform because it has previously validated the identity and determined the proper integrity metric of the platform.

[0017] Once a user has established trusted operation of the platform, he exchanges other data with the platform. For a local user, the exchange might be by interacting with some software application running on the platform. For a remote user, the exchange might involve a secure transaction. In either case, the data exchanged is 'signed' by the trusted device. The user can then have greater confidence that data is being exchanged with a platform whose behaviour can be trusted.

[0018] The trusted device uses cryptographic processes but does not necessarily provide an external interface to those cryptographic processes. Also, a most desirable implementation would be to make the trusted device tamperproof, to protect secrets by making them inaccessible to other platform functions and provide an environment that is substantially immune to unauthorised modification. Since tamper-proofing is impossible, the best approximation is a trusted device that is tamper-resistant, or tamper-detecting. The trusted device, therefore, preferably consists of one physical component that is tamper-resistant.

[0019] Techniques relevant to tamper-resistance are well known to those skilled in the art of security. These techniques include methods for resisting tampering (such as appropriate encapsulation of the trusted device), methods for detecting tampering (such as detection of out of specification voltages, X-rays, or loss of physical integrity in the trusted device casing), and methods for eliminating data when tampering is detected. Further dis-

cussion of appropriate techniques can be found at <http://www.cl.cam.ac.uk/~mgk25/tamper.html>. It will be appreciated that, although tamper-proofing is a most desirable feature of the present invention, it does not enter into the normal operation of the invention and, as such, is beyond the scope of the present invention and will not be described in any detail herein.

[0020] The trusted device is preferably a physical one because it must be difficult to forge. It is most preferably tamper-resistant because it must be hard to counterfeit. It typically has an engine capable of using cryptographic processes because it is required to prove identity, both locally and at a distance, and it contains at least one method of measuring some integrity metric of the platform with which it is associated.

[0021] A trusted platform 10 is illustrated in the diagram in Figure 1. The platform 10 includes the standard features of a keyboard 14, mouse 16 and visual display unit (VDU) 18, which provide the physical 'user interface' of the platform. This embodiment of a trusted platform also contains a smart card reader 12 - a smart card reader is not an essential element of all trusted platforms, but is employed in various preferred embodiments described below. Along side the smart card reader 12, there is illustrated a smart card 19 to allow trusted user interaction with the trusted platform as shall be described further below. In the platform 10, there are a plurality of modules 15: these are other functional elements of the trusted platform of essentially any kind appropriate to that platform (the functional significance of such elements is not relevant to the present invention and will not be discussed further herein).

[0022] As illustrated in Figure 2, the motherboard 20 of the trusted computing platform 10 includes (among other standard components) a main processor 21, main memory 22, a trusted device 24, a data bus 26 and respective control lines 27 and address lines 28, BIOS memory 29 containing the BIOS program for the platform 10 and an Input/Output (IO) device 23, which controls interaction between the components of the motherboard and the smart card reader 12, the keyboard 14, the mouse 16 and the VDU 18. The main memory 22 is typically random access memory (RAM). In operation, the platform 10 loads the operating system, for example Windows NT™, into RAM from hard disk (not shown). Additionally, in operation, the platform 10 loads the processes or applications that may be executed by the platform 10 into RAM from hard disk (not shown).

[0023] Typically, in a personal computer the BIOS program is located in a special reserved memory area, the upper 64K of the first megabyte of the system memory (addresses F000h to FFFFh), and the main processor is arranged to look at this memory location first, in accordance with an industry wide standard.

[0024] The significant difference between the platform and a conventional platform is that, after reset, the main processor is initially controlled by the trusted device, which then hands control over to the platform-specific

BIOS program, which in turn initialises all input/output devices as normal. After the BIOS program has executed, control is handed over as normal by the BIOS program to an operating system program, such as Windows NT (TM), which is typically loaded into main memory 22 from a hard disk drive (not shown).

[0025] Clearly, this change from the normal procedure requires a modification to the implementation of the industry standard, whereby the main processor 21 is directed to address the trusted device 24 to receive its first instructions. This change may be made simply by hard-coding a different address into the main processor 21. Alternatively, the trusted device 24 may be assigned the standard BIOS program address, in which case there is no need to modify the main processor configuration.

[0026] It is highly desirable for the BIOS boot block to be contained within the trusted device 24. This prevents subversion of the obtaining of the integrity metric (which could otherwise occur if rogue software processes are present) and prevents rogue software processes creating a situation in which the BIOS (even if correct) fails to build the proper environment for the operating system.

[0027] Although, in the preferred embodiment to be described, the trusted device 24 is a single, discrete component, it is envisaged that the functions of the trusted device 24 may alternatively be split into multiple devices on the motherboard, or even integrated into one or more of the existing standard devices of the platform. For example, it is feasible to integrate one or more of the functions of the trusted device into the main processor itself, provided that the functions and their communications cannot be subverted. This, however, would probably require separate leads on the processor for sole use by the trusted functions. Additionally or alternatively, although in the present embodiment the trusted device is a hardware device that is adapted for integration into the motherboard 20, it is anticipated that a trusted device may be implemented as a 'removable' device, such as a dongle, which could be attached to a platform when required. Whether the trusted device is integrated or removable is a matter of design choice. However, where the trusted device is separable, a mechanism for providing a logical binding between the trusted device and the platform should be present.

[0028] The trusted device 24 comprises a number of blocks, as illustrated in Figure 3. After system reset, the trusted device 24 performs a secure boot process to ensure that the operating system of the platform 10 (including the system clock and the display on the monitor) is running properly and in a secure manner. During the secure boot process, the trusted device 24 acquires an integrity metric of the computing platform 10. The trusted device 24 can also perform secure data transfer and, for example, authentication between it and a smart card via encryption/decryption and signature/verification. The trusted device 24 can also securely enforce various security control policies, such as locking of the user interface.

[0029] Specifically, the trusted device comprises: a controller 30 programmed to control the overall operation of the trusted device 24, and interact with the other functions on the trusted device 24 and with the other devices on the motherboard 20; a measurement function 31 for acquiring the integrity metric from the platform 10; a cryptographic function 32 for signing, encrypting or decrypting specified data; an authentication function 33 for authenticating a smart card; and interface circuitry 34 having appropriate ports (36, 37 & 38) for connecting the trusted device 24 respectively to the data bus 26, control lines 27 and address lines 28 of the motherboard 20. Each of the blocks in the trusted device 24 has access (typically via the controller 30) to appropriate volatile memory areas 4 and/or non-volatile memory areas 3 of the trusted device 24. Additionally, the trusted device 24 is designed, in a known manner, to be tamper resistant.

[0030] For reasons of performance, the trusted device 24 may be implemented as an application specific integrated circuit (ASIC). However, for flexibility, the trusted device 24 is preferably an appropriately programmed micro-controller. Both ASICs and micro-controllers are well known in the art of microelectronics and will not be considered herein in any further detail.

[0031] One item of data stored in the non-volatile memory 3 of the trusted device 24 is a certificate 350. The certificate 350 contains at least a public key 351 of the trusted device 24 and an authenticated value 352 of the platform integrity metric measured by a trusted party (TP). The certificate 350 is signed by the TP using the TP's private key prior to it being stored in the trusted device 24. In later communications sessions, a user of the platform 10 can verify the integrity of the platform 10 by comparing the acquired integrity metric with the authentic integrity metric 352. If there is a match, the user can be confident that the platform 10 has not been subverted. Knowledge of the TP's generally-available public key enables simple verification of the certificate 350. The non-volatile memory 3 also contains an identity (ID) label 353. The ID label 353 is a conventional ID label, for example a serial number, that is unique within some context. The ID label 353 is generally used for indexing and labelling of data relevant to the trusted device 24, but is insufficient in itself to prove the identity of the platform 10 under trusted conditions.

[0032] The trusted device 24 is equipped with at least one method of reliably measuring or acquiring the integrity metric of the computing platform 10 with which it is associated. In the present embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory. Such an acquired integrity metric, if verified as described above, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level. Other known processes, for example virus checkers, will typically be in place to check that the operating system and application program code has not been subverted.

[0033] The measurement function 31 has access to: non-volatile memory 3 for storing a hash program 354 and a private key 355 of the trusted device 24, and volatile memory 4 for storing acquired integrity metric in the form of a digest 361. In appropriate embodiments, the volatile memory 4 may also be used to store the public keys and associated ID labels 360a-360n of one or more authentic smart cards 19s that can be used to gain access to the platform 10.

[0034] In one preferred implementation, as well as the digest, the integrity metric includes a Boolean value, which is stored in volatile memory 4 by the measurement function 31, for reasons that will become apparent.

[0035] A preferred process for acquiring an integrity metric will now be described with reference to Figure 4.

[0036] In step 500, at switch-on, the measurement function 31 monitors the activity of the main processor 21 on the data, control and address lines (26, 27 & 28) to determine whether the trusted device 24 is the first memory accessed. Under conventional operation, a main processor would first be directed to the BIOS memory first in order to execute the BIOS program. However, in accordance with the present embodiment, the main processor 21 is directed to the trusted device 24, which acts as a memory. In step 505, if the trusted device 24 is the first memory accessed, in step 510, the measurement function 31 writes to volatile memory 4 a Boolean value which indicates that the trusted device 24 was the first memory accessed. Otherwise, in step 515, the measurement function writes a Boolean value which indicates that the trusted device 24 was not the first memory accessed.

[0037] In the event the trusted device 24 is not the first accessed, there is of course a chance that the trusted device 24 will not be accessed at all. This would be the case, for example, if the main processor 21 were manipulated to run the BIOS program first. Under these circumstances, the platform would operate, but would be unable to verify its integrity on demand, since the integrity metric would not be available. Further, if the trusted device 24 were accessed after the BIOS program had been accessed, the Boolean value would clearly indicate lack of integrity of the platform.

[0038] In step 520, when (or if) accessed as a memory by the main processor 21, the main processor 21 reads the stored native hash instructions 354 from the measurement function 31 in step 525. The hash instructions 354 are passed for processing by the main processor 21 over the data bus 26. In step 530, main processor 21 executes the hash instructions 354 and uses them, in step 535, to compute a digest of the BIOS memory 29, by reading the contents of the BIOS memory 29 and processing those contents according to the hash program. In step 540, the main processor 21 writes the computed digest 361 to the appropriate volatile memory location 4 in the trusted device 24. The measurement function 31, in step 545, then calls the BIOS program in the BIOS memory 29, and execution continues in a conven-

tional manner.

[0039] Clearly, there are a number of different ways in which the integrity metric may be calculated, depending upon the scope of the trust required. The measurement of the BIOS program's integrity provides a fundamental check on the integrity of a platform's underlying processing environment. The integrity metric should be of such a form that it will enable reasoning about the validity of the boot process - the value of the integrity metric can be used to verify whether the platform booted using the correct BIOS. Optionally, individual functional blocks within the BIOS could have their own digest values, with an ensemble BIOS digest being a digest of these individual digests. This enables a policy to state which parts of BIOS operation are critical for an intended purpose, and which are irrelevant (in which case the individual digests must be stored in such a manner that validity of operation under the policy can be established).

[0040] Other integrity checks could involve establishing that various other devices, components or apparatus attached to the platform are present and in correct working order. In one example, the BIOS programs associated with a SCSI controller could be verified to ensure communications with peripheral equipment could be trusted. In another example, the integrity of other devices, for example memory devices or co-processors, on the platform could be verified by enacting fixed challenge/response interactions to ensure consistent results. Where the trusted device 24 is a separable component, some such form of interaction is desirable to provide an appropriate logical binding between the trusted device 24 and the platform. Also, although in the present embodiment the trusted device 24 utilises the data bus 26 as its main means of communication with other parts of the platform, it would be feasible, although not so convenient, to provide alternative communications paths, such as hard-wired paths or optical paths. Further, although in the present embodiment the trusted device 24 instructs the main processor 21 to calculate the integrity metric in other embodiments, the trusted device itself is arranged to measure one or more integrity metrics.

[0041] Preferably, the BIOS boot process includes mechanisms to verify the integrity of the boot process itself. Such mechanisms are already known from, for example, Intel's draft "Wired for Management baseline specification v 2.0 - BOOT Integrity Service", and involve calculating digests of software or firmware before loading that software or firmware. Such a computed digest is compared with a value stored in a certificate provided by a trusted entity, whose public key is known to the BIOS. The software/firmware is then loaded only if the computed value matches the expected value from the certificate, and the certificate has been proven valid by use of the trusted entity's public key. Otherwise, an appropriate exception handling routine is invoked.

[0042] Optionally, after receiving the computed BIOS digest, the trusted device 24 may inspect the proper value of the BIOS digest in the certificate and not pass control

to the BIOS if the computed digest does not match the proper value. Additionally, or alternatively, the trusted device 24 may inspect the Boolean value and not pass control back to the BIOS if the trusted device 24 was not the first memory accessed. In either of these cases, an appropriate exception handling routine may be invoked.

[0043] Figure 5 illustrates the flow of actions by a TP, the trusted device 24 incorporated into a platform, and a user (of a remote platform) who wants to verify the integrity of the trusted platform. It will be appreciated that substantially the same steps as are depicted in Figure 5 are involved when the user is a local user. In either case, the user would typically rely on some form of software application to enact the verification. It would be possible to run the software application on the remote platform or the trusted platform. However, there is a chance that, even on the remote platform, the software application could be subverted in some way. Therefore, it is anticipated that, for a high level of integrity, the software application would reside on a smart card of the user, who would insert the smart card into an appropriate reader for the purposes of verification. Figure 5 illustrates the flow of actions for the general case - a more specific flow of actions for verification by a user smart card will be described with reference to Figure 6 further below.

[0044] At the first instance, a TP, which vouches for trusted platforms, will inspect the type of the platform to decide whether to vouch for it or not. This will be a matter of policy. If all is well, in step 600, the TP measures the value of integrity metric of the platform. Then, the TP generates a certificate, in step 605, for the platform. The certificate is generated by the TP by appending the trusted device's public key, and optionally its ID label, to the measured integrity metric, and signing the string with the TP's private key.

[0045] The trusted device 24 can subsequently prove its identity by using its private key to process some input data received from the user and produce output data, such that the input/output pair is statistically impossible to produce without knowledge of the private key. Hence, knowledge of the private key forms the basis of identity in this case. Clearly, it would be feasible to use symmetric encryption to form the basis of identity. However, the disadvantage of using symmetric encryption is that the user would need to share his secret with the trusted device. Further, as a result of the need to share the secret with the user, while symmetric encryption would in principle be sufficient to prove identity to the user, it would insufficient to prove identity to a third party, who could not be entirely sure the verification originated from the trusted device or the user.

[0046] In step 610, the trusted device 24 is initialised by writing the certificate 350 into the appropriate non-volatile memory locations 3 of the trusted device 24. This is done, preferably, by secure communication with the trusted device 24 after it is installed in the motherboard 20. The method of writing the certificate to the trusted device 24 is analogous to the method used to initialise

smart cards by writing private keys thereto. The secure communications is supported by a 'master key', known only to the TP, that is written to the trusted device (or smart card) during manufacture, and used to enable the writing of data to the trusted device 24; writing of data to the trusted device 24 without knowledge of the master key is not possible.

[0047] At some later point during operation of the platform, for example when it is switched on or reset, in step 615, the trusted device 24 acquires and stores the integrity metric 361 of the platform.

[0048] When a user wishes to communicate with the platform, in step 620, he creates a nonce, such as a random number, and, in step 625, challenges the trusted device 24 (the operating system of the platform, or an appropriate software application, is arranged to recognise the challenge and pass it to the trusted device 24, typically via a BIOS-type call, in an appropriate fashion). The nonce is used to protect the user from deception caused by replay of old but genuine signatures (called a 'replay attack') by untrustworthy platforms. The process of providing a nonce and verifying the response is an example of the well-known 'challenge/response' process.

[0049] In step 630, the trusted device 24 receives the challenge and creates an appropriate response. This may be a digest of the measured integrity metric and the nonce, and optionally its ID label. Then, in step 635, the trusted device 24 signs the digest, using its private key, and returns the signed digest, accompanied by the certificate 350, to the user.

[0050] In step 640, the user receives the challenge response and verifies the certificate using the well known public key of the TP. The user then, in step 650, extracts the trusted device's 24 public key from the certificate and uses it to decrypt the signed digest from the challenge response. Then, in step 660, the user verifies the nonce inside the challenge response. Next, in step 670, the user compares the computed integrity metric, which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate. If any of the foregoing verification steps fails, in steps 645, 655, 665 or 675, the whole process ends in step 680 with no further communications taking place.

[0051] Assuming all is well, in steps 685 and 690, the user and the trusted platform use other protocols to set up secure communications for other data, where the data from the platform is preferably signed by the trusted device 24.

[0052] Further refinements of this verification process are possible. It is desirable that the challenger becomes aware, through the challenge, both of the value of the platform integrity metric and also of the method by which it was obtained. Both these pieces of information are desirable to allow the challenger to make a proper decision about the integrity of the platform. The challenger also has many different options available - it may accept that the integrity metric is recognised as valid in the trusted

device 24, or may alternatively only accept that the platform has the relevant level of integrity if the value of the integrity metric is equal to a value held by the challenger (or may hold there to be different levels of trust in these two cases).

[0053] The techniques of signing, using certificates, and challenge/response, and using them to prove identity, are well known to those skilled in the art of security and therefore need not be described in any more detail herein.

[0054] As indicated above, Figure 6 shows the flow of actions in an example of verification of platform integrity by a user interacting with the trusted platform with a smart card 19. As will be described, the process conveniently implements a challenge/response routine. There exist many available challenge/response mechanisms. The implementation of an authentication protocol used in the present embodiment is mutual (or 3-step) authentication, as described in ISO/IEC 9798-3, "Information technology - Security techniques - Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm", International Organization for Standardization, November 1993. Of course, there is no reason why other authentication procedures cannot be used, for example 2-step or 4-step, as also described in this reference.

[0055] Initially, the user inserts their smart card 19 into the smart card reader 12 of the platform in step 700.

[0056] Beforehand, a platform configured for use by users of in this way will typically be operating under the control of its standard operating system and executing the authentication process, which waits for a user to insert their smart card 19. Apart from the smart card reader 12 being active in this way, such a platform is typically rendered inaccessible to users by 'locking' the user interface (i.e. the screen, keyboard and mouse). This will however not be the case in all embodiments of the invention.

[0057] When the smart card 19 is inserted into the smart card reader 12, the trusted device 24 is triggered to attempt mutual authentication in step by generating and transmitting a nonce A to the smart card 19 in step 705. A nonce, such as a random number, is used to protect the originator from deception caused by replay of old but genuine responses (called a 'replay attack') by untrustworthy third parties.

[0058] In response, in step 710, the smart card 19 generates and returns a response comprising the concatenation of: the plain text of the nonce A, a new nonce B generated by the smart card 19, an ID of the trusted device 24 and some redundancy; the signature of the plain text, generated by signing the plain text with the private key of the smart card 19; and a certificate containing the ID and the public key of the smart card 19.

[0059] The trusted device 24 authenticates the response by using the public key in the certificate to verify the signature of the plain text in step 715. If the response is not authentic, the process ends in step 720. If the response is authentic, in step 725 the trusted device 24

generates and sends a further response including the concatenation of: the plain text of the nonce A, the nonce B, an ID of the smart card 19 and the acquired integrity metric; the signature of the plain text, generated by signing the plain text using the private key of the trusted device 24; and the certificate comprising the public key of the trusted device 24 and the authentic integrity metric, both signed by the private key of the TP.

[0060] The smart card 19 authenticates this response by using the public key of the TP and comparing the acquired integrity metric with the authentic integrity metric, where a match indicates successful verification, in step 730. If the further response is not authentic, the process ends in step 735.

[0061] If the procedure is successful, both the trusted device 24 has authenticated the logon card 19 and the smart card 19 has verified the integrity of the trusted platform and, in step 740, the authentication process executes the secure process for the user.

[0062] In certain types of interaction, the authentication process can end at this point. However, if a session is to be continued between the user and the trusted platform, it is desirable to ensure that the user remains authenticated to the platform.

[0063] Where continued authentication is required, the authentication process sets an interval timer in step 745. Thereafter, using appropriate operating system interrupt routines, the authentication process services the interval timer periodically to detect when the timer meets or exceeds a pre-determined timeout period in step 750.

[0064] Clearly, the authentication process and the interval timer run in parallel with the secure process. When the timeout period is met or exceeded, the authentication process triggers the trusted device 24 to re-authenticate the smart card 19, by transmitting a challenge for the smart card 19 to identify itself in step 760. The smart card 19 returns a certificate including its ID and its public key in step 765. In step 770, if there is no response (for example, as a result of the smart card 19 having been removed) or the certificate is no longer valid for some reason (for example, the smart card has been replaced with a different smart card), the session is terminated by the trusted device 24 in step 775. Otherwise, in step 770, the process from step 745 repeats by resetting the interval timer.

[0065] Additionally, or alternatively, in some embodiments it may be required that the user profile is encrypted and signed to protect privacy and integrity. If so, a secure data transfer protocol may be needed between the trusted device 24 and the smart card 19. There exist many available mechanisms for transferring secure credentials between two entities. A possible implementation, which may be used in the present embodiment, is secure key transport mechanisms from ISO/IEC DIS 11770-3, "Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques", International Organization for Standardization, March 1997.

[0066] Modifications of this verification process using other well-known challenge and response techniques can easily be achieved by the skilled person. Similarly, alternative verification processes can be used by parties interacting with the platform in a different manner (that is, other than as a user equipped with a smart card).

Claims

1. Computing apparatus comprising main processing means (21) and main memory means (22), each being mounted on an assembly (20) and connected for communication with one or more other components on the assembly (20), wherein:

the computing apparatus further comprises a trusted device (24) mounted on the assembly (20) and being connected for communications with one or more other components on the assembly (20), the trusted device (24) comprising device memory means (3, 4) and device processing means (30, 31, 32, 33); the device processing means (30, 31, 32, 33) is programmed to acquire a value of an integrity metric that provides an indication of whether the computing apparatus (10) will operate as intended; and

the device memory means (3, 4) stores the private key (355) of a public/private key pair and the device processing means (30, 31, 32, 33) is operable to respond to an integrity challenge from a local or remote user of the computer apparatus (10) by using the private key (355) in a cryptographic process to authenticate the trusted device (24) to the local or remote user and to sign the acquired value of the integrity metric, the trusted device (24) being operable to output the signed integrity metric for reporting to the local or remote user in response to the challenge.

2. Computing apparatus according to claim 1, wherein the device processing means (30, 31, 32, 33) is programmed to instruct the main processing means (21) to determine the integrity metric and return the integrity metric for storage in the device memory means (3, 4).
3. Computing apparatus according to claim 2, wherein the device processing means (30, 31, 32, 33) is programmed to instruct the main processing means (21) by transferring to the main processing means (21) program code native to the main processing means (21) that is stored in the device memory means (3, 4).
4. Computing apparatus according to claim 3, wherein the computing apparatus is arranged to cause the

instructions to be the first instructions executed after release from reset.

5. Computing apparatus according to claim 3 or claim 4, wherein the trusted device (24) is arranged to transfer the instructions to the main processing means (21) in response to memory read signals from the main processing means (21).
6. Computing apparatus according to any one of claims 1 to 5, wherein the trusted device (24) is arranged to monitor the data bus means (26) by which components mounted on the assembly (20) are adapted to communicate and store in the device memory means (3, 4) a flag in the event the first memory read signals generated by the main processing means (21) after the computing apparatus (10) is released from reset are addressed to the trusted device (24).
7. Computing apparatus according to any one of claims 1 to 6, wherein the trusted device (24) has stored in device memory means (3, 4) at least one of:
 - a unique identity of the trusted device (24); and
 - an authenticated integrity metric generated by a trusted party.
8. Computing apparatus according to claim 1, wherein the device processing means (30, 31, 32, 33) is programmed to determine the correctness of the acquired value of the integrity metric by comparing the acquired value with an authenticated integrity metric generated by a trusted party and stored in the device memory means (3, 4).
9. Computing apparatus according to claim 1, wherein the trusted device (24) also has stored in its device memory means (3, 4) the public key of said public/private key pair that has been signed by a trusted party, and wherein the device processing means (30, 31, 32, 33) is further operable to respond to an integrity challenge from a local or remote user by returning the signed public key to the local or remote user.
10. Computing apparatus according to claim 1, wherein the trusted device (24) also has stored in its device memory means (3, 4) an authenticated integrity metric generated by a trusted party and wherein the device processing means (30, 31, 32, 33) is further operable to respond to an integrity challenge from a local or remote user by returning the authenticated integrity metric to the local or remote user.
11. Computing apparatus as claimed in any preceding claim, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus (10).

12. Computing apparatus as claimed in any preceding claim, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus (10).

13. Computing apparatus as claimed in any preceding claim, wherein the trusted device (24) is adapted to acquire a plurality of integrity metrics.

14. Computing apparatus as claimed in any preceding claim, wherein the trusted device (24) is adapted to be tamper resistant.

15. A trusted device configured for use in computing apparatus according to any one of the preceding claims.

16. A method of operating a system comprising trusted computing apparatus (10) and a local or remote user, the trusted computing apparatus (10) incorporating a trusted device (24) comprising device memory means (3, 4) and device processing means (30, 31, 32, 33), wherein the device memory means (3, 4) stores the private key (355) of a public/private key pair and the device processing means (30, 31, 32, 33) is arranged to acquire a value of an integrity metric of the trusted computing apparatus (10), wherein the integrity metric provides an indication of whether trusted computing apparatus (10) will operate as intended, the method comprising the steps of:

the trusted device acquiring the value of the integrity metric of the trusted computing apparatus (10);

the user generating a challenge for the trusted computing apparatus (10) to prove its integrity and submitting the challenge to the trusted computing apparatus (10);

the trusted computing apparatus (10) receiving the challenge, and in response the device processing means of the trusted device (24) using the private key (355) stored in the device memory means in a cryptographic process to authenticate the trusted device (24) to the user and to sign the acquired value of the integrity metric, the trusted device (24) outputting the signed integrity metric for reporting to the user in a response to the challenge; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus (10) that had been generated by a trusted party.

17. A method according to claim 16, wherein the challenge includes a nonce, the response includes the integrity metric and the nonce, both digitally signed by the trusted device using the private key, and the

user verifies the integrity metric and the nonce using the public key of said public/private key pair.

18. A method according to claim 17, wherein the response includes a certificate (350) held by the trusted device (24) in its device memory means (3, 4), which certificate has been digitally signed by a trusted party using a private encryption key of the trusted party, the certificate including the public key of the public/private key pair, and the user verifies the certificate using the public encryption key of the trusted party and uses the public key from the certificate to verify the integrity metric and the nonce.
19. A method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus (10), the method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus (10) using the method according to any one of claims 16 to 18, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus (10) is successfully verified by the remote computing apparatus.
20. A method of verifying that trusted computing apparatus (10) is trustworthy for use by a user for processing a particular application, the method including the step of the user verifying the integrity of the trusted computing apparatus (10) using the method according to any one of claims 16 to 18, and the user using the trusted computing apparatus (10) to process the particular application in the event the integrity of the trusted computing apparatus (10) is successfully verified by the remote computing apparatus.
21. A trusted device arranged for use in accordance with any one of claims 16 to 20.

Patentansprüche

1. Computervorrichtung, umfassend Hauptverarbeitungsmittel (21) und Hauptspeichermittel (22), welche jeweils auf einer Anordnung (20) montiert sind und für Kommunikation mit einer oder mehreren Komponenten auf der Anordnung (20) verbunden sind, wobei:

die Computervorrichtung ferner ein gesichertes Gerät (24) umfasst, das auf der Anordnung (20) montiert und für Kommunikationen mit einer oder mehreren anderen Komponenten auf der Anordnung (20) verbunden ist, wobei das gesicherte Gerät (24) Gerätespeichermittel (3, 4) und Geräteverarbeitungsmittel (30, 31, 32, 33) umfasst;

die Geräteverarbeitungsmittel (30, 31, 32, 33) so programmiert sind, dass sie einen Wert einer Integritätsmetrik erfassen und anzeigen, ob die Computervorrichtung (10) wie beabsichtigt funktioniert; und

das Gerätespeichermittel (3, 4) den privaten Schlüssel (355) eines öffentlichen/privaten Schlüsselpaars speichert, und das Geräteverarbeitungsmittel (30, 31, 32, 33) so betrieben werden kann, dass es auf eine Integritätsabfrage von einem lokalen oder entfernten Benutzer der Computervorrichtung (10) durch Verwenden des privaten Schlüssel (355) in einem kryptographischen Prozess abantwortet, um das gesicherte Gerät (24) für den lokalen oder entfernten Benutzer zu authentifizieren und den erfassten Wert der Integritätsmetrik zu signieren, wobei das gesicherte Gerät (24) so betrieben werden kann, dass es die signierte Integritätsmetrik zur Meldung an den lokalen oder entfernten Benutzer als Antwort auf die Abfrage ausgibt.

2. Computervorrichtung nach Anspruch 1, wobei das Geräteverarbeitungsmittel (30, 31, 32, 33) so programmiert ist, dass es die Hauptverarbeitungsmittel (21) anweist, die Integritätsmetrik zu bestimmen und die Integritätsmetrik zur Speicherung in den Gerätespeichermitteln (3, 4) zurückzusenden.

3. Computervorrichtung nach Anspruch 2, wobei das Geräteverarbeitungsmittel (30, 31, 32, 33) so programmiert ist, dass es die Hauptverarbeitungsmittel (21) durch Übermitteln an die Hauptverarbeitungsmittel (21) von zu den Hauptverarbeitungsmitteln (21) gehörigem Programmcode, der in den Gerätespeichermitteln (3, 4) gespeichert ist, anweist.

4. Computervorrichtung nach Anspruch 3, wobei die Computervorrichtung so ausgeordnet ist, dass sie bewirkt, dass die Anweisungen die ersten Anweisungen sind, die nach der Freigabe von dem Reset ausgeführt werden.

5. Computervorrichtung nach Anspruch 3 oder 4, wobei das gesicherte Gerät (24) so angeordnet ist, dass es die Anweisungen an die Hauptverarbeitungsmittel (21) als Antwort auf Speicherlesesignale von der Hauptverarbeitungsmittel (21) übermittelt.

6. Computervorrichtung nach einem der Ansprüche 1 bis 5, wobei das gesicherte Gerät (24) so angeordnet ist, dass es die Datenbusmittel (26) überwacht, durch welche auf der Anordnung (20) montierte Komponenten kommunizieren können, und ein Flag in den Gerätespeichermitteln (3, 4) speichert, falls die ersten Speicherlesesignale, die durch die Hauptverarbeitungsmittel (21) nach der Freigabe der Computervorrichtung (10) von dem Reset erzeugt wer-

- den, an das gesicherte Gerät (24) adressiert sind.
7. Computervorrichtung nach einem der Ansprüche 1 bis 6, wobei das gesicherte Gerät (24) in den Gerätespeichermitteln (3, 4) mindestens eines der folgenden speichert:
 - eine eindeutigen Kennung des gesicherten Geräts (24); und
 - eine authentifizierte Integritätsmetrik, die durch einen gesicherten Partner erzeugt wurde.
 8. Computervorrichtung nach Anspruch 1, wobei das Geräteverarbeitungsmittel (30, 31, 32, 33) so programmiert ist, dass es die Korrektheit des erfassten Wertes der Integritätsmetrik durch Vergleichen des erfassten Wertes mit einer authentifizierten Integritätsmetrik bestimmt, die durch einen gesicherten Partner erzeugt wurde und in den Gerätespeichermitteln (3, 4) gespeichert ist.
 9. Computervorrichtung nach Anspruch 1, wobei das gesicherte Gerät (24) außerdem den öffentlichen Schlüssel des öffentlichen/privaten Schlüsselpaars, der durch einen gesicherten Partner signiert wurde, in seinen Gerätespeichermitteln (3, 4) gespeichert aufweist, und wobei das Geräteverarbeitungsmittel (30, 31, 32, 33) ferner so betrieben werden kann, dass es auf eine Integritätsabfrage von einem lokalen oder entfernten Benutzer durch Zurücksenden des signierten öffentlichen Schlüssels an den lokalen oder entfernten Benutzer antwortet.
 10. Computervorrichtung nach Anspruch 1, wobei das gesicherte Gerät (24) außerdem eine authentifizierte Integritätsmetrik, die durch einen gesicherten Partner erzeugt wurde, in seinen Gerätespeichermitteln (3, 4) gespeichert aufweist, und wobei das Geräteverarbeitungsmittel (30, 31, 32, 33) ferner so betrieben werden kann, dass es auf eine Integritätsabfrage von einem lokalen oder entfernten Benutzer durch Zurücksenden der authentifizierten Integritätsmetrik an den lokalen oder entfernten Benutzer antwortet.
 11. Computervorrichtung nach einem der vorhergehenden Ansprüche, wobei die Integritätsmetrik ein Digest von allen oder einem Teil der Eingabe-/Ausgabe-Basissoftware für die Computervorrichtung (10) ist.
 12. Computervorrichtung nach einem der vorhergehenden Ansprüche, wobei die Integritätsmetrik ein Digest von allen oder einem Teil der Eingabe-/Ausgabe-Basissoftware für Komponenten oder Vorrichtungen ist, die an die Computervorrichtung (10) angeschlossen sind.
 13. Computervorrichtung nach einem der vorhergehenden Ansprüche, wobei das gesicherte Gerät (24) so angeordnet ist, dass es eine Mehrzahl von Integritätsmetriken erfasst.
 14. Computervorrichtung nach einem der vorhergehenden Ansprüche, wobei das gesicherte Gerät (24) so angeordnet ist, dass es manipulationssicher ist.
 15. Gesichertes Gerät, das zur Verwendung in einer Computervorrichtung nach einem der vorhergehenden Ansprüche konfiguriert ist.
 16. Verfahren zum Betreiben eines Systems, das eine gesicherte Computervorrichtung (10) und einen lokalen oder entfernten Benutzer umfasst, wobei die gesicherte Computervorrichtung (10) ein gesichertes Gerät (24) umfasst, das Gerätespeichermittel (3, 4) und Geräteverarbeitungsmittel (30, 31, 32, 33) umfasst, wobei das Gerätespeichermittel (3, 4) den privaten Schlüssel (355) eines öffentlichen/privaten Schlüsselpaars speichert, und das Geräteverarbeitungsmittel (30, 31, 32, 33) so angeordnet ist, dass es einen Wert einer Integritätsmetrik der gesicherten Computervorrichtung (10) erfasst, wobei die Integritätsmetrik eine Anzeige dessen bereitstellt, ob die gesicherte Computervorrichtung (10) wie beabsichtigt funktioniert, wobei das Verfahren die Schritte umfasst, dass:
 - das gesicherte Gerät den Wert der Integritätsmetrik der gesicherten Computervorrichtung (10) erfasst;
 - der Benutzer eine Abfrage für die gesicherte Computervorrichtung (10) erstellt, um ihre Integrität zu prüfen, und die Abfrage an die gesicherte Computervorrichtung (10) sendet;
 - die gesicherte Computervorrichtung (10) die Abfrage empfängt, und die Geräteverarbeitungsmittel des gesicherten Geräts (24) als Antwort den privaten Schlüssel (355), der in den Gerätespeichermitteln gespeichert ist, in einem kryptographischen Prozess verwenden, um das gesicherte Gerät (24) für den Benutzer zu authentifizieren und den erfassten Wert der Integritätsmetrik zu signieren, wobei das gesicherte Gerät (24) die signierte Integritätsmetrik zur Meldung an den Benutzer in einer Antwort auf die Abfrage ausgibt; und
 - der Benutzer die Antwort empfängt, die Integritätsmetrik aus der Antwort extrahiert und die Integritätsmetrik mit einer authentifizierten Metrik für die gesicherte Computervorrichtung (10) vergleicht, die durch einen gesicherten Partner erzeugt wurde.
 17. Verfahren nach Anspruch 16, wobei die Abfrage einen Zeitstempel umfasst, die Antwort die Integritäts-

metrik und den Zeitstempel umfasst, die beide durch das gesicherte Gerät unter Verwendung des privaten Schlüssels digital signiert sind, und der Benutzer die Integritätsmetrik und den Zeitstempel unter Verwendung des öffentlichen Schlüssels des öffentlichen/privaten Schlüsselpaars verifiziert.

18. Verfahren nach Anspruch 17, wobei die Antwort ein Zertifikat (350) umfasst, das durch das gesicherte Gerät (24) in seinen Gerätespeichermitteln (3, 4) gespeichert wird, wobei das Zertifikat durch einen gesicherten Partner unter Verwendung eines privaten Verschlüsselungsschlüssels des gesicherten Partners digital signiert wurde, das Zertifikat den öffentlichen Schlüssel des öffentlichen/privaten Schlüsselpaars umfasst, und der Benutzer das Zertifikat unter Verwendung des öffentlichen Verschlüsselungsschlüssels verifiziert und den öffentlichen Schlüssel aus dem Zertifikat zum Verifizieren der Integritätsmetrik und des Zeitstempels verwendet.
19. Verfahren zur Herstellung eines Kommunikationskanals in einem System zwischen einer gesicherten Computervorrichtung und einer entfernten Computervorrichtung (10), wobei das Verfahren den Schritt umfasst, dass die entfernte Computervorrichtung die Integrität der gesicherten Computervorrichtung (10) unter Verwendung des Verfahrens nach einem der Ansprüche 16 bis 18 verifiziert und den Kommunikationskanal für weitere Transaktionen aufrechterhält, falls die Integrität der gesicherten Vorrichtung (10) durch die entfernte Computervorrichtung erfolgreich verifiziert wird.
20. Verfahren zum Verifizieren, dass eine gesicherte Computervorrichtung zur Verwendung durch einen Benutzer zum Verarbeiten einer bestimmten Anwendung gesichert ist, wobei das Verfahren den Schritt umfasst, dass der Benutzer die Integrität der gesicherten Computervorrichtung (10) unter Verwendung des Verfahrens nach einem der Ansprüche 16 bis 18 verifiziert, und der Benutzer die gesicherte Computervorrichtung (10) verwendet, um die bestimmte Anwendung auszuführen, falls die Integrität der gesicherten Vorrichtung (10) durch die entfernte Computervorrichtung erfolgreich verifiziert wird.
21. Gesichertes Gerät, das zur Verwendung nach einem der Ansprüche 16 bis 20 angeordnet ist.

Revendications

1. Appareil informatique comprenant des moyens principaux de traitement (21) et des moyens principaux de mémoire (22), chacun étant montés sur un ensemble (20) et connectés pour une communication avec un ou plusieurs autres composants sur l'en-

semble (20), dans lequel :

l'appareil informatique comprend en outre un dispositif de confiance (24) monté sur l'ensemble (20) et qui est connecté pour des communications avec un ou plusieurs autres composants sur l'ensemble (20), le dispositif de confiance (24) comprenant des moyens de mémoire de dispositif (3, 4) et des moyens de traitement de dispositif (30, 31, 32, 33) ; les moyens de traitement de dispositif (30, 31, 32, 33) sont programmés pour acquérir une valeur d'une métrique d'intégrité qui fournit une indication quant à savoir si l'appareil informatique (10) fonctionnera comme prévu ; et les moyens de mémoire de dispositif (3, 4) stockent la clé privée (355) d'une paire de clés publique/privée et les moyens de traitement de dispositif (30, 31, 32, 33) sont actionnables pour répondre à un défi d'intégrité émanant d'un utilisateur local ou à distance de l'appareil informatique (10) par utilisation de la clé privée (355) dans un traitement cryptographique pour authentifier le dispositif de confiance (24) à l'utilisateur local ou à distance et pour signer la valeur acquise de la métrique d'intégrité, le dispositif de confiance (24) étant actionnable pour délivrer en sortie la métrique d'intégrité signée pour un rapport à l'utilisateur local ou à distance en réponse au défi.

2. Appareil informatique selon la revendication 1, dans lequel les moyens de traitement de dispositif (30, 31, 32, 33) sont programmés pour donner instruction aux moyens principaux de traitement (21) de déterminer la métrique d'intégrité et de renvoyer la métrique d'intégrité pour stockage dans les moyens de mémoire de dispositif (3, 4).
3. Appareil informatique selon la revendication 2, dans lequel les moyens de traitement de dispositif (30, 31, 32, 33) sont programmés pour donner instruction aux moyens principaux de traitement (21) par transfert aux moyens principaux de traitement (21) d'un code de programme natif des moyens principaux de traitement (21) qui est stocké dans les moyens de mémoire de dispositif (3, 4).
4. Appareil informatique selon la revendication 3, dans lequel l'appareil informatique est agencé pour amener les instructions à être les premières instructions exécutées après la remise à l'état initial.
5. Appareil informatique selon l'une des revendications 3 ou 4, dans lequel le dispositif de confiance (24) est agencé pour transférer les instructions aux moyens principaux de traitement (21) en réponse à des signaux de lecture de mémoire provenant des moyens

principaux de traitement (21).

6. Appareil informatique selon l'une quelconque des revendications 1 à 5, dans lequel le dispositif de confiance (24) est agencé pour surveiller les moyens de bus de données (26) par lesquels des composants montés sur l'ensemble (20) sont aptes à communiquer et stocker dans les moyens de mémoire de dispositif (3, 4) un drapeau dans le cas où les premiers signaux de lecture de mémoire générés par les moyens principaux de traitement (21) après que l'appareil informatique (10) est remis à l'état initial sont adressés au dispositif de confiance (24).

7. Appareil informatique selon l'une quelconque des revendications 1 à 6, dans lequel le dispositif de confiance (24) a stocké dans des moyens de mémoire de dispositif (3, 4) au moins l'une parmi :

une identité unique du dispositif de confiance (24) ; et
une métrique d'intégrité authentifiée générée par une partie de confiance.

8. Appareil informatique selon la revendication 1, dans lequel les moyens de traitement de dispositif (30, 31, 32, 33) sont programmés pour déterminer l'exactitude de la valeur acquise de la métrique d'intégrité par comparaison de la valeur acquise à une métrique d'intégrité authentifiée générée par une partie de confiance et stockée dans les moyens de mémoire de dispositif (3, 4).

9. Appareil informatique selon la revendication 1, dans lequel le dispositif de confiance (24) a également stocké dans ses moyens de mémoire de dispositif (3, 4) la clé publique de ladite paire de clés publique/privée qui a été signée par une partie de confiance, et dans lequel les moyens de traitement de dispositif (30, 31, 32, 33) sont en outre actionnables pour répondre à un défi d'intégrité émanant d'un utilisateur local ou à distance par renvoi de la clé publique signée à l'utilisateur local ou à distance.

10. Appareil informatique selon la revendication 1, dans lequel le dispositif de confiance (24) a également stocké dans ses moyens de mémoire de dispositif (3, 4) une métrique d'intégrité authentifiée générée par une partie de confiance et dans lequel les moyens de traitement de dispositif (30, 31, 32, 33) sont en outre actionnables pour répondre à un défi d'intégrité émanant d'un utilisateur local ou à distance par renvoi de la métrique d'intégrité authentifiée à l'utilisateur local ou à distance.

11. Appareil informatique selon l'une quelconque des revendications précédentes, dans lequel la métrique d'intégrité est un condensé de l'ensemble ou d'une

partie du logiciel d'entrée/sortie de base pour l'appareil informatique (10).

12. Appareil informatique selon l'une quelconque des revendications précédentes, dans lequel la métrique d'intégrité est un condensé de l'ensemble ou d'une partie du logiciel d'entrée/sortie de base pour des composants ou un appareil fixé(s) à l'appareil informatique (10).

13. Appareil informatique selon l'une quelconque des revendications précédentes, dans lequel le dispositif de confiance (24) est conçu pour acquérir une pluralité de métriques d'intégrité.

14. Appareil informatique selon l'une quelconque des revendications précédentes, dans lequel le dispositif de confiance (24) est conçu pour être inviolable.

15. Dispositif de confiance configuré pour être utilisé dans un appareil informatique selon l'une quelconque des revendications précédentes.

16. Procédé de fonctionnement d'un système comprenant un appareil informatique de confiance (10) et un utilisateur local ou à distance, l'appareil informatique de confiance (10) comprenant un dispositif de confiance (24) comprenant des moyens de mémoire de dispositif (3, 4) et des moyens de traitement de dispositif (30, 31, 32, 33), les moyens de mémoire de dispositif (3, 4) stockant la clé privée (355) d'une paire de clés publique/privée et les moyens de traitement de dispositif (30, 31, 32, 33) étant agencés pour acquérir une valeur d'une métrique d'intégrité de l'appareil informatique de confiance (10), la métrique d'intégrité fournissant une indication quant à savoir si l'appareil informatique de confiance (10) fonctionnera comme prévu, le procédé comprenant les étapes suivantes :

le dispositif de confiance acquiert la valeur de la métrique d'intégrité de l'appareil informatique de confiance (10) ;

l'utilisateur génère un défi pour l'appareil informatique de confiance (10) pour prouver son intégrité et soumet le défi à l'appareil informatique de confiance (10) ;

l'appareil informatique de confiance (10) reçoit le défi et, en réponse, les moyens de traitement de dispositif du dispositif de confiance (24) utilisent la clé privée (355) stockée dans les moyens de mémoire de dispositif dans un traitement cryptographique pour authentifier le dispositif de confiance (24) à l'utilisateur et pour signer la valeur acquise de la métrique d'intégrité, le dispositif de confiance (24) délivre en sortie la métrique d'intégrité signée pour un rapport à l'utilisateur dans une réponse au défi ; et

l'utilisateur reçoit la réponse, extrait la métrique d'intégrité à partir de la réponse et compare la métrique d'intégrité à une métrique authentifiée pour l'appareil informatique de confiance (10) qui a été générée par une partie de confiance. 5

17. Procédé selon la revendication 16, dans lequel le défi comprend un nombre aléatoire, la réponse comprend la métrique d'intégrité et le nombre aléatoire, les deux étant signés numériquement par le dispositif de confiance à l'aide de la clé privée, et l'utilisateur vérifie la métrique d'intégrité et le nombre aléatoire à l'aide de la clé publique de ladite paire de clés publique/privée. 10

15

18. Procédé selon la revendication 17, dans lequel la réponse comprend un certificat (350) conservé par le dispositif de confiance (24) dans ses moyens de mémoire de dispositif (3, 4), lequel certificat a été signé numériquement par une partie de confiance à l'aide d'une clé de chiffrement privée de la partie de confiance, le certificat comprenant la clé publique de la paire de clés publique/privée, et l'utilisateur vérifie le certificat à l'aide de la clé de chiffrement publique de la partie de confiance et utilise la clé publique provenant du certificat pour vérifier la métrique d'intégrité et le nombre aléatoire. 20

25

19. Procédé d'établissement d'un canal de communication dans un système entre un appareil informatique de confiance et un appareil informatique à distance (10), le procédé comprenant l'étape suivant laquelle l'appareil informatique à distance vérifie l'intégrité de l'appareil informatique de confiance (10) à l'aide du procédé selon l'une quelconque des revendications 16 à 18, et maintient le canal de communication pour d'autres transactions dans le cas où l'intégrité de l'appareil informatique de confiance (10) est vérifiée avec succès par l'appareil informatique à distance. 30

35

40

20. Procédé de vérification du fait qu'un appareil informatique de confiance (10) est fiable pour une utilisation par un utilisateur pour traiter une application particulière, le procédé comprenant l'étape suivant laquelle l'utilisateur vérifie l'intégrité de l'appareil informatique de confiance (10) à l'aide du procédé selon l'une quelconque des revendications 16 à 18, et l'utilisateur utilise l'appareil informatique de confiance (10) pour traiter l'application particulière dans le cas où l'intégrité de l'appareil informatique de confiance (10) est vérifiée avec succès par l'appareil informatique à distance. 45

50

21. Dispositif de confiance agencé pour être utilisé conformément à l'une quelconque des revendications 16 à 20. 55

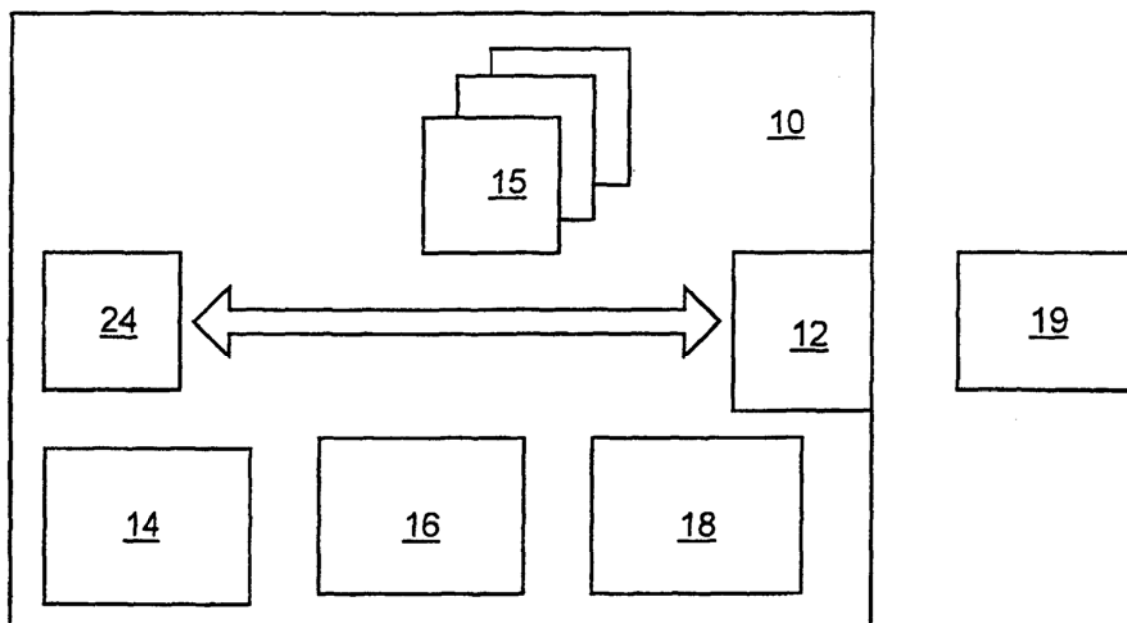


FIGURE 1

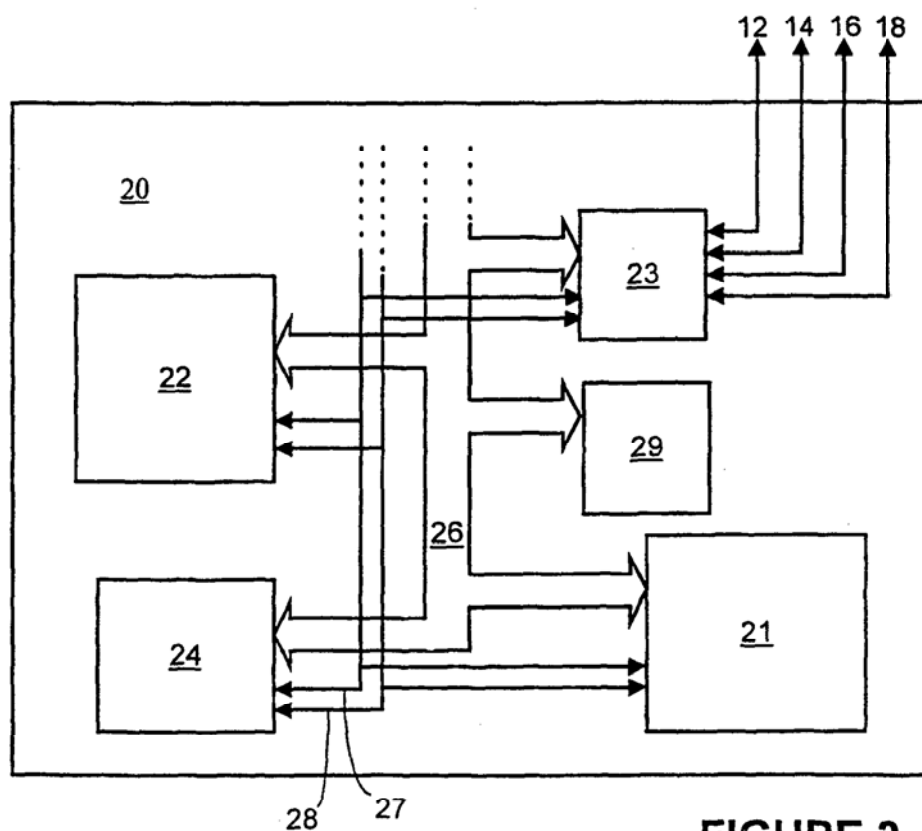
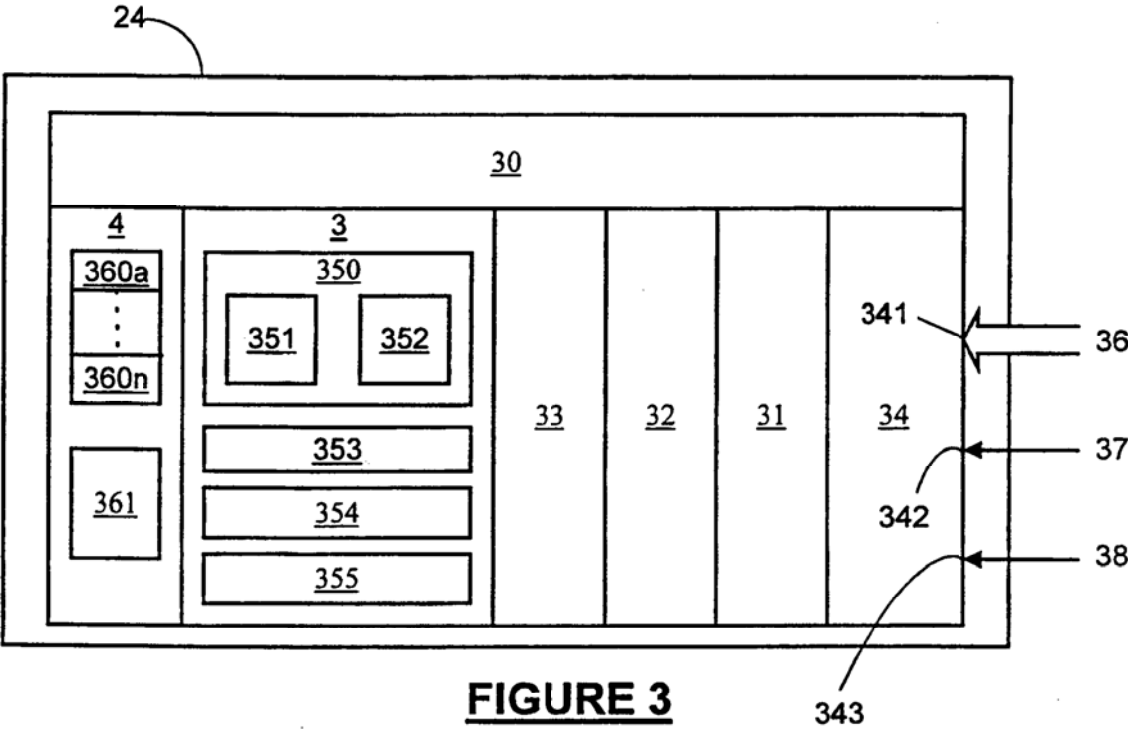
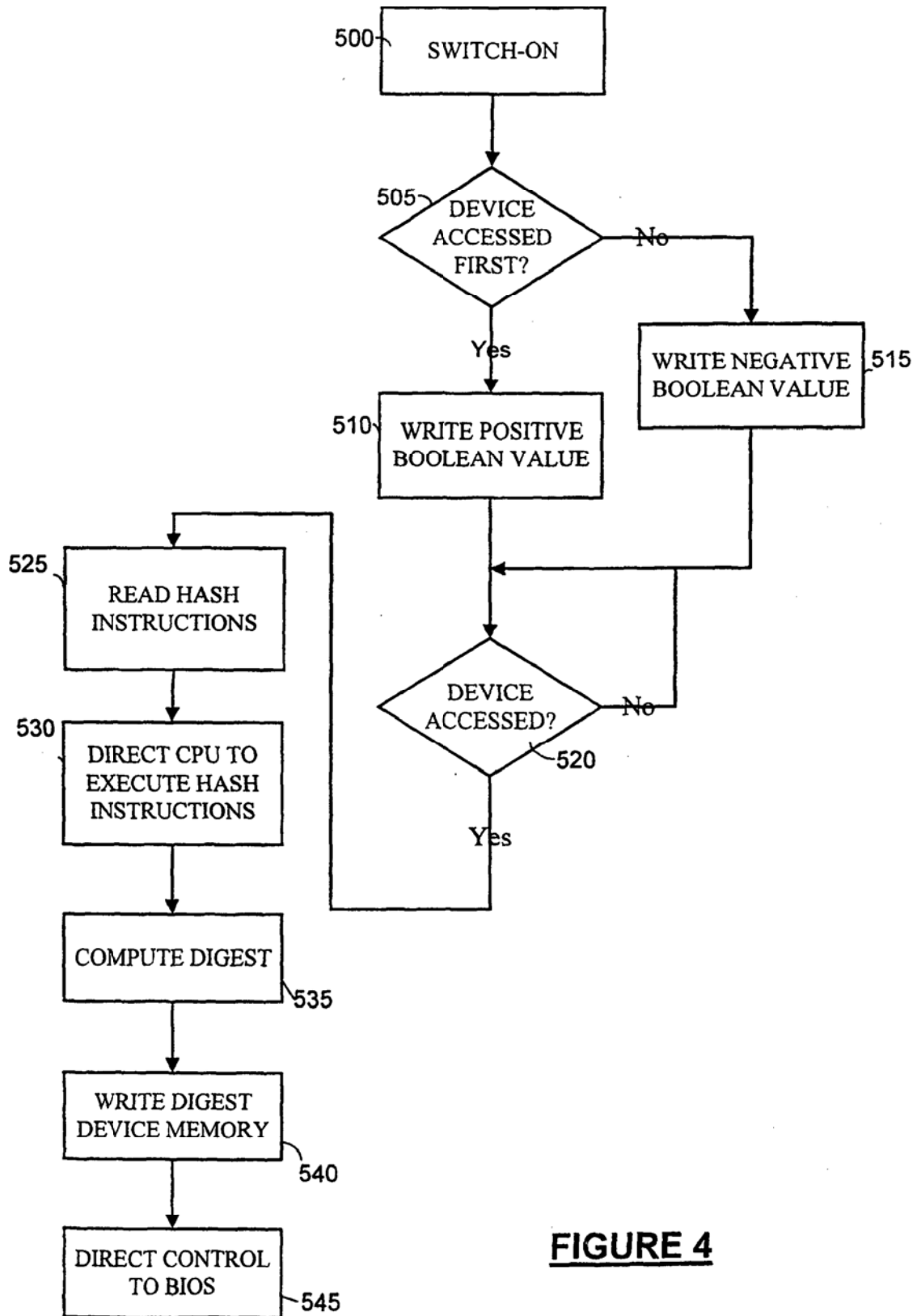
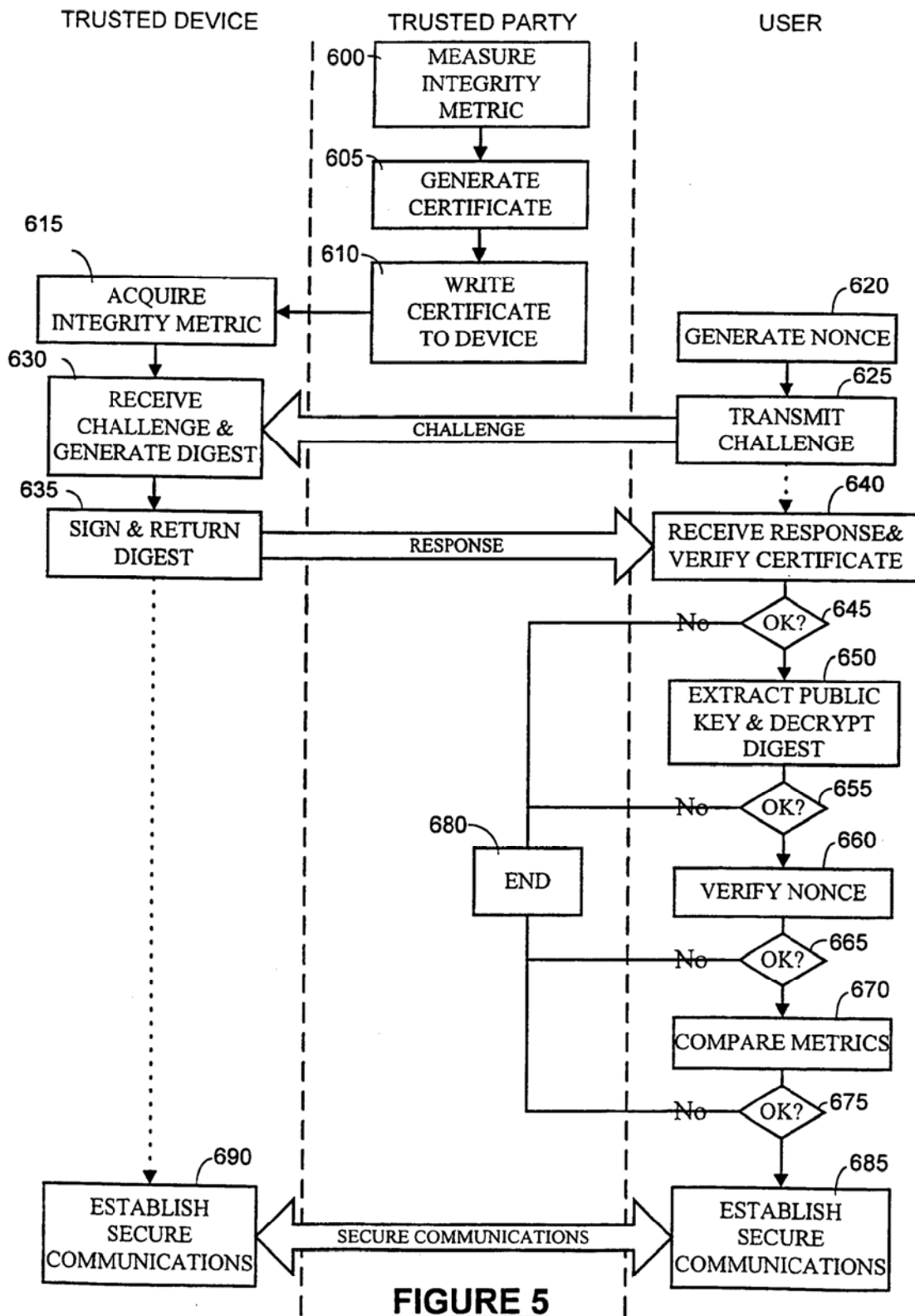
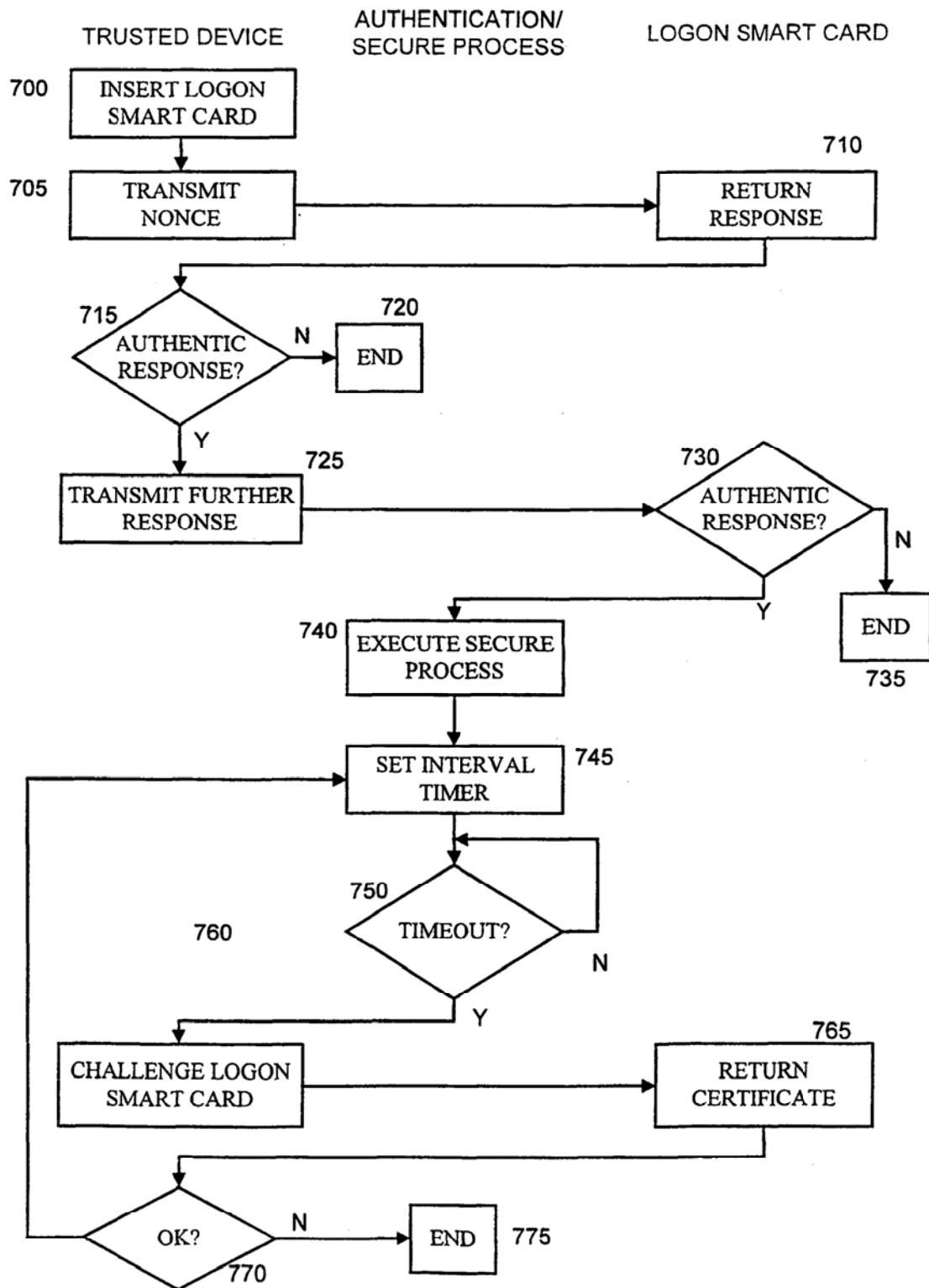


FIGURE 2



**FIGURE 4**

**FIGURE 5**

**FIGURE 6**

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 0849657 A [0004]

Non-patent literature cited in the description

- Information technology - Security techniques - Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm. *International Organization for Standardization*, November 1993 [0054]
- Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques. *International Organization for Standardization*, March 1997 [0065]