IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Michael GRELL
Ralf FINDEISEN
Frank SCHUECKE

Serial No.: Unknown

Filed: Concurrently Herewith

For: **A COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION**

§ Examiner: Unknown

§ Group Art Unit: Unknown

§ Attorney Docket: 2000.162700

§ Customer No. 23720

POWER OF ATTORNEY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The undersigned, being the inventors named in the above-identified application, hereby revoke any previous Powers of Attorney and appoint:

Kent Cooper, Reg. No. 37,296; Paul S. Drake, Reg. No. 33,491; and Barry Newberger, Reg. No. 41,527; of Advanced Micro Devices, Inc.; and

Terry D. Morgan, Reg. No. 31,181; J. Mike Amerson, Reg. No. 35,426; Jeffrey A. Pyle, Reg. No. 34,904; Jaison C. John, Reg. No. 50,737; Ruben S. Bains, Reg. No. 46,532; Mark W. Sincell, Reg. No. 52,226; and Scott F. Diring, Reg. No. 35,119 of Williams, Morgan & Amerson, P.C.,

as its attorney or agent so long as they remain with such firms, with full power of substitution and revocation, to prosecute the application, to make alterations and amendments therein, to transact all business in the Patent and Trademark Office in connection therewith, and to receive any Letters Patent, and for one year after issuance of such Letters Patent to file any request for a certificate of correction that may be deemed appropriate.

Please direct all communications to Customer No. 23720.

Signature: Michael Grell
Michael GRELL

Date: 04.07.2008

Signature: Ralf Findeisen
Ralf FINDEISEN

Date: 04.07.2008

Signature: Frank Schuecke
Frank SCHUECKE

Date: 04.07.2008

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Filer:	J. Mike Amerson/Mary Paul
Attorney Docket Number:	2000.162700/DE0892

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Claims in excess of 20	1202	1	52	52
Independent claims in excess of 3	1201	1	220	220
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1362**

Electronic Acknowledgement Receipt

EFS ID:	4636007
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	23720
Filer:	J. Mike Amerson/Mary Paul
Filer Authorized By:	J. Mike Amerson
Attorney Docket Number:	2000.162700/DE0892
Receipt Date:	19-JAN-2009
Filing Date:	
Time Stamp:	14:50:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1362
RAM confirmation Number	7595
Deposit Account	500786
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Patent_Application.pdf	282551 22974e1c1d53dbc41564b4ebdfdebed6bbb3a51b	yes	41

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	28
Claims	29	33
Abstract	34	34
Drawings-only black and white line drawings	35	41

Warnings:					
Information:					
2	Oath or Declaration filed	Declaration.pdf	97382 c65351cf40e9674e22878191d43cd71b8a6d8af8	no	2
Warnings:					
Information:					
3	Power of Attorney	Power_of_Attorney.pdf	41046 fa7889a39b90693fc716149ddc1ef0f56dc8fec6	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-06)	fee-info.pdf	38177 6fa5f03302109fab59c3e2cd1270870b97bd7c99	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	459156		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Application for United States Letters Patent

for

COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

by

Michael Grell
Ralf Findeisen
Frank Schuecke

COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

BACKGROUND

1. FIELD OF THE DISCLOSURE

The present disclosure generally relates to the field of computer systems of enhanced integrity and corresponding mechanisms implemented therein, which may enable the provision of enhanced security standards requiring a secure boot mechanism.

2. DESCRIPTION OF THE RELATED ART

The widespread use of computer systems has led to a significant increase of information processing on the basis of electronic computer systems, thereby involving the creation, distribution and processing of very large amounts of digital data. With the increasing capabilities of computer systems in view of data storage capacity and increased processing speed, the reproduction of large data sets, such as audio data, movies and the like, has become available for an increasing number of persons and is frequently practiced despite any protective rights, which may be associated with many of the data provided in electronic form. Thus, significant economic damage may be created by the illegal copying, storage and redistribution of electronic data. Furthermore, the distribution of application programs over widespread networks, such as the internet, may also provide the possibility of distributing malicious software applications, which may in turn be used for manipulating data and/or tampering with the configuration of a respective computer platform. For example, significant damage may be created in private environments, and in particular in the industry, by introducing software applications which may, for instance, manipulate software files such as stored data, communicate information via the internet without knowledge of the actual user of the platform, start a denial of service attack, thereby possibly rendering the platform to be no

longer usable for a dedicated application requiring a specific status of the platform, and the like.

For these reasons, great efforts are being made in developing mechanisms for enhancing integrity of computer platforms to reduce the probability of "successful" external attacks, for instance in the form of malicious software, denial of service attacks, sniffing, spoofing and the like, and also to enhance data integrity with respect to internal manipulations of the computer platform. For example, a plurality of encryption techniques are available, such as symmetric or asymmetric encryption/decryption techniques, which enable the exchange of data with a high degree of resistance against the tampering of data by a third party during the transmission and storage of data. In asymmetric encryption techniques, a pair of a private key and a public key may be used for encrypting data by means of one of the keys and deciphering the data by using the other key, wherein one of the keys may be publicly accessible. In symmetric key encryption techniques, a unique key is used for both the encryption and decryption of data, wherein access to the unique key may have to restricted to authorized parties. Although these techniques may provide enhanced integrity in data communication and data storage, the actual configuration of a computer platform under consideration may still provide the possibility of a plurality of attacks, in particular, as many applications intended for increasing computer security may rely on a trusted platform configuration.

A trusted computer platform may be considered as a computer system in which the hardware configuration as well as the software applications may be assumed to be in a dedicated configuration. However, a secure platform configuration may be established only be establishing a "chain" of trusted platform levels, wherein each subsequent level may be

initialized by the preceding level only if the integrity of the subsequent level has been verified. Hence, the integrity at system level may be preserved through a chain of integrity verifications, wherein a root of the chain of verification steps may have to be provided with a high degree of tamper resistance so as to also accomplish a high confidence with respect to integrity of the system after initializing the highest level, *i.e.*, the level of user applications.

In a typical computer platform, the initialization of the system requires various degrees of abstraction, for example, with respect to initializing the central processing unit (CPU), initializing the system memory, which is typically provided externally to the CPU, loading an operating system into the system memory from an external mass storage device, and finally executing user applications. Thus, in view of enhancing the overall integrity of the system as a whole, it may not be sufficient to assume that the various system activities prior to loading the operating system may be considered to be secure so as to rely on the integrity of the operating system and the user application, since the operating system may be invoked by a "mistrusted" process, thereby providing the opportunity of manipulating the basic platform configuration by modifying hardware and software components. Hence, the process of initializing the various hardware components of the computer system, such as the system memory and the execution of the instructions contained therein for initializing the higher system levels, which may also be referred to as boot strapping or booting, may have to be incorporated into the chain of trust to provide enhanced overall system integrity.

A typical start sequence for initializing a computer system after applying power or after a reset event causes a "power on self-test" of the CPU, wherein the processor also starts execution of instructions at a dedicated entry address that is indicated by the processor's reset vector. That is, after an initial processor self-test, the execution of instructions may start at

the entry point, which may typically be an address of a software routine, frequently referred to as BIOS (basic input/output system), which may be stored in a dedicated external non-volatile memory of the computer platform. Under the control of the BIOS, the remaining self-test may be performed and the hardware configuration of the platform may be determined or "measured." Thereafter, a search for a bootable device may be performed, such as a mass storage device, for instance, the hard disk of the computer system, a disk, a CD-ROM, an extension card and the like, from which a primary boot block may be loaded into the system memory, wherein control is then passed to the primary boot block, which may load an operating system into the system memory.

Although great efforts have been made in also enhancing security of the entire boot process, it is difficult to provide a reliable core root of trust for measurement (CRTM) for the boot process, for example, in view of platform modifications such as replacement of the non-volatile memory chip including the BIOS software, since a corresponding chip replacement may therefore interrupt the chain of trust, thereby also rendering all subsequent verification steps as not trustworthy. Hence, great efforts are made in providing a secure boot mechanism, wherein, however, frequently a trust center has to be used, thereby requiring comprehensive resources, whereas flexibility in updating the BIOS software may be reduced.

The present disclosure is directed to various devices and methods that may avoid, or at least reduce, the effects of one or more of the problems identified above.

SUMMARY OF THE DISCLOSURE

The following presents a simplified summary of the disclosure in order to provide a basic understanding of some aspects disclosed herein. This summary is not an exhaustive

overview, and it is not intended to identify key or critical elements of the invention or to delineate the scope of the invention. Its sole purpose is to present some concepts in a simplified form as a prelude to the more detailed description that is discussed later.

Generally, the present disclosure relates to devices and mechanisms for enhancing integrity of computer systems by establishing a static root of trust for measurement in that a certain set of data is provided that may include executable instructions and data values which, if a secure boot mechanism is enabled, will be accessed by the central processing unit without providing the possibility of circumventing access to the dedicated data set so that a defined root for the initialization of the platform is obtained. The set of data is implemented in such a manner that a high level of resistance against any attacks for manipulation may be achieved. During execution of instructions contained in the set of data, the execution may not be changed or interrupted, thereby providing a high degree of integrity of the data which may thus be considered as a pre-boot set of instructions and data values. Since the processing of the instructions of the pre-boot data is mandatory at the start-up time of the system under consideration, a chain of trusted software may be started, thereby enabling a high degree of system integrity since the dedicated state of pre-boot data represents the static core root for the chain of subsequent verification steps. According to the principles disclosed herein, an encryption key may also be stored in the internal non-volatile memory, which may be accessed during the pre-boot phase on the basis of the secure instruction set in order to verify the integrity of at least a portion of signed boot data, the signature of which may also be generated on the basis of the encryption key stored in the non-volatile memory. Hence, prior to actually initializing the system memory, the boot data, or at least a portion thereof, may be verified by determining a signature of the boot data and comparing the currently determined signature with the stored signature of the boot data. Consequently, using a unique symmetric

encryption key for any desired platform results in a higher level of protection and also makes the BIOS non-interchangeable. This may be accomplished without involving a trust center and may avoid general attacks which might concern a plurality of computer platforms, while at the same time a scaleable degree of security may be provided, wherein the "multiplicity" with which the unique symmetric encryption key is used may determine the "granularity" of the degree of security. In some illustrative aspects disclosed herein, the unique encryption key stored in the non-volatile internal memory may also be used for creating a signature upon updating of the system BIOS, thereby further enhancing the overall flexibility of the trusted platform mechanism disclosed herein. Since the pre-boot data set and the unique symmetric encryption key may be maintained in a non-volatile internal memory, for instance in the CPU core itself, a high degree of integrity of the encryption key is achieved while substantially avoiding any attacks, for instance, with respect to replacing BIOS chips and the like.

One illustrative method disclosed herein relates to booting of a computer system. The method comprises, upon a power-on event or a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, wherein the internal non-volatile memory area contains an encryption key. The method further comprises determining a current signature of at least a signed portion of boot data, wherein the signed portion of boot data concerns a stored signature of the portion of boot data wherein the stored signature is created by applying the encryption key. The method further comprises executing boot instructions contained in the signed portion of boot data when the current signature and the stored signature are identical.

A further illustrative method disclosed herein relates to the booting of a computer system. The method comprises, upon a power-up event or a reset event, accessing an internal

non-volatile memory of a central processing unit, wherein the internal non-volatile memory contains pre-boot instructions and data values for initializing an internal volatile memory of the central processing unit and for verifying the integrity of at least a portion of boot instructions and boot data values. The method further comprises loading the at least a portion of the boot instructions and boot data values from a non-volatile memory into the internal volatile memory by executing the pre-boot instructions. Furthermore, the method comprises verifying an integrity of the at least a portion of the boot instructions and boot data values by using an encryption key stored in the internal non-volatile memory and using a signature associated with the at least a portion of the boot instructions and boot data values, wherein the signature is formed on the basis of the encryption key. Additionally, the method comprises determining whether an upgrade version of the boot instructions and boot data values is available when the integrity of the at least a portion of the boot instructions and boot data values has been successfully verified. Finally, the method comprises generating a signature of the upgrade version by using the encryption key when an upgrade version is available.

An illustrative central processing unit (CPU) disclosed herein comprises a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting the CPU core, the volatile random access memory and the non-volatile memory. The CPU further comprises pre-boot information stored in the non-volatile memory, wherein the pre-boot information includes instructions executable by the CPU core which also includes a symmetric encryption key for verifying at least a portion of a boot routine that is assigned by applying the symmetric encryption key.

One illustrative computer system disclosed herein comprises a central processing unit as specified above and a non-volatile boot memory configured to hold at least a first boot routine and a second boot routine.

BRIEF DESCRIPTION OF THE DRAWINGS

The disclosure may be understood by reference to the following description taken in conjunction with the accompanying drawings, in which like reference numerals identify like elements, and in which:

Figure 1a schematically illustrates a central processing unit (CPU) including a random access memory (CACHE), a CPU core and a non-volatile memory including pre-boot information and a symmetric encryption key, according to illustrative embodiments;

Figure 1b schematically illustrates a computer system including a CPU with pre-boot information and an encryption key, according to other illustrative embodiments;

Figure 1c schematically illustrates a process for verifying a portion of BIOS data, also referred to as initial BIOS loader (IBL), on the basis of a symmetric encryption mechanism, according to illustrative embodiments;

Figure 1d schematically illustrates a flow diagram for a method of verifying integrity of boot data instructions and values, according to still further illustrative embodiments;

Figure 1e schematically illustrates a flow diagram of a method for verifying integrity of BIOS data and generating a signature for an upgrade version of BIOS data, according to still further illustrative embodiments; and

Figures 1f-1g schematically illustrate flow diagrams of methods for performing verification of BIOS integrity and updating the BIOS data, according to still other illustrative embodiments.

While the subject matter disclosed herein is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and are herein described in detail. It should be understood, however, that the description herein of specific embodiments is not intended to limit the invention to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION

Various illustrative embodiments are described below. In the interest of clarity, not all features of an actual implementation are described in this specification. It will of course be appreciated that in the development of any such actual embodiment, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which will vary from one implementation to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking for those of ordinary skill in the art having the benefit of this disclosure.

The present subject matter will now be described with reference to the attached figures. Various structures, systems and devices are schematically depicted in the drawings for purposes of explanation only and so as to not obscure the present disclosure with details that are well known to those skilled in the art. Nevertheless, the attached drawings are included to describe and explain illustrative examples of the present disclosure. The words and phrases used herein should be understood and interpreted to have a meaning consistent with the understanding of those words and phrases by those skilled in the relevant art. No special definition of a term or phrase, *i.e.*, a definition that is different from the ordinary and customary meaning as understood by those skilled in the art, is intended to be implied by consistent usage of the term or phrase herein. To the extent that a term or phrase is intended to have a special meaning, *i.e.*, a meaning other than that understood by skilled artisans, such a special definition will be expressly set forth in the specification in a definitional manner that directly and unequivocally provides the special definition for the term or phrase.

Generally, the present disclosure provides a system and a mechanism for executing – at start-up or reset or any other operational state requiring an initialization of the system – instructions stored in a memory area that may not be accessed after completing a verification phase of at least a portion of boot instructions. For this purpose, the verification process may be based on a symmetric encryption key also stored in a memory area that may be locked in view of any operational state of the CPU except for start-up or reset events. For example, the instructions and the symmetric encryption key may be stored in a non-volatile memory forming a part of a central processing unit, thereby significantly reducing the possibility of manipulating the data included in the non-volatile memory. Consequently, the contents of the non-volatile memory may be used as a static root of trust for measurement during the

initialization of the CPU and the entire computer system by ensuring that, upon power-up or reset of the CPU, the first instruction is fetched from the non-volatile memory. Thus, the set of data contained therein may serve as a pre-boot or pre-BIOS component, which may enable the initialization of further system components, such as an internal random access memory, which may be used for storing operational data like variables and stack and instructions for running a portion of the BIOS software. For instance, the data cache as part of the random access memory area and an instruction cache may be initialized by the pre-boot data of the internal non-volatile memory, thereby substantially avoiding the possibility of external access to data contained therein during the initialization process. That is, the random access memory area, *i.e.*, the data cache and the instruction cache, are CPU-internal components so that unwanted manipulation thereof may be very difficult, in particular as the external system memory is not initialized, as long as at least a portion of the BIOS software has been verified. Depending on the storage capacity of the random access memory, the BIOS routine may be divided into two or more portions such that verification of one or more signatures in view of BIOS integrity may be performed in the random access memory for a first portion that is configured to have a size to fit into the cache memory. Thus, this portion of the boot information may, after verification on the basis of the symmetric encryption key, be executed, for instance, directly from the random access memory, thereby substantially avoiding any manipulation process of verifying the first portion of the boot instructions. Thus, after verification of the signature of the first portion by applying the stored symmetric encryption key, flow control may be passed to the verified portion and the further boot process may be continued by initializing the system memory and copying the remaining boot information, while also verifying integrity of the further boot information, for instance, on the basis of hash algorithms wherein, however, the generation of a signature may not be required, due to the chain of trust created to the preceding verification on the basis of a signature and the

stored symmetric encryption key. Consequently, the data, *i.e.*, the instructions and data values including the symmetric encryption key contained in a non-volatile internal memory area provided as an integral part of the CPU, may be used as a static core root of trust for measurement, thereby providing a computer platform in which a tamper-resistant system hardware and software configuration may be realized. In particular, in view of attacks, such as replacement of the BIOS chip, the mechanism of embodiments disclosed herein may provide enhanced security for typical practical applications, which use the platform in the context of financial transactions or digital rights management, which may be based on the requirement of a trustworthy computer platform. Additionally, using a symmetric encryption key mechanism provides security without having to rely on a trust center for handling private and public keys, as is the case in asymmetric encryption techniques, thereby significantly reducing the overall complexity. At the same time, the desired degree of security may be determined by restricting the usage of the unique encryption key to a specified type of central processing unit so that manipulations or loss of secrecy for one unique encryption key may not affect other CPUs that have been fabricated on the basis of a different unique encryption key. Moreover, illustrative embodiments disclosed herein may provide an efficient technique for updating the BIOS software using the stored encryption key for generating a respective signature, which may then be added to the upgrade version of the BIOS software, which may then be verified upon booting the computer system on the basis of the newly created signature and the stored encryption key.

Figure 1a schematically illustrates a central processing unit (CPU) 100 according to illustrative embodiments in which a core root of trust for measurement (CRTM) may be implemented with a high degree of tamper resistance. The CPU 100 may comprise a CPU core 102 which may include components for data processing, such as for performing

arithmetic operations, logic operations and the like. The CPU core 102 may be functionally connected to a random access memory 101, which may comprise a plurality of static RAM cells and the like, corresponding to the overall configuration of the CPU 100. In one illustrative embodiment, the RAM 101 may comprise a first memory portion, also indicated as data cache 101A, and a second portion indicated as instruction cache 101B. For example, the RAM 101 may be implemented in a fast memory technology so as to enhance the overall performance of the CPU 100, as is typically required in sophisticated applications. It should be appreciated, however, that any appropriate memory technology may be used for the memory 101, as long as direct control of the memory 101 via the CPU core 102 may be accomplished without the possibility of external access during the initialization of the CPU 100. The CPU 100 may further comprise a non-volatile memory 103, which may be provided in any appropriate memory technology, for instance in the form of a flash memory or a read-only memory technique, which may not enable external access for modifying the contents of the memory 103. Hence, the memory 103 may be considered as a secure memory area, the contents of which may therefore represent a static root of trust. For this purpose, a set of data 103A, which is to be understood as instructions executable by the CPU core 102 and data values representing operands and the like of the instructions, may be provided, at least in a portion of the memory 103, which may not be overwritten with new data once the respective portion of the memory 103 is programmed. Additionally, the memory 103 may contain a symmetric encryption key 103B, which may also be used for signing a portion of boot information that may initially be used for initializing a computer system comprising the CPU 100. It should be appreciated that the memory 103 may not necessarily represent a continuous memory area, a portion of which may contain the data set 103A and a portion of which may contain the encryption key 103B, but may be implemented in any appropriate manner, for instance as substantially independent components of the CPU 100, as long as

external access of the data set 103A and the encryption key 103B may be suppressed after a certain phase of the initialization process. Furthermore, the CPU 100 may comprise a lock mechanism 105, which may be configured such that access of the CPU core 102 to the memory 103, or at least the encryption key 103B, may be enabled upon power-on or a reset event only, while disabling the memory 103, which may be accomplished by instructing the lock mechanism 105 during the boot process after verification of at least a portion of the boot information. For instance, the lock mechanism 105 may comprise circuitry for shutting down supply energy for the memory 103 and also for the mechanism 105 itself, thereby locking the mechanism 105 and also the memory 103 non-responsive to any accesses performed after a request for "locking" the memory 103 or at least a portion thereof including the symmetric encryption key 103B. On the other hand, enabling the memory 103, for instance by providing power to the lock mechanism 105, may be associated with a power-up or a reset event only. It should be appreciated, however, that the lock mechanism 105 may have any other appropriate configuration in which external access to the encryption key 103B may be restricted to an operational status of the CPU 100 in which, after reset or power-on, a corresponding instruction for locking the encryption key 103B has not yet been executed.

The internal components of the CPU 100, that is, the memory 103, the CPU core 102, the internal RAM 101 and the lock mechanism 105, may be interconnected by means of a bus system 104 such that, upon power-up or reset, a jump to a specified address of the memory 103 is performed. Consequently, a "hard-wired" target for a reset vector of the CPU core 102 may be provided which ensures that execution of instructions may start from the memory 103, at least for a power-up event or a reset event.

It should be appreciated that the CPU 100 may be formed on the basis of sophisticated semiconductor manufacturing techniques in which an appropriate carrier material, such as a semiconductor substrate and the like, may receive a plurality of circuit elements formed on the basis of a technology under consideration, such as CMOS processes and the like, in which transistor elements, capacitors, resistors and the like may be formed in accordance with specific device architecture for the CPU 100. In the embodiments illustrated herein, the various components of the CPU 100 may therefore be formed on a common substrate during a common manufacturing process flow, thereby providing the memory 101 and 103 as an internal or integral component of the device 100. For example, respective manufacturing techniques are well established in which volatile and fast memory cells may be formed together with non-volatile memory cells and high performance logic gates, as may be required in the CPU core 102. Additionally, appropriate mechanisms may be provided such that, after programming the memory 103 or at least a portion thereof, including the data set 103A and the symmetric unique encryption key 103B, further access may be prevented so as to provide a protected environment for the data set 103A and the encryption key 103B.

Figure 1b schematically illustrates a computer system 150 comprising the CPU 100 providing the protected environment for the data set 103A and the encryption key 103B, as previously explained, wherein, in the embodiment shown, the CPU 100 may comprise the random access memory 101 in the form of the data cache 101A and the instruction cache 101B, which may have a size of, for example, 64 Kb to accommodate a portion of boot information and to act as a "system RAM" when performing instructions of the data set 103A. Similarly, the instruction cache 101B may be provided with the size of 64 Kb, wherein it should be appreciated that any other appropriate memory size may be used that is compatible with the size of a respective portion of boot information that is to be performed

from the memory 101 during a verification process. Also, the internal non-volatile memory 103 may be provided with any appropriate size and configuration so as to be compatible with the requirements for the data 103A and the symmetric encryption key 103B. For example, the set of data 103A may comprise instructions and data values representing a secure load routine for loading a respective portion of boot information into the internal memory 101 for performing a verification process.

The computer system 150 may further comprise a system memory 110, for instance in the form of any appropriate memory device including random access memory cells, such as dynamic RAM cells and the like. The size of the system memory 110 may be adapted to the requirements of the system 150 in view of performance and storage capacity. Furthermore, the system 150 may comprise a non-volatile memory 120, such as a flash memory and the like, which may include information, also referred to as BIOS information, at least a portion of which may be a signed portion, that is, a signed portion may comprise a signature obtained on the basis of an appropriate hash algorithm in combination with an encryption mechanism using the symmetric encryption key 103B as stored in the memory 103. In one illustrative embodiment, the non-volatile memory 120 may contain the boot information divided into two portions, wherein a first portion may comprise data and instructions for initializing other system components, such as the system memory 110 for accommodating the second portion of boot information and executing the second portion once the first portion has been verified on the basis of the protected environment provided by the CPU 100. The first portion may also be referred to as an initial boot loader (IBL), which may represent the signed portion of the boot information contained in the memory 120.

In some illustrative embodiments, the non-volatile memory 120 may comprise a first portion 120A for containing a first BIOS version that may be accessed upon initializing the system 150, which may be indicated as an enabled version of BIOS information contained in the memory 120. Moreover, a second portion 120B may be provided, which may contain a second BIOS version, such as an upgrade version, and which may be in a non-enabled state, thereby requiring validation and the creation of a signature on the basis of the stored encryption key 103B during an initialization phase, as will be described later on in more detail. Consequently, the memory 120 may have a sufficient capacity for holding at least two BIOS versions, thereby providing the possibility of efficiently updating the BIOS information for the system 150 while nevertheless providing enhanced security of the update process, as will be described later on.

The computer system 150 may further comprise an interface system 140 configured to operatively connect the system memory 110 and the non-volatile memory 120 with the CPU 100. In one illustrative embodiment, the system 150 may further comprise a one-time programmable memory 130, which may include platform-specific information, for instance about boot sources and related parameters. For instance, as shown, the one-time programmable memory 130 may comprise information concerning boot options in order to indicate to the CPU 100 whether to boot from the internal memory 103 or not. For example, security bits may provided in the memory 130 including a respective bit that determines where the initial instruction fetch of the CPU 100 after reset is rooted to. For example, with this bit set to "1", execution may be passed to the internal memory 103, thereby enabling the secure boot processing. It should be appreciated that, in other illustrative embodiments, the one-time programmable memory 130 may be omitted or may be provided so as to include other

information controlling the secure boot processing during development and actual applications.

Figure 1c schematically illustrates the configuration of boot information 121 that may be stored in the non-volatile memory 120, for instance in one of the portions 120A, 120B, as an "enabled" version of boot information contained therein. In the embodiment shown in Figure 1c, the boot information 121, which may also be referred to as BIOS, may comprise a first portion 121A which may represent a set of data including instructions and data values having a size so as to be compatible with the size of the memory 101, as previously explained. For example, for the above-given exemplary values of 64 Kb for each of the RAM areas 101A, 101B, a maximum size of the portion 121A may be restricted to be approximately 32 Kb. It should be appreciated, however, that any other appropriate size for the portion 121A may be applied, depending on the available amount of storage within the RAM 101. It should further be appreciated that providing the portion 121A may be necessary for boot information 121 which exceeds the size of the memory 101, so that the entire boot processing may not be performed on the basis of the memory 101, since typical boot routines may have a size of several hundred kilobytes and more. In other cases, when sufficient storage space may be available in the CPU 100, the boot information 121 as a whole may be used during the secure boot processing, as will be explained later on in more detail.

Thus, if the portion 121A may be provided, as shown in Figure 1c, this portion may serve as an initial BIOS loader (IBL) for a second portion 121B, wherein the first portion 121A may also contain a hash value obtained over the portion 121B. The hash value for the portion 121B may also be protected by a signature contained in the portion 121A obtained from a hash value generated over the first portion 121A, which may be encrypted by the

encryption key 103B. Thus, an encryption of the hash value of the second portion may not be necessary. The signature of the hash value for the portion 121A may be used for verifying the portion 121A during a secure boot processing. The portion 121A may, therefore, be contained in instructions for performing necessary platform initialization actions, such as initialization of a memory controller 141 and the like, followed by the shadowing of the portion 121B from the memory 120, *i.e.*, from one of the portions 120A, 120B, into the initialized system memory 110. Thus, after storing the portion 121A, 121B, the respective hash values may be created and may be added to the portion 121A, which may then, for an initial version of the BIOS information 121, be encrypted by a version of the symmetric encryption key 103B. The corresponding signature obtained by applying the key 103B may also be added to the portion 121A, as shown at the right-hand side of Figure 1c.

Figure 1d schematically illustrates a sequence for verifying the signature 121S contained in the portion 121A, which may be performed on the basis of the data set 103A and the encryption key 103B during start-up or reset of the system 150. The verification may be accomplished on the basis of any appropriate encryption algorithm using the symmetric key 103B, wherein the initially created hash value, such as hash 0, obtained over the portion 121A, which may include respective hash values for the portion 121B, may be used for generating the signature 121S by applying the key 103B. The initially created hash value for the portion 121A may then be compared to a respective hash value obtained by applying the appropriate hash algorithm over the portion 121A that is copied into the RAM memory 101. The portion 121A may be considered as verified if a signature generated by applying the key 103B to a calculated hash value match with the signature 121S contained in the portion 121A.

In view of implementing the system 150 as a secure platform, a static root of trust may have to be implemented to enable a secure start-up of an operating system after power-up or reset of the computer system 150. For this purpose, a defined execution of the trusted BIOS information 121 may be accomplished by verifying at least the portion 121A on the basis of the trusted set of data 103A and the encryption key 103B, which are substantially resistant against any external manipulation. Thus, each time the system 150 may be activated by using a secure boot process, thereby enabling integrity of the entire boot process and trusted initialization of an operating system, which in turn may be used for performing security sensitive applications. On the other hand, if the integrity check may fail, for instance, during verifying the portions 121A or 121B, an appropriate policy may be applied, for instance the boot process may be terminated or services provided by the system 150 may be limited. Thus, the secure boot architecture disclosed herein may protect against "class breaks," which are to be understood as attacks that will work against every instance of a given security system. For example, a piece of software generated by an external source may be considered as class break, which may be easy to install and enable circumvention of security measures, thereby enabling unauthorized use of the platform. In digital rights management (DRM) environments, a class break may already be given when the DRM protected data file may be broken once, thereby enabling a redistribution of the unprotected file. Consequently, the mechanisms and systems disclosed herein may provide enhanced security with respect to class breaks since a protected environment may be obtained on the basis of an integral portion within the CPU itself, thereby requiring manipulation of the CPU itself, wherein, for instance, the revealing of the encryption key 103B may only concern respective CPUs into which this version of the encryption key 103B has been incorporated during the production process, while, however, other products manufactured on the basis of a different encryption key may nevertheless provide a secure platform.

In step 161, the system may be reset or power may be supplied thereto or any other event may occur that may require a secure boot processing. Consequently, an appropriate self-test may be performed by the CPU core 102 and respective components, such as registers and the like, may be initialized. It should be appreciated that, in some embodiments, a secure boot processing may not be enabled in an operating state in which the operating system may stay in control of the system 150. In step 162, the first instruction is fetched from the internal non-volatile memory 103, which may be accomplished by mapping the internal memory 103 to the corresponding reset vector address. Consequently, the CPU 100 starts execution on the basis of the secure data set 103A in any instances in which a jump to the reset vector is caused by an external event. In step 163, the internal random access memory 101 may be initialized, caused by the execution of the instructions contained in the data set 103A. In step 164, at least a portion of the boot information 121, for instance the portion 121A, including the signature 121S thereof, may be loaded into the internal random access memory 101. As previously explained, the signature 121S has been generated by applying the symmetric encryption key 103B. In step 165, a signature of the boot data in the memory 101, for instance the portion 121A, is generated by, for instance, calculating a respective hash value, as previously explained, and applying the encryption key 103B by accessing the memory 103.

In step 166, the currently calculated signature is compared with the signature 121S and, if both values match, the process flow advances to step 167 in which the boot process may be continued, for instance, by initializing the system memory and verifying the rest of the boot information 121. In the verification phase in step 166, the encryption key 103B is locked in step 168, for instance by disabling a respective portion of the memory 103 via the

lock mechanism 105, as previously explained. Next, in step 169, the boot process may be terminated, which may include, for instance, an indication that an invalid BIOS information 121 is present in the internal memory 120.

Figure 1e schematically illustrates a sequence of steps for continuing the boot process after step 167 in Figure 1d. In step 167A, the system memory 110 may be initialized and, in step 167B, the BIOS information 121, or at least the portion 121B, may be loaded into the system memory 110. In step 167C, the BIOS information 121, or at least the portion 121B, may be verified in the system memory 110, for instance, by calculating one or more respective hash values and comparing the values with the corresponding hash values contained in the portion 121A, which has been verified in step 166 (Figure 1d). In step 167D, the process flow branches into step 167E, when the remaining portion of the boot information has not been verified, or into step 167F, when the boot process may be continued, for instance, by loading the operating system, as previously explained.

In the above-described embodiment, before passing execution to the boot information 121 or the portion 121A, the secure boot process, *i.e.*, the process flow represented by the steps 161-166, may not apply any reset procedures to any components of the system 150, thereby enabling reliable "measurement" of the hardware configuration of the system 150.

Figure 1f schematically illustrates a flow diagram for representing the operation of the system 150 when updating of a BIOS information may be possible. In step 171, a reset event, such as power-on, may occur and the process flow may advance to step 172, in which it is determined whether the secure boot processing is enabled or not. If secure boot processing is not enabled, which may be advantageous during testing and debugging the system 150, an

alternative process flow may be initiated. If secure boot processing is enabled, the process flow may advance to step 173 in which execution of instructions may be started by accessing the internal non-volatile memory 103 and performing instructions of the set 103A, as previously explained. In step 174, integrity of at least a portion of the boot information, such as the portion 121A, may be checked, for instance, in the same way as previously described with reference to the process flow in Figure 1d. If integrity of the boot information 121A is not verified in step 174, the process may advance to step 175 in which the encryption key 103B may be locked and the boot process may be terminated or booting may be continued, however, with limited services provided by the system 150. If integrity is validated in step 174, execution of instructions of the boot information 121A may be started in step 176. In step 177, it may be determined whether or not updating of the BIOS information 121 may be required. For this purpose, for instance, the internal memory 110 may be accessed to determine whether or not a non-enabled version of BIOS information is available or not. If a respective updating of the BIOS information is not required, the process flow advances to step 178 in which the encryption key 103B is locked, as previously explained. Thereafter, in step 179, the boot processing may be continued, as previously explained. When, in step 177, updating of the BIOS information 121 is required, the process flow advances to step 180 in which the BIOS version contained in one of the memory areas 120A or 120B of the non-volatile memory 120 may be validated. For this purpose, any appropriate mechanism may be used, for instance, using an asymmetric encryption mechanism, on which, upon creating the BIOS version, respective hash sums may have been calculated and have been encrypted by a secret key, which may now be validated on the basis of a public key, which may be contained in the new BIOS information.

When, in step 181, a valid version of the new BIOS information is identified, a signature may be created by applying the encryption key 103B in that a respective hash sum may be calculated over the respective IBL portion of the new BIOS information, which may then be signed by applying the encryption key 103B. In step 182, the encryption key 103B may then be locked, as previously explained, and, in step 183, the signature generated in step 181 may be added to the new BIOS information, for instance to the respective IBL portion 121A, when the BIOS information is provided in several parts. In step 184, the new BIOS information may be enabled, that is, an indication may be stored in the non-volatile memory 103 or any other appropriate storage that the new BIOS version is a BIOS information to be used for performing the boot process. In step 185, a reset event is generated so that the process flow returns to step 171. Consequently, upon enabling the upgrade version of the BIOS information in step 184, the steps 172-177 may be repeated on the basis of the upgrading of the BIOS information and the boot processing may be performed on the basis of the new BIOS information.

Figure 1g schematically illustrates a secure boot processing according to still other illustrative embodiments. As shown, in steps 181 and 182, reset events may be detected and it may be determined whether or not secure boot is enabled, as also previously explained. In step 183, instruction execution is performed from the internal data set 103A. In step 184, a CPU internal initialization may take place. In some illustrative embodiments, this may include steps 184A-184J. For example, in step 184A, the memory 103 may be remapped. In step 184B, a boot source may be detected and may be initialized in step 184C, followed by initialization of the data cache 101A and the instruction cache 101B according to steps 184D, 184E. In step 184F, an unreal mode for the data cache may be set up and the image of the boot information 121 for the portion 121A may be copied into the data cache 101A, while, in

step 184H, storage space may be assigned for variables in the data cache 101A. If required, in step 184I, vendor identification may be retrieved and, in step 184J, a respective encryption engine may be initialized. Thereafter, in step 185, the hash sum over the signed BIOS data 121A, that is, the IBL, may be calculated. In step 186, the internal encryption key 103B may be applied to a previously calculated hash sum to generate a signature. In step 187, the signature determined in step 186 may be compared with the signature contained in the signed BIOS information 121A. In step 189, the boot processing may be terminated if the signed BIOS information has been identified as an invalid information and the internal key 103B may be locked in step 189. In step 188, execution of the BIOS information may be started when a valid version of the BIOS information has been identified in step 187. In step 190, it may be determined whether updating of the BIOS information is required. If so, in step 191, the new BIOS information may be validated, for instance as previously indicated, and, in step 192, it may be decided whether or not the new BIOS information is valid information or not. If a valid BIOS version is detected in step 192, in step 193, a hash sum may be calculated over the new BIOS information, *i.e.*, a respective portion thereof, such as an IBL portion, and, in step 194, the internal encryption key 103B may be applied to the hash value to generate a new signature. In step 195, the internal key used in step 194 may be locked and, in step 196, the newly created signature may be added to the new BIOS information. In step 197, the new BIOS information may be enabled, as also previously explained. If in step 192 the new BIOS information is identified as an invalid information or if in step 190 updating of the BIOS information is not required, the process flow advances to step 198, in which the encryption key 103B may be locked. Thereafter, the boot processing may continue in step 199 which, in some illustrative embodiments, may include the initialization of further system components of the system 150, such as the system memory 110 in step 199A. Thereafter, in step 199B, the BIOS information, as presently enabled, may be loaded into the system

memory and, in step 199C, the BIOS information may be verified, for instance, by calculating respective hash sums and comparing the hash sums with the values contained in the BIOS information, as previously explained. If in step 199D the BIOS information is identified as valid information, the boot processing may be continued in step 199E, for instance by performing further steps for finally loading an operating system. If in step 199D the BIOS information is identified as an invalid BIOS information, in step 199F, the boot process may be terminated or an indication may be given and the services of the system 150 may be enabled in a restricted form, as previously explained.

As a result, the systems and mechanisms disclosed herein provide enhanced integrity of computer platforms by providing a secure boot processing on the basis of a pre-boot routine contained in a non-volatile memory and a symmetric encryption key. Since the non-volatile memory is a part of the CPU itself, system initialization may be accomplished on the basis of the pre-boot information stored in the non-volatile internal memory and verification of the boot information may be accomplished by using the symmetric encryption key. Thus, enhanced security of the platform may be accomplished without requiring a trust center, wherein an efficient protection against class breaks may be obtained, while the degree of security may be determined on the basis of the granularity of the symmetric encryption key, which may be incorporated into the non-volatile memory during fabrication of the CPU device.

The particular embodiments disclosed above are illustrative only, as the invention may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. For example, the process steps set forth above may be performed in a different order. Furthermore, no limitations are intended to the

details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope and spirit of the invention. Accordingly, the protection sought herein is as set forth in the claims below.

CLAIMS

WHAT IS CLAIMED:

1. A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

2. The method of claim 1, wherein executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory.

3. The method of claim 2, wherein executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data.

4. The method of claim 2, wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache.

5. The method of claim 1, further comprising locking said encryption key for external access prior to executing said boot instructions.

6. The method of claim 5, further comprising determining whether an upgrade version of said boot data is available.

7. The method of claim 6, wherein determining whether an upgrade version of said boot data is available is performed prior to locking said encryption key.

8. The method of claim 7, further comprising verifying said upgrade version of said boot data.

9. The method of claim 8, further comprising calculating a new signature over a hash sum of said upgrade version of the boot data using said encryption key and adding said new signature to said upgrade version of the boot data.

10. The method of claim 9, further comprising enabling said upgrade version of said boot data.

11. The method of claim 10, further comprising generating a reset event.

12. The method of claim 10, further comprising locking said encryption key prior to enabling said upgrade version of the boot data.

13. A method for booting a computer system, the method comprising:

upon at least one of a power-up event and a reset event, accessing an internal non-volatile memory of a central processing unit, said internal non-volatile memory containing pre-boot instructions and data values for initializing an internal volatile memory of said central processing unit and verifying an integrity of at least a portion of boot instructions and boot data values;

loading said at least a portion of said boot instructions and boot data values from a non-volatile memory into said internal volatile memory by executing said pre-boot instructions;

verifying integrity of said at least a portion of said boot instructions and boot data values by using an encryption key stored in said internal non-volatile memory and a signature associated with said at least a portion of said boot instructions and boot data values, said signature being formed on the basis of said encryption key;

after successfully verifying integrity of said at least a portion of said boot instructions and boot data values, determining whether an upgrade version of said boot instructions and boot data values is available; and

when an upgrade version is available, generating a signature of said upgrade version by using said encryption key.

14. The method of claim 13, wherein executing said boot instructions comprises initializing a system memory of said computer system and loading a second portion of boot instructions and boot data values into said system memory.

15. The method of claim 14, further comprising verifying integrity of said second portion and continuing booting of said computer system on the basis of said second portion when verification of said second portion is successful.

16. The method of claim 13, wherein initializing said volatile internal memory comprises initializing a data cache of said central processing unit and wherein said at least a portion is loaded into said data cache and is verified therein.

17. The method of claim 13, further comprising locking said encryption key prior to executing said boot instructions when an upgrade version is not available.

18. The method of claim 13, further comprising verifying said upgrade version of the boot instructions and boot data prior to generating said new signature.

19. A central processing unit (CPU), comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric

encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key.

20. The central processing unit of claim 19, further comprising a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power-on event only.

21. A computer system, comprising:

a central processing unit comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory, and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key; and

a non-volatile boot memory configured to hold at least said boot routine and a second boot routine.

ABSTRACT OF THE DISCLOSURE

A CPU, a computer system and a secure boot mechanism are provided in which a symmetric encryption key may be incorporated into a non-volatile memory area of the CPU core, thereby substantially avoiding any tampering of the encryption key by external sources. Moreover, pre-boot information may be internally stored in the CPU and may be retrieved upon a reset or power-on event in order to verify a signed boot information on the basis of the internal symmetric encryption key. Furthermore, the BIOS information may be efficiently updated by generating a signature using the internal encryption key.

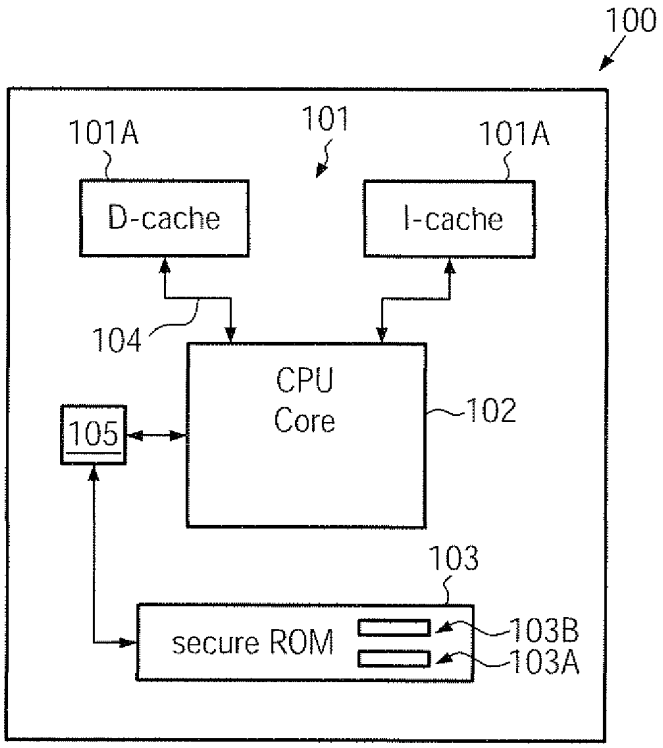

100
101A
101
101A
D-cache
I-cache
104
CPU
Core
102
105
103
secure ROM
103B
103A

FIG. 1a

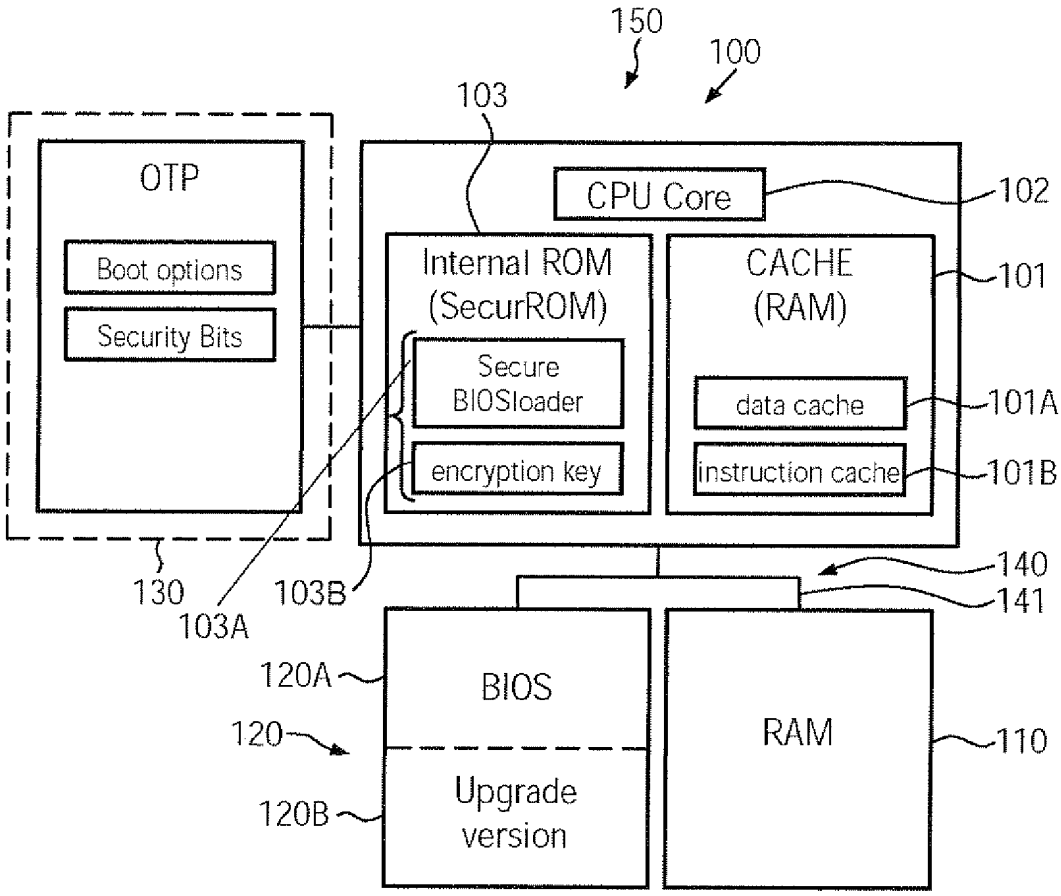

150
100
103
OTP
Boot options
Security Bits
CPU Core
102
Internal ROM
(SecurROM)
Secure
BIOSloader
encryption key
CACHE
(RAM)
101
data cache
101A
instruction cache
101B
130
103A
103B
140
141
120A
BIOS
120
Upgrade
version
120B
RAM
110

FIG. 1b

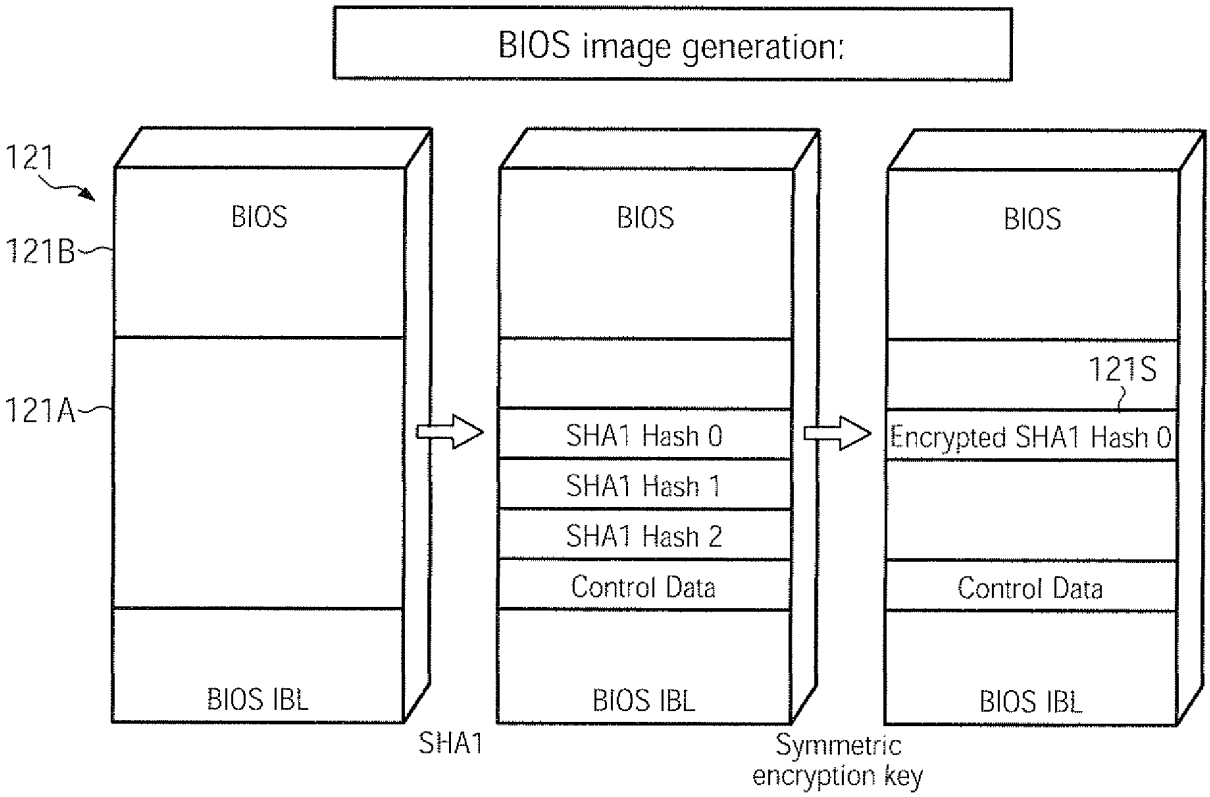

BIOS image generation:
121
121B
121A
BIOS
BIOS IBL
SHA1
BIOS
SHA1 Hash 0
SHA1 Hash 1
SHA1 Hash 2
Control Data
BIOS IBL
Symmetric
encryption key
BIOS
121S
Encrypted SHA1 Hash 0
Control Data
BIOS IBL

FIG. 1c

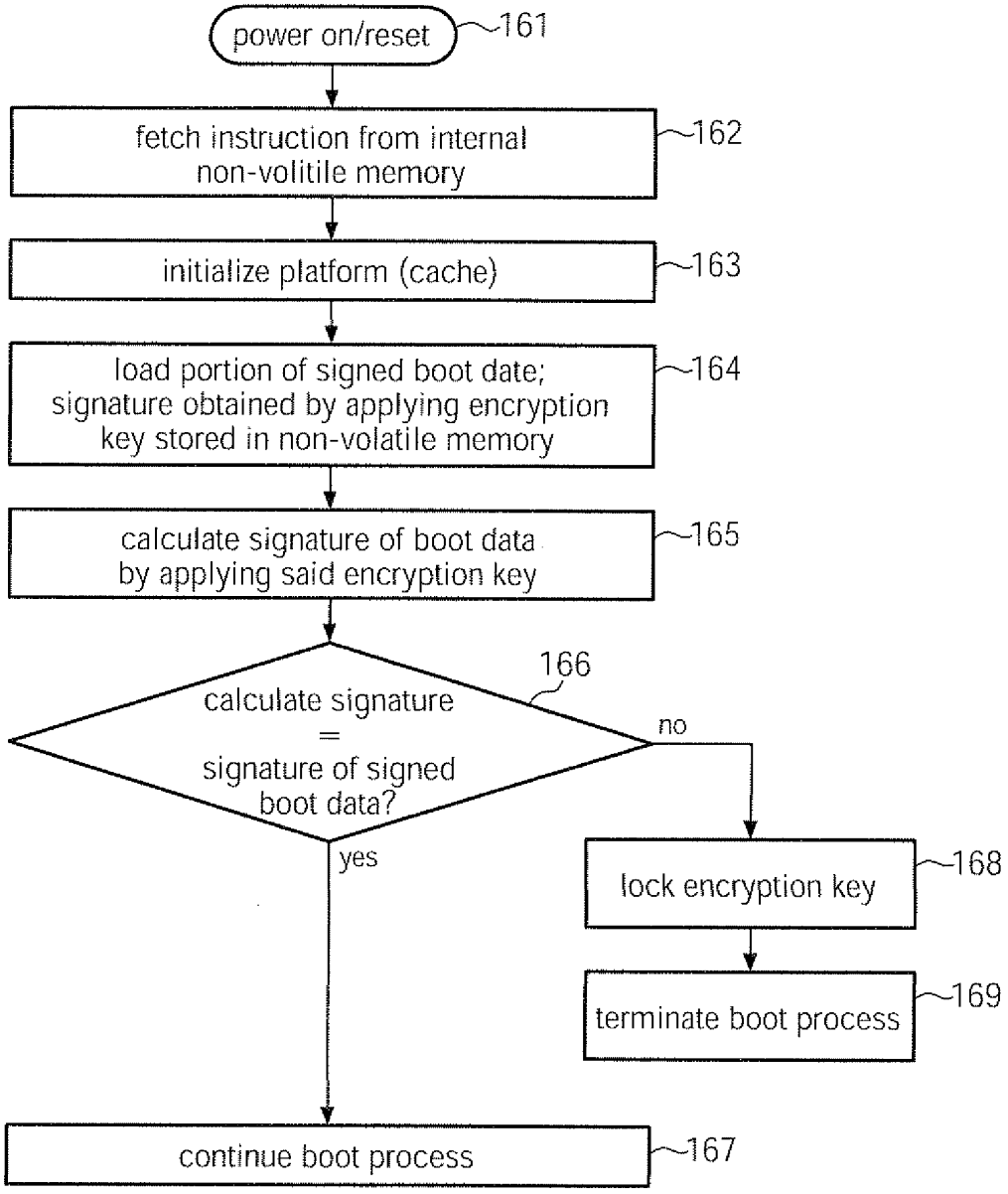

power on/reset
161
fetch instruction from internal non-volitile memory
162
initialize platform (cache)
163
load portion of signed boot date; signature obtained by applying encryption key stored in non-volatile memory
164
calculate signature of boot data by applying said encryption key
165
calculate signature = signature of signed boot data?
166
no
yes
lock encryption key
168
terminate boot process
169
continue boot process
167

FIG. 1d

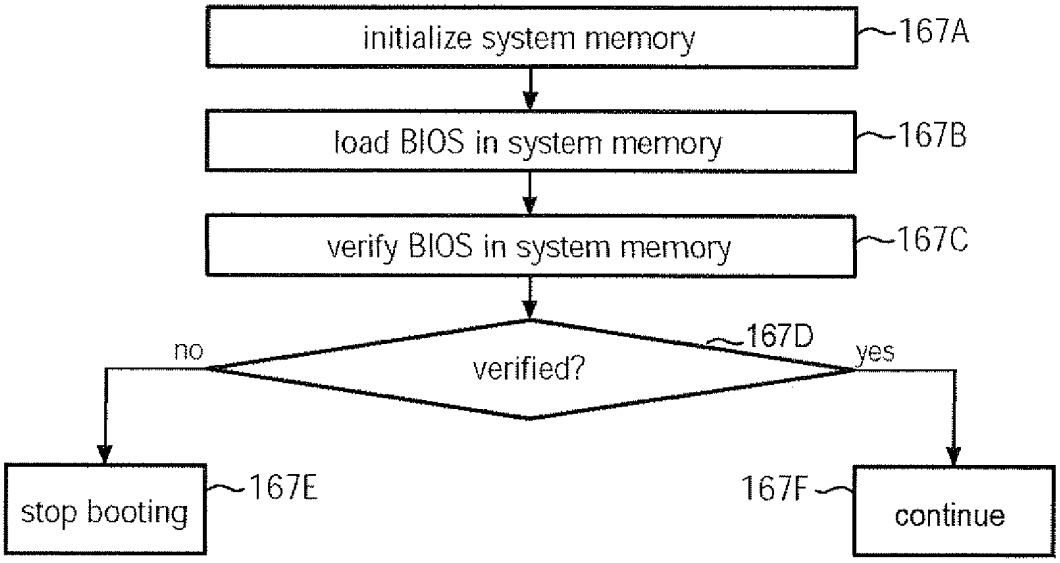

initialize system memory
167A
load BIOS in system memory
167B
verify BIOS in system memory
167C
verified?
167D
no
yes
stop booting
167E
167F
continue

FIG. 1e

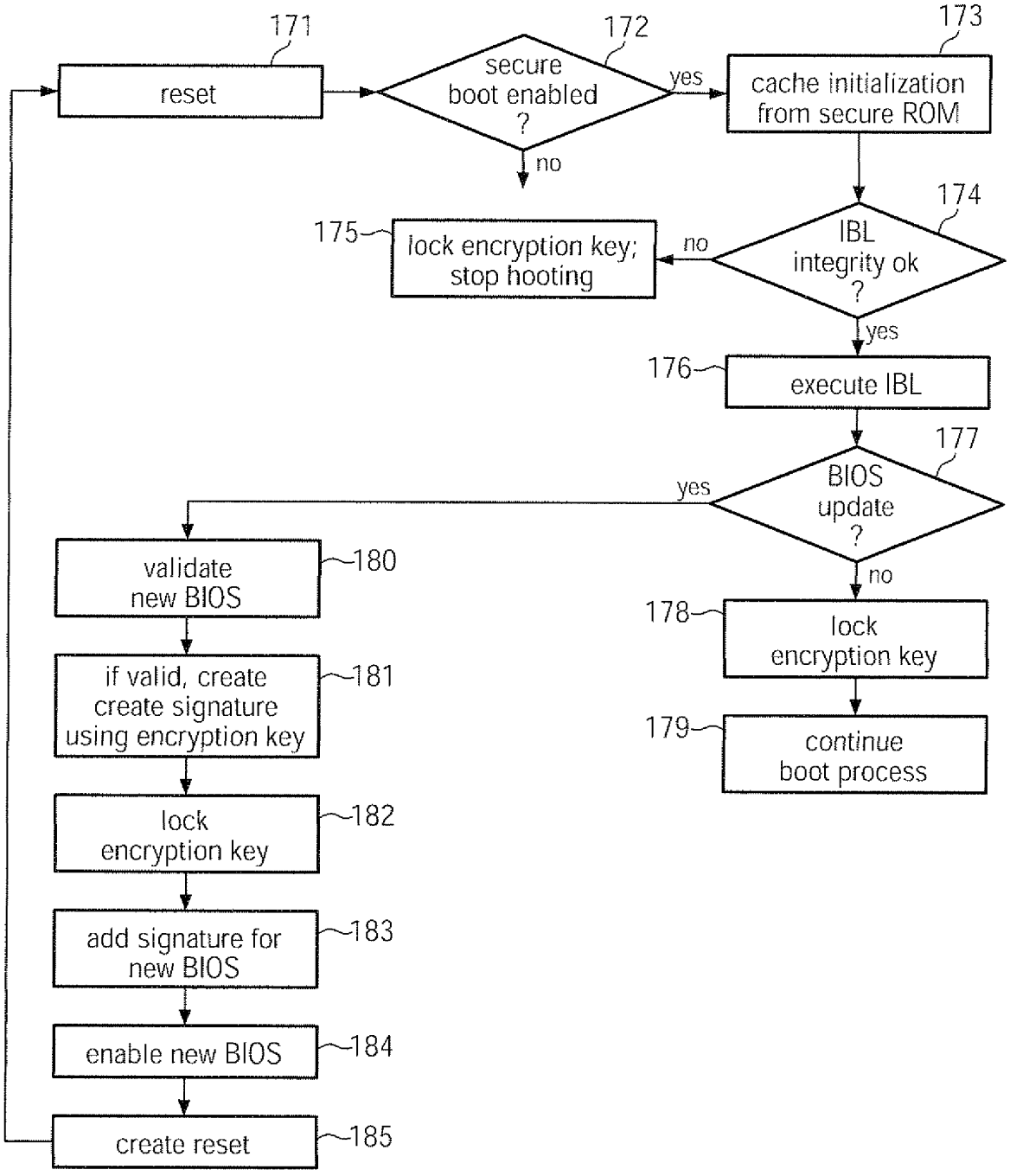

171
reset
172
secure boot enabled ?
yes
no
173
cache initialization from secure ROM
174
IBL integrity ok ?
no
175
lock encryption key; stop hooting
yes
176
execute IBL
177
BIOS update ?
yes
no
178
lock encryption key
179
continue boot process
180
validate new BIOS
181
if valid, create create signature using encryption key
182
lock encryption key
183
add signature for new BIOS
184
enable new BIOS
185
create reset

FIG. 1f

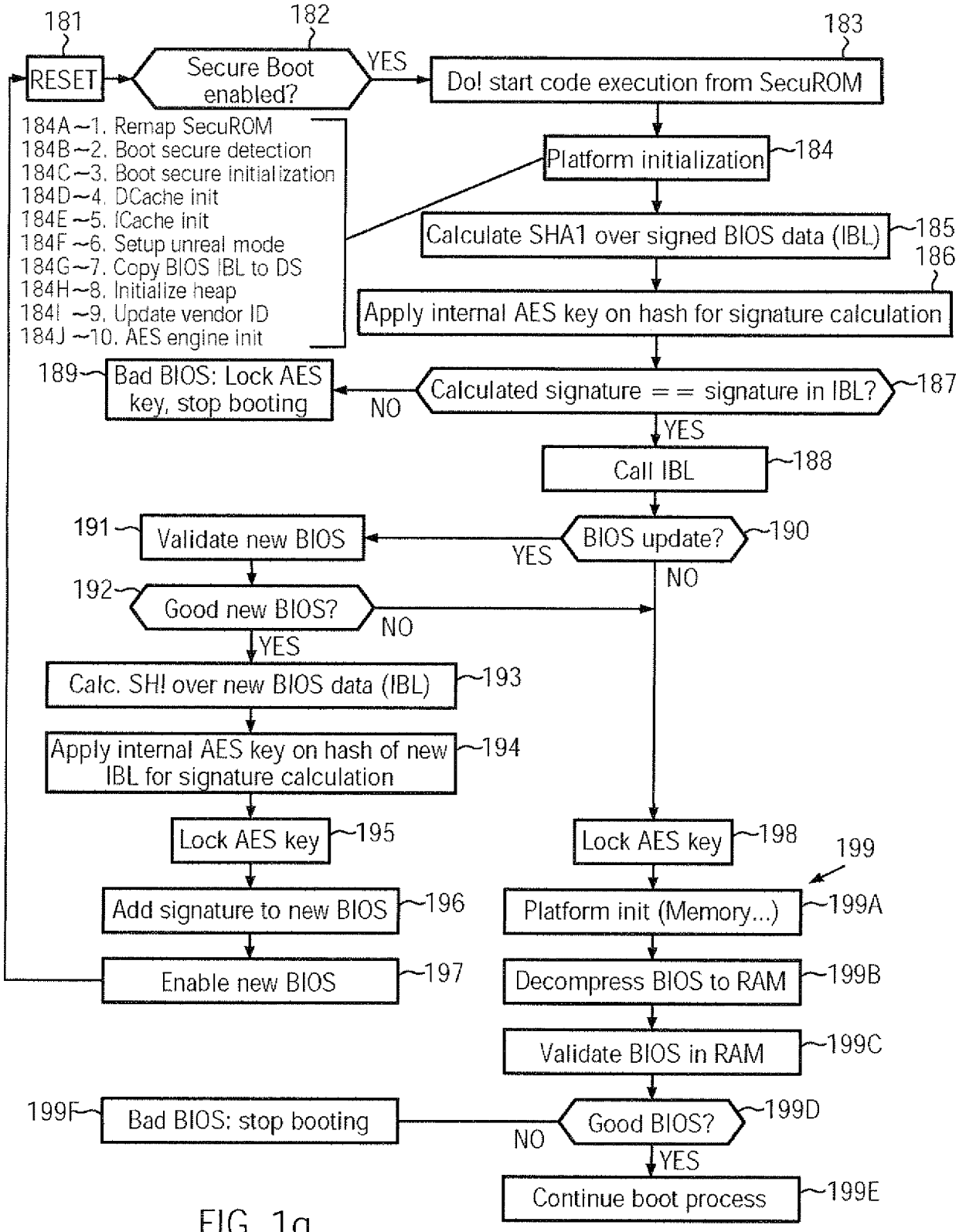

181
RESET
182
Secure Boot enabled?
YES
183
Do! start code execution from SecuROM
184A ~1. Remap SecuROM
184B ~2. Boot secure detection
184C ~3. Boot secure initialization
184D ~4. DCache init
184E ~5. ICache init
184F ~6. Setup unreal mode
184G ~7. Copy BIOS IBL to DS
184H ~8. Initialize heap
184I ~9. Update vendor ID
184J ~10. AES engine init
Platform initialization
184
Calculate SHA1 over signed BIOS data (IBL)
185
186
Apply internal AES key on hash for signature calculation
189
Bad BIOS: Lock AES key, stop booting
NO
Calculated signature == signature in IBL?
187
YES
Call IBL
188
191
Validate new BIOS
YES
BIOS update?
190
NO
192
Good new BIOS?
NO
YES
Calc. SHI over new BIOS data (IBL)
193
Apply internal AES key on hash of new IBL for signature calculation
194
Lock AES key
195
Lock AES key
198
199
Add signature to new BIOS
196
Platform init (Memory...)
199A
Enable new BIOS
197
Decompress BIOS to RAM
199B
Validate BIOS in RAM
199C
199F
Bad BIOS: stop booting
NO
Good BIOS?
199D
YES
Continue boot process
199E

FIG. 1g

DECLARATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or the below named inventors are the original, first and joint inventors (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **A COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION**, the Specification of which:

☒ is attached hereto.
☐ was filed on _____ as Application Serial No. _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose to the Patent and Trademark Office all information known to me to be material to patentability of the subject matter claimed in this application, as "materiality" is defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim priority benefits under Title 35, United States Code, § 119 and/or § 365 of any foreign application(s) for patent or inventor's certificate, PCT international application(s), and United States provisional application(s), listed below and have also identified below any foreign application for patent or inventor's certificate, PCT international application, or United States provisional application, having a filing date before that of the application on which priority is claimed:

PRIORITY APPLICATION(S)			**Priority Claimed**
10 2008 021 567.8	Germany	30 April 2008	Yes
(Number)	(Country)	(Date Filed)	Yes/No
(Number)	(Country)	(Date Filed)	Yes/No

I hereby claim the benefit under Title 35, United States Code, § 120 and/or § 365 of any United States application(s) and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose all information known to me to be material to patentability of the subject matter claimed in this application, as "materiality" is defined in Title 37, Code of Federal Regulations, § 1.56, which becomes available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status)
(Application Serial No.)	(Filing Date)	(Status)

I hereby direct that all correspondence and telephone calls be addressed to Customer No. 23,720.

I HEREBY DECLARE THAT ALL STATEMENTS MADE OF MY OWN KNOWLEDGE ARE TRUE AND THAT ALL STATEMENTS MADE ON INFORMATION AND BELIEF ARE BELIEVED TO BE TRUE; AND FURTHER THAT THESE STATEMENTS WERE MADE WITH THE KNOWLEDGE THAT WILLFUL FALSE STATEMENTS AND THE LIKE SO MADE ARE PUNISHABLE BY FINE OR IMPRISONMENT, OR BOTH, UNDER SECTION 1001 OF TITLE 18 OF THE UNITED STATES CODE AND THAT SUCH WILLFUL FALSE STATEMENTS MAY JEOPARDIZE THE VALIDITY OF THE APPLICATION OR ANY PATENT ISSUED THEREON.

Inventor's Full Name:	Michael GRELL	
Inventor's Signature:	Michael Grell	
Country of Citizenship:	Germany	Date:
Residence Address: (street, number, city, state, and/or country)	Calberlastr 12 01326 Dresden, Germany	
Post Office Address: (if different from above)		

Inventor's Full Name:	Ralf FINDEISEN	
Inventor's Signature:		
Country of Citizenship:	Germany	Date:
Residence Address: (street, number, city, state, and/or country)	Osterbergstr 7 01127 Dresden, Germany	
Post Office Address: (if different from above)		

Inventor's Full Name:	Frank SCHUECKE	
Inventor's Signature:	Frank Schuecke	
Country of Citizenship:	Germany	Date:
Residence Address: (street, number, city, state, and/or country)	Trachenberger Str 23 01129 Dresden, Germany	
Post Office Address: (if different from above)		

Filing Date: 01/19/09

Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 12/355,900

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	540
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	1	x$26		OR	x$52	52
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x$110			x$220	220
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			195			390	
			TOTAL			TOTAL	1362

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Confirmation No.: 7735 Group Art Unit: Unknown
Serial No.: 12/355,900	Examiner: Unknown
Filed: January 19, 2009	Att'y Docket: 2000.162700/DE0892
For: METAL CAP LAYER OF INCREASED ELECTRODE POTENTIAL FOR COPPER-BASED METAL REGIONS IN SEMICONDUCTOR DEVICES	Customer No.: 23720

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In compliance with the duty of disclosure under 37 C.F.R. § 1.56, it is respectfully requested that this Information Disclosure Statement be entered and the documents listed on attached Form PTO-1449 be considered by the Examiner and made of record. Copies of the listed foreign patent document and foreign official communication have been submitted herewith.

In accordance with 37 C.F.R §§ 1.97(g),(h), this Information Disclosure Statement is not to be construed as a representation that a search has been made, and is not to be construed to be an admission that the information cited is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

In accordance with 37 C.F.R § 1.97(e)(1), Applicants hereby certify that each item of information contained in this Information Disclosure Statement was cited in a communication

from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the present statement, as evidenced by the enclosed translation of an Official Communication from the German Patent Office.

The present Information Disclosure Statement is being filed prior to the receipt of a first Official Action reflecting an examination on the merits, and hence is believed to be timely filed in accordance with 37 C.F.R § 1.97(b). No fees are believed to be due in connection with the filing of this Information Disclosure Statement; however, should any fees under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to these materials, the Director is hereby authorized to deduct said fees from Williams, Morgan & Amerson, P.C., Deposit Account No. 50-0786/2000.162700.

Applicants respectfully request that the listed documents be made of record in the present case.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON
CUSTOMER NO. 23720

Date: January 22, 2009

/J. Mike Amerson/

J. Mike Amerson
Reg. No. 35,426
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4055
(713) 934-7011 (facsimile)

ATTORNEY FOR APPLICANTS

Form PTO-1449 (modified)	Atty. Docket No. 2000.162700/DE0892	Serial No. 12/355,900
List of Patents and Publications for Applicant's INFORMATION DISCLOSURE STATEMENT (Use several sheets if necessary)	**Applicant** Michael Grell, Ralf Findeisen and Frank Schuecke	
	Filing Date: January 19, 2009	**Group:** Unknown

U.S. Patent Documents	Foreign Patent Documents	Other Art
See Page 1	*See Page 1*	*See Page 1*

U.S. Patent Documents

Exam. Init.	Ref. Des.	Document Number	Date	Name	Class	Sub Class	Filing Date of App.
	A1						
	A2						
	A3						
	A4						
	A5						

Foreign Patent Documents

Exam. Init.	Ref. Des.	Document Number	Date	Country	Class	Sub Class	Translation Yes/No
	B1	WO 2006/086301 A1	8/17/06	PCT	G06F	12/02	Yes
	B2						
	B3						

Other Art (Including Author, Title, Date Pertinent Pages, Etc.)

Exam. Init.	Ref. Des.	Citation
	C1	Translation of Official Communication from German Patent Office for German Patent Application No. 10 2008 021 567.8-53 dated November 12, 2008.
	C2	
	C3	

EXAMINER:	DATE CONSIDERED:

EXAMINER: INITIAL IF REFERENCE CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED. INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

P46953

1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 August 2006 (17.08.2006)

PCT

(10) International Publication Number
WO 2006/086301 A1

(51) International Patent Classification:
G06F 12/02 (2006.01) *G06F 9/24* (2006.01)

(21) International Application Number:
PCT/US2006/004094

(22) International Filing Date: 3 February 2006 (03.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/053,081 7 February 2005 (07.02.2005) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 11/053,081 (CON)
Filed on 7 February 2005 (07.02.2005)

(71) Applicant *(for all designated States except US)*: **TRANSMETA CORPORATION** [US/US]; 3990 Freedom Circle, Santa Clara, CA 95054 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MORGAN, Andrew** [GB/US]; 18163 Mountain View Court, Los Gatos, CA 95033 (US). **LUDLOFF, Christian** [DE/US]; 560 N. 6th Street, #322, San Jose, CA 95112 (US). **ROZAS, Guillermo** [US/US]; 104 Magneson Terrace, Los Gatos, CA 95032 (US).

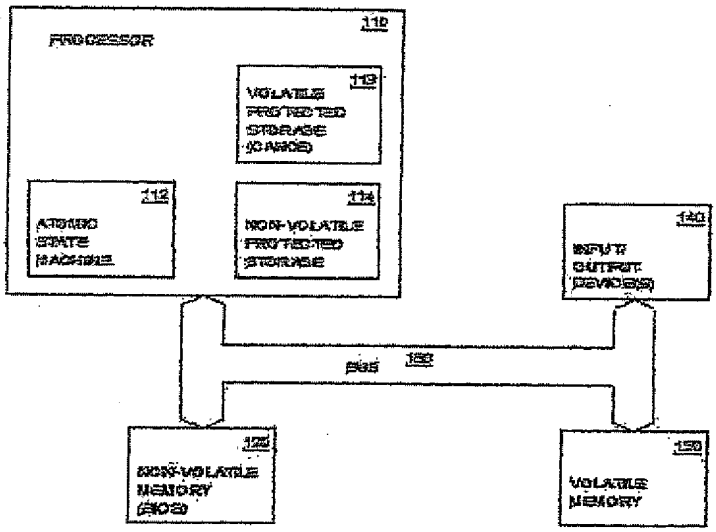
(74) Agent: **GALLENSON, Mavis, S.**; Ladas & Parry LLP, Suite 2100, 5670 Wilshire Boulevard, Los Angeles, CA 90036-5679 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US (patent), UZ, VC, VN, YU, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING A SECURE BOOT ARCHITECTURE



(57) Abstract: A system and method for providing a secure boot architecture, in accordance with one embodiment of the present invention, includes a processor having an atomic state machine and a physically protected storage area. The atomic state machine stores a state of the processor in a state save map upon a boot-mode event. The atomic state machine also authenticates an object of a Pre-BIOS Boot Vector Region (PBBVR) in response to the boot-mode event. The PBBVR may be stored in the physically protected storage area. The atomic state machine loads the PBBVR from the physically protected storage area into an overlay memory if the PBBVR is successfully authenticated. The processor executes the PBBVR from the overlay memory if the PBBVR is successfully authenticated. The atomic state machine may also receive a candidate PBBVR upgrade image, authenticate the candidate PBBVR upgrade image, and replace the current PBBVR with a new PBBVR contained in the candidate PBBVR upgrade image if the new PBBVR in the candidate PBBVR upgrade image is authenticated.

WO 2006/086301 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

SYSTEM AND METHOD FOR PROVIDING A SECURE BOOT ARCHITECTURE

BACKGROUND

[0001] The execution of blocks of instructions by a processor generally performs some operation. To a great extent all instructions sequences are valid from the perspective of the processor. The processor has no meaningful notion of a complete and/or valid program or function. Thus, if a block of instructions can be presented to a processor, they will generally be executed. Accordingly, instruction sequences containing so-called illegal instructions may reliably cause the processor to execute, fault or halt.

[0002] Hence, it is desirable to restrict the execution of code by a processor. One way to restrict execution is by authentication of the sequence of instructions. In the conventional art, one or more blocks of code may be authenticated to provide a secure computing environment. The authentication process establishes a block of code as a trusted sequence of instructions. However, the conventional authentication process relies upon the assumption that the given block of code from which another block of code's authentication depends upon can be trusted. The authentication process may be utilized to establish a chain of trust. However the process of chaining the authentication of multiple code blocks together still relies upon the assumption that a root block of code is trusted. Accordingly, a conventional secure computing architecture remains vulnerable as a result of the fact that the root block of code may not be trusted.

SUMMARY

[0003] Accordingly, embodiments of the present invention are directed toward a system having a secure boot architecture. In the secure boot architecture, a target instruction for a processor may be authenticated in a boot-mode such that all instructions executed on the processor can root their trust back to the processor implementation. Embodiments of the present invention may also provide a processor enforced boot-mode upgrade mechanism.

[0004] In one embodiment, a processor having a secure boot architecture includes an atomic state machine coupled to a physically protected storage area. The physically protected storage area stores a boot-mode object. The atomic state machine authenticates the boot-mode object before execution by a processor of a first target instruction. The atomic state machine may also receive a candidate boot-mode upgrade image, authenticate the candidate boot-mode upgrade image, and replace the current boot-mode object with a new boot-mode object contained in the candidate boot-mode upgrade image if the candidate boot-mode upgrade in the candidate boot-mode upgrade image is authenticated.

[0005] In another embodiment, a method for providing a secure boot architecture includes receiving a boot-mode event, authenticating a boot-mode object, and executing a first target instruction if the boot-mode object is authenticated. The method may further include receiving a candidate boot-mode upgrade image, authenticating the candidate boot-mode upgrade image and replacing the current boot-mode code with the new boot-mode code

in the candidate boot-mode upgrade image if the candidate boot-mode upgrade image is authenticated.

[0006] In yet another embodiment, a system for providing a secure boot architecture includes an atomic state machine coupled to a physically protected storage area. The atomic state machine stores a state of a processor in a state save map upon the occurrence of a boot-mode event. The atomic state machine also authenticates an object of a Pre-BIOS Boot Vector Region (PBBVR) in response the boot-mode event. The PBBVR may be stored in the physically protected storage area. The atomic state machine loads the PBBVR from the physically protected storage area into an overlay memory, if the PBBVR is successfully authenticated. The processor may then execute the PBBVR from the overlay memory, if the PBBVR is successfully authenticated.

This disclosure describes a system and method for providing a secure boot architecture, in accordance with one embodiment of the present invention, includes a processor having an atomic state machine and a physically protected storage area. The atomic state machine stores a state of the processor in a state save map upon a boot-mode event. The atomic state machine also authenticates an object of a Pre-BIOS Boot Vector Region (PBBVR) in response to the boot-mode event. The PBBVR may be stored in the physically protected storage area. The atomic state machine loads the PBBVR from the physically protected storage area into an overlay memory if the PBBVR is successfully authenticated. The processor executes the PBBVR from the overlay memory if the PBBVR is successfully authenticated. The atomic state machine may also receive a candidate PBBVR upgrade image, authenticate the candidate PBBVR upgrade image, and replace the current PBBVR with a new PBBVR contained in the candidate PBBVR upgrade image if the new PBBVR in the candidate PBBVR upgrade image is authenticated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments of the present invention are illustrated by way of example and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Figure 1 shows a block diagram of a system for establishing a secure boot architecture, in accordance with one embodiment of the present invention.

Figures 2A and 2B show a flow diagram of a method for establishing a secure boot architecture, in accordance with one embodiment of the present invention.

Figure 3 shows a format of a Pre-BIOS Boot Vector Region (PBBVR)) object, in accordance with one embodiment of the present invention.

Figure 4 shows a format of a physical memory and an overlay memory, in accordance with one embodiment of the present invention.

Figure 5 shows a flow diagram of a method for controlling the upgrade of the boot-mode code, in accordance with one embodiment of the present invention.

Figure 6 shows a format of a boot-mode upgrade object, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

[0008] Reference will now be made in detail to the embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with these embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it is understood that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present invention.

[0009] Embodiments of the present invention provide a secure boot architecture. A boot-mode, of the secure boot architecture, authenticates the target instruction for a processor such that all instructions executed on the processor can root their trust back to the processor implementation. Therefore, authentication is established before the basic input output system (BIOS) boot block. Embodiments of the present invention may also provide a mechanism by which authenticated boot-mode code may be upgraded without loss of trust.

[0010] Referring to Figure 1, a block diagram of a system for establishing a secure boot architecture, in accordance with one embodiment of the present invention, is shown. As

depicted in Figure 1, the secure boot architecture system includes a processor 110, one or more physical memory units 120, 130, one or more input/output devices 140 and the like. It is appreciated that the processor 110 referred to herein may be a general purpose processor, a dedicated controller or the like. The one or more physical memory units 120, 130 and the one or more input/output devices 140 may be communicatively coupled to the processor 110. In one implementation, the one or more physical memory units 120, 130 and the one or more input/output devices 140 may be communicatively coupled to the processor 110 by one or more buses 150.

[0011] The processor 110 may include an atomic state machine 112, a volatile physically protected storage area (e.g., cache) 113 and a non-volatile physically protected storage area 114. The atomic state machine 112 may implement a boot-mode and may optionally implement a boot-mode upgrade mechanism. The non-volatile physically protected storage area 114 may contain boot-mode code. In one implementation, the volatile 113 and non-volatile 114 physically protected storage areas may be integral parts of the processor 110 (e.g., fabricated on the processor die). In another implementation, the volatile 113 and non-volatile 114 physically protected storage areas may be separate from the processor 110. In one implementation, the non-volatile physically protected storage area 114 containing boot-mode code may be writeable non-volatile memory (e.g., flash memory or the like).

[0012] The system for establishing a secure boot architecture of Figure 1, will be further described herein in conjunction with Figures 2A and 2B. As depicted in Figures 2A and 2B, a flow diagram of a method for establishing a secure boot architecture, in accordance with one embodiment of the present invention, is shown.

[0013] Establishing a secure boot architecture may be initiated by receipt of a boot-mode entry-event, at 210, by the processor 110. The boot-mode entry-events may include events that have implications for the trustability of post-event code execution and/or benefit from the authentication gate provided by the boot-mode. The boot-mode entry-event may include one or more events such as a reset, a partial reset, one or more interrupts from an interrupt controller, one or more interrupts from a shutdown state (e.g., for multiprocessor systems). In one implementation, the boot-mode entry-events in a legacy system (e.g., x86) may include:

ENTRY_ID	BOOT-MODE ENTRY-EVENT
0	RESET
1	INIT
2	APIC_IPI_INIT
3	APIC_IPI_INIT_W_VECTOR
4	APIC_INI_SMI
5	APIC_INI_NMI
6	RESET_FROM_SHUTDOWN

7	INIT_FROM_SHUTDOWN
8	SMI_FROM_SHUTDOWN
9	NMI_FROM_SHUTDOWN

The boot-mode entry-event may be a non-maskable interrupt. Once in boot-mode, the processor will defer delivery of non-maskable interrupts, including the system management interrupt (SMI), until boot-mode is exited.

[0014] At 215, receipt of a boot-mode entry-event may cause the processor 110 to modify its state. In one implementation, for the RESET boot-mode entry-event, the code segment register (e.g., cs_base), instruction pointer register (e.g., eip) and system management base register (e.g., sm_base) of the processor 110 may be modified to the following values:

cs_base = 0xffff0000

eip = 0x0000fff0

sm-base = 0x00030000

It is appreciated that the code segment register and the instruction pointer register point to the BIOS boot block. In one implementation, entering boot-mode cause the current state (e.g., legacy reset) to be written to the state save map at the end of an extended overlay memory.

[0015] At optional process 217, the atomic state machine 112 may determine if the overlay memory is initialized. It is appreciated that reinitialization of the overlay memory may be avoided for one or more boot-mode entry-events. Accordingly, if the overlay memory is currently initialized the method for establishing a secure boot architecture may proceed at process 227. If the overlay memory is not currently initialized the method may proceed at process 220.

[0016] At 220, the atomic state machine 112 authenticates the boot-mode code stored in the non-volatile physically protected storage area 114. The authentication of the boot-mode code may be implementation specific. In one implementation, authentication of the boot-mode code may be accomplished utilizing a simple checksum algorithm. In another implementation, authentication of the boot-mode code may be accomplished utilizing a complicated digital signature verification process. The sophistication of the authentication process may be a function of the physical security of the non-volatile physically protected storage area 114 used to hold the boot-mode code. Accordingly, the more tightly coupled the physically protected storage area 114 is to the processor 110 the lesser degree of authentication may be needed.

[0017] At 225, the overlay memory may be initialized and the boot-mode code may be mapped into the overlay memory. The overlay memory may be constructed by combining the authenticated boot-mode code and reserved boot-mode data area. In a modified x86 implementation, the boot-mode code is a Pre-BIOS Boot Vector Region

(PBBVR) object. In such an implementation, the overlay memory is mapped to a portion of the physical address space obscuring a portion of the regular physical memory (e.g., RAM 130) while executing in boot-mode. In one implementation this overlay memory is maintained as processor internal memory 113 (e.g., a processor internal cache array). In one implementation, this overlay memory is a processor protected fraction of main memory 130.

[0018] The modified state of the processor 110 may be stored in a state save map (SSM), at 227. In a modified x86 implementation, entering boot-mode as a result of the RESET event, causes the current state (e.g., legacy reset) to be written to the state save map at the end of the extended overlay memory.

[0019] Referring now to Figure 3, a format of a Pre-BIOS Boot Vector Region (PBBVR)) object, in accordance with one embodiment of the present invention, is shown. As depicted in Figure 3, the PBBVR may contain a header 310 and a combined code and data payload 320. The length of the PBBVR may be an integer number of contiguous pages. The header 310 may have a defined layout and includes PBBVR configuration and authentication data that covers the entire PBBVR object and its run-time environment. The combined code and data payload 320 may contain any desired code and data for execution in boot-mode.

[0020] Referring now to Figure 4, a format of a physical memory 405 and an overlay memory 410, in accordance with one embodiment of the present invention, is shown. As depicted in Figure 4, the overlay memory 410 may be mapped to a predetermined

physical memory 405 location. The overlay memory 410 may be mapped such that it ends on a predetermined boundary (e.g., 1MiB) 415. In a modified x86 implementation, the overlay memory 410 is mapped to the physical address surrounding 0x00100000 (e.g., 1MB). In the context of such an implementation, it is appreciated that the overlay appears to be regular volatile memory (e.g., RAM 130) closer to the core than the APIC memory, but it is not visible to direct memory access (DMA) from input/output devices 140. It is also appreciated that it is not visible to code executing outside boot-mode.

[0021] Referring again to Figures 1, 2A and 2B, once the current state of the processor 110 is stored in the state save map and the boot-mode code has been authenticated, the state of the processor 100 may be changed by the atomic state machine 112 to initiate run time execution of the boot-mode code from the overlay memory, at 230. In a modified x86 implementation, boot-mode is entered with a register state most like that of System Management Mode (SMM), e.g., a 16-bit code segment, and flat data segments. However, the instruction pointer is set as follows:

```
cs_base = 0x000f0000
    eip = 0x0000fff0
```

Accordingly, code execution (e.g., following a RESET event) will begin at a location different than where the BIOS boot vector is located.

[0022] The reason for processor entry into boot-mode, may be captured in some machine state register. In a modified x86 implementation, one or more parameters of the event that causes entry into the boot-mode may also be captured in a boot-mode machine specific register (MSR):

MSR_TMx86_BOOT_MODE_ENTRY_STATE = 0x80868077

The boot-mode specific MSR performs as follows:

```
RDMSR [MSR_TMx86_BOOT_MODE_ENTRY_STATE] :
    If (NOT executing_in_boot_mode) {
        #GP(0) ;
    } else {
        Fill eax and edx as per the following 'C' union ;
        Typedef union tsb_msr_info_u {
            struct {
                uint32 eax_lo ;
                uint32 edx_hi ;
            } flat ;
            struct {
                unsigned entry_event : 5 ;
                unsigned _rsvl : 6;
```

```
                unsigned data_preserved : 1 ;
                unsigned data_page_extension_count : 8 ;
                unsigned _rsv2 : 12 ;
                unsigned _rsv3 : 32 ;
            } bits ;
        } tsb_msr_info_t ;
    }
```

The value tsb_msr_info_t.bits.entry_event bitfield contains the entry_id as described above. Accordingly, a code indicative of the event that caused the boot-mode entry is returned. The tsb_msr_info_t.bits.data_page_extension_count contains the number of additional 4KiB pages provided in boot-mode. The extended overlay size returned is the actually additional memory allocated by the processor 110, not the pages requested in the header of the PBBVR. The tsb_msr_info_t.bits.data_preserved bit indicates whether the entry into boot-mode preserved the contents of the overlay memory from a previous invocation (a value of '0' indicates that the boot-mode overlay has been freshly instantiated, and a value of '1' indicates that the overlay contains data preserved since the last exit from boot-mode).

[0023] In one implementation, after having authenticated the PBBVR, the processor extends the overlay to include one or more extra data pages (e.g., a non-zero multiple of 4 KiB). The size of the overlay memory may be defined in the header of the PBBVR. In one implementation, the PBBVR may be copied to an overlay memory which is up to 192 KiB. The extended overlay memory may be initialized to 0xff.

[0024] It is appreciated by those skilled in the art how code execution in SMM can enter protected mode. Protected mode may enable paging, exception and interrupt handling and the like, without leaving SMM. It is furthermore appreciated, that such protected mode features are shared by boot-mode. Accordingly, operations that can be performed from boot-mode range from: the trivial, such as simply executing the RSM instruction; to imitating a legacy x86 (e.g., with no boot-mode support), to the extensive, such as pre-BIOS execution of code to fully validate the BIOS with peripheral based recovery of the BIOS in the event of BIOS corruption; or to implement a non-legacy boot sequence that could initialize an SMM handler or operating system hidden in a locked T-segment. Thus, through modification of the boot-mode SSM prior to the PBBVR code executing the RSM instruction, arbitrary machine states and modes can be realized.

[0025] At 235, the combined code and data payload of the boot-mode object may be executed from the overlay memory. In one implementation, the code may authenticate the BIOS boot block. At 240, the boot-mode may be exited. In one implementation, the PBBVR code may exit by executing a resume from system management mode (RSM) instruction. It is appreciated that, following a RESET boot-mode entry-event, the cs_base, eip and sm_base values stored in the boot-mode state save map (SSM) are those of the legacy reset vector. It is further appreciated that if the code present at the overlay boot-mode entry vector (e.g., 0xf000:fff0) contain a single RSM instruction, then the modified processor will immediately exit boot-mode and initiate a legacy boot, chaining to the BIOS.

[0026] If the PBBVR is authenticated, the BIOS code may be executed at 250. At 265-270, operation of the processor may continue with execution of one or more other blocks of code. One or more of the other blocks of code may be authenticated, at 255-260, against the authenticated BIOS code which roots its authentication back to the PBBVR boot-mode code.

[0027] If the PBBVR is not authenticated, operation of the processor may be halted at 290. Optionally, prior to halting operation of the processor, a recovery version of the PBBVR may be run-time authenticated by the processor, at 275. At 280, the recovery version of the PBBVR may be loaded from the physically protected storage area 114 into the predetermined overlay memory, if the recovery version of the PBBVR is successfully authenticated. If the recovery version of the PBBVR is authenticated, run-time execution of the processor may continue with process 230 as described above. If the recovery version of the PBBVR is not authenticated, the operation of the processor may be halted at 290. Thus, the processor may refuse to execute further if neither the primary boot-mode code nor recovery boot-mode code are authenticated.

[0028] Accordingly, embodiments of the present invention provide a secure boot architecture. The boot-mode of the secure boot architecture advantageously authenticates the target instruction for a processor such that all instructions executed on the processor can root their trust back to the processor implementation. Hence, authentication is established before the basic input output system (BIOS) boot block is executed.

[0029] The processor implementation of the above described boot-mode may be complimented by an additional processor enforced upgrade mechanism. Referring now to Figure 5, a flow diagram of a method for controlling the upgrade of the boot-mode code, in accordance with one embodiment of the present invention, is shown. The method for controlling the upgrade of boot-mode code will be described with reference to the system of Figure 1.

[0030] A system having a secure boot architecture may be upgraded if at least one pre-existing correctly formatted and authenticated boot-mode object (e.g., PBBVR) is present in the physically protected storage area 114. The boot-mode code upgrade mechanism may utilizes a private/public key authentication algorithm. The process for upgrading the boot-mode code in a system begins with receipt of a boot-mode upgrade image, at 510. In one implementation, a platform manufacturer generates the signed PBBVR upgrade object, which is passed to the system via an input/output device 140.

[0031] Referring now to Figure 6, a format of a boot-mode upgrade object (e.g., signed PBBVR upgrade image), in accordance with one embodiment of the present invention, is shown. As depicted in Figure 6, the object includes a digital signature (e.g., DSA signature) 610, padding data 620, a new boot-mode code (e.g., new PBBVR) object 630 and an upgrade image header 640. The upgrade image header 640 includes upgrade image size and version-matching information. The new PBBVR 630 contains authentication information to be used by the upgraded system. The new PBBVR 630 is not used as part of

the upgrade authentication for the present upgrade. It is the combination of the running PBBVR, as it exists in the non-volatile physically protected storage area 114, the contents of the upgrade image header 640 and digital signature 610 that is utilized to authenticate the boot-mode upgrade image.

[0032] At 520, the received boot-mode upgrade image (e.g., candidate upgrade image) may be cached in the volatile physically protected storage area 113. In a modified x86 implementation, upon receipt of the boot-mode upgrade image, x86 code executing in any privileged mode (e.g., boot-mode, system management mode, real mode, protected mode or the like) initializes the values of the ECX, EAX and EDX registers as follows:

ECX = MSR_TMx86_PBBVR_UPGRADE = 0x80868008

EAX = linear address of base of signed PBBVR image

EDX = number of DWORDS in signed PBBVR image

Given that the legacy code has arranged for the signed PBBVR upgrade image to be based at the value held in EAX and that it is EDX DWORDS in length, the legacy code executes a WRMSR instruction. The WRMSR machine specific operation causes the current processor to cache a copy of the candidate upgrade image. The cached copy of the candidate upgrade image should be protected from direct memory access and snoop requests from peer processors.

[0033] At 530, the public key in the header of the current boot-mode object is used to validate the digital signature 610 in the upgrade image header of the candidate boot-mode upgrade image. In one implementation, the WRMSR instruction re-reads the header of the current PBBVR from the non-volatile physically protected storage area 114 to extract a public DSA key. The WRMSR instruction also validates the DSA signature of the received candidate PBBVR upgrade image with respect to this public DSA key. If the candidate upgrade image fails this authentication, completion of the WRMSR machine specific operation may generate a status report via RDMSR (e.g., 0x80868000).

[0034] At 535, additional validation of the candidate boot-mode upgrade image may be performed. In one implementation, the WRMSR instruction may also validate the candidate PBBVR upgrade image against access control information, such as matching 'current' fields to permitted ranges specified in the incoming candidate PBBVR upgrade image. If the candidate upgrade image fails this access control test, completion of the WRMSR machine specific operation may generate a status report via RDMSR (e.g., 0x80868000).

[0035] If the authentication and access control checks succeed, the processor 110 may overwrite the current boot-mode object in the physically protected storage area 114, at 540. At 545, the new boot-mode object written to the physically protected storage area 114 may then be verified. In one implementation, if the current primary PBBVR in the physically protected storage area 114 can be verified to be valid, the processor 110 may first

overwrite the current recovery PBBVR. The processor may then verify that the new recovery PBBVR was written to the physically protected storage area 114 correctly. The processor may then repeat the procedure to write the upgrade PBBVR as the new primary PBBVR in the physically protected storage area 114.

[0036] In an alternative implementation, if the primary PBBVR in the physically protected storage area 114 is found to be invalid, the processor may overwrite the invalid primary PBBVR with the new PBBVR and verify that the new primary PBBVR was correctly written to the physically protected storage area 114. The processor may then overwrite the recovery PBBVR with the new PBBVR and verify that the new recovery PBBVR was also correctly written to the physically protected storage area 114. Hence, there will exist at least one uncorrupted PBBVR image in the physically protected storage area 114, even in the face of events such as power failure, thermal event and the like that may cause corruption of the PBBVR upgrade process.

[0037] Accordingly, embodiments of the present invention provide a mechanism by which authenticated boot-mode code may be upgraded. It is appreciated that the boot-mode code may advantageously be upgraded in a running system without loss of trust.

[0038] The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not

intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

CLAIMS

What is claimed is:

1. A processor having a secure boot architecture comprising:

a physically protected storage area for storing a boot-mode object; and

an atomic state machine, coupled to said physically protected storage area, for authenticating said boot-mode object before execution of a first target instruction.

2. The processor of Claim 1, wherein said boot-mode object comprises a header portion and a combined code and data payload portion.

3. The processor of Claim 2, wherein said header portion comprises a defined memory size.

4. The processor of Claim 3, wherein said header comprises configuration and authentication data.

5. The processor of Claim 1, wherein said atomic state machine is operable to:

receive a candidate boot-mode upgrade image;

authenticate said candidate boot-mode upgrade image; and

replace said boot-mode object with a new boot-mode object in said candidate boot-mode upgrade image if said candidate boot-mode upgrade image is authenticated.

6. A method for providing a secure boot architecture for a computer system having a processor comprising:

receiving a boot-mode event;

authenticating a boot-mode object; and

executing a first target instruction if said boot-mode object is authenticated.

7. The method according to Claim 6, further comprising:

storing an initialization state;

executing a first instruction in said boot-mode object after storing said initialization state; and

restoring said initialization state after executing said first instruction.

8. The method according to Claim 6, further comprising:

authenticating a recovery boot-mode object if said boot-mode object is not authenticated;

executing said first instruction if said recovery boot-mode object is authenticated; and

halting execution if said recovery boot-mode object is not authenticated.

9. The method according to Claim 6, wherein said authenticating said boot-mode object comprises a digital signature verification process.

10. The method according to Claim 6, wherein said authenticating said boot-mode object comprises a checksum verification process.

11. The method according to Claim 6, wherein said boot-mode event comprises a non-maskable interrupt.

12. The method according to Claim 6, wherein said boot-mode object comprises a header having a defined layout.

13. The method according to Claim 12, wherein said header comprises configuration and authentication data.

14. The method according to Claim 6, further comprising storing a parameter of said boot-mode event in a boot-mode specific machine state register.

15. The method according to Claim 6, further comprising:

receiving a candidate boot-mode upgrade image;

authenticating said candidate boot-mode upgrade image; and

replacing said boot-mode object with a new boot-mode object of said candidate boot-mode upgrade image if said candidate boot-mode upgrade image is authenticated.

16. The method according to Claim 15, wherein authenticating said candidate boot-mode upgrade image comprises validating a digital signature of said candidate boot-mode upgrade image with respect to a public key of said boot-mode code.

17. A system for providing a secure boot architecture comprising:

a physically protected storage area for storing a primary boot-mode object;

an atomic state machine for;

storing a state of a processor in a state save map upon receipt of a boot-mode event;

authenticating an object of said primary primary boot-mode object upon receipt of said boot-mode event; and

loading said primary primary boot-mode object from said physically protected storage area into an overlay memory if said primary PBBVR is successfully authenticated; and

said processor for executing said primary primary boot-mode object from said overlay memory if said primary primary boot-mode object is successfully authenticated.

18. The system according to Claim 17, wherein said primary boot-mode object comprises a primary Pre-BIOS Boot Vector Region (PBBVR).

19. The system according to Claim 18, said atomic state machine for further restoring said state of said processor from said state save map after executing said primary PBBVR.

20. The system according to Claim 17, wherein:

said physically protected storage area is for further storing a recovery primary boot-mode object;

said atomic state machine is for further:

authenticating an object of said recovery boot-mode object if said primary boot-mode object is not successfully authenticated;

loading said recovery boot-mode object from said physically protected storage area into said overlay memory if said recovery boot-mode object is successfully authenticated; and

restoring said state of said processor from said state save map after executing said recovery boot-mode object; and

halting execution by said processor if said recover boot-mode object is not successfully authenticated; and

said processor is for executing said recovery boot-mode object from said overlay memory if said recovery boot-mode object is successfully authenticated.

21. The system according to Claim 20, wherein said recovery boot-mode object comprises a recovery PBBVR.

22. The system according to Claim 17, wherein restoring said state of said processor causes execution by said processor to jump to a BIOS boot block.

23. The system according to Claim 19, wherein said primary PBBVR comprises a header and a combined code and data payload.

24. The system according to Claim 23, wherein said primary PBBVR comprises an integer number of contiguous pages.

25. The system according to Claim 23, wherein said primary PBBVR comprises processor configuration and authentication data.

26. The system according to Claim 17, wherein said overlay memory is mapped to a predetermined physical memory location.

27. The system according to Claim 17, wherein said overlay memory appears to be regular memory.

28. The system according to Claim 17, wherein said overlay memory is not visible to direct memory access by an input/output device.

29. The system according to Claim 17, wherein said overlay memory is not visible to code executing outside boot-mode.

30. The system according to Claim 17, wherein said state save map is stored at the end of said overlay memory.

31. The system according to Claim 17, further comprising a boot-mode specific machine state register for capturing a parameter of said boot-mode event.

32. The system according to Claim 18, said atomic state machine for further:

receiving a candidate PBBVR upgrade image;

authenticating said candidate PBBVR upgrade image; and

replacing said primary PBBVR and said recovery PBBVR with a new PBBVR of said candidate PBBVR upgrade image if said candidate PBBVR upgrade image is authenticated.

33. The system according to Claim 18, wherein authenticating said candidate PBBVR upgrade image comprises validating a digital signature of said candidate boot-mode upgrade image with respect to a public key of said primary PBBVR or said recovery PBBVR.

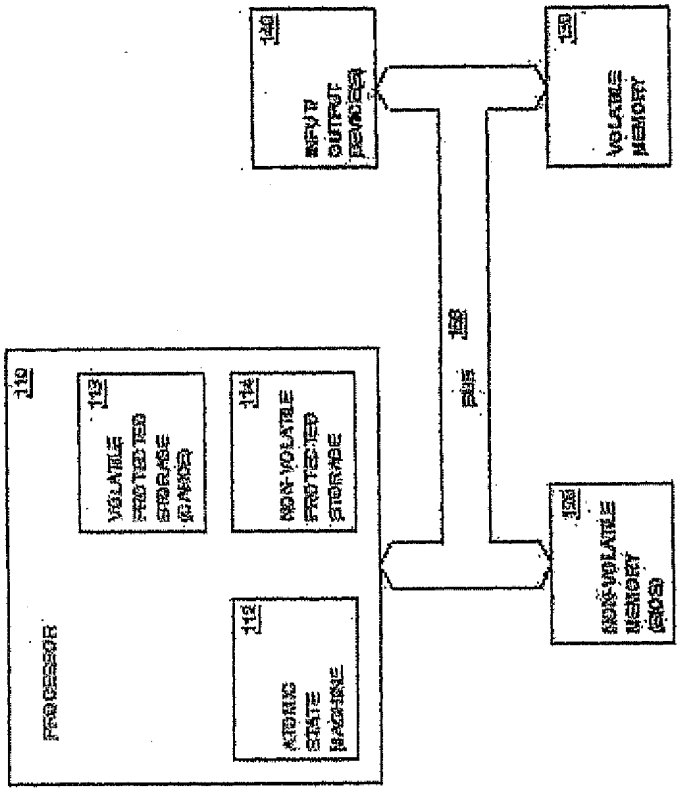

110
PROCESSOR
112
ATOMIC STATE MACHINE
114
NON-VOLATILE PROTECTED STORAGE
116
VOLATILE PROTECTED STORAGE (CACHE)
118
BUS
120
INPUT / OUTPUT DEVICES
130
VOLATILE MEMORY
150
NON-VOLATILE MEMORY (DISK)

FIGURE 1

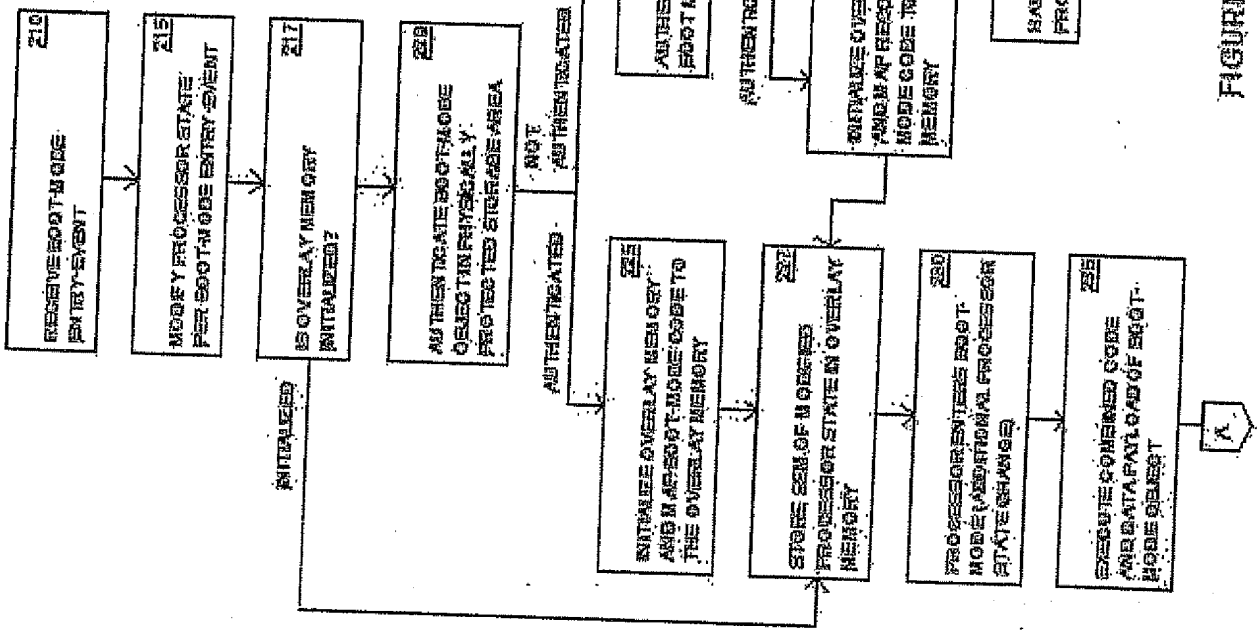

210
RESERVE BOOT MODE ENTRY EVENT
215
MODIFY PROCESSOR STATE FOR BOOT MODE ENTRY EVENT
217
IS OVERLAY MEMORY INITIALIZED?
220
AUTHENTICATE BOOT MODE OBJECTS IN PHYSICALLY PROTECTED STORAGE AREA
NOT AUTHENTICATED
AUTHENTICATED
INITIALIZED
225
275
AUTHENTICATE RECOVERY BOOT MODE OBJECT
NOT AUTHENTICATED
AUTHENTICATED
INITIALIZE OVERLAY MEMORY AND M ARESET-MODE CODE TO THE OVERLAY MEMORY
230
INITIALIZE OVERLAY MEMORY AND M RECOVERY BOOT MODE CODE TO THE OVERLAY MEMORY
235
SALT EXECUTION OF PROCESSOR
232
STORE SEED OF M OBSCURED PROCESSOR STATE IN OVERLAY MEMORY
240
PROCESSOR ENTERS BOOT MODE (ADDITIONAL PROCESSOR STATE CHANGES)
245
EXECUTE CONFINED CODE AND DATA FAIL LOAD OF BOOT MODE OBJECT
A

FIGURE 2A

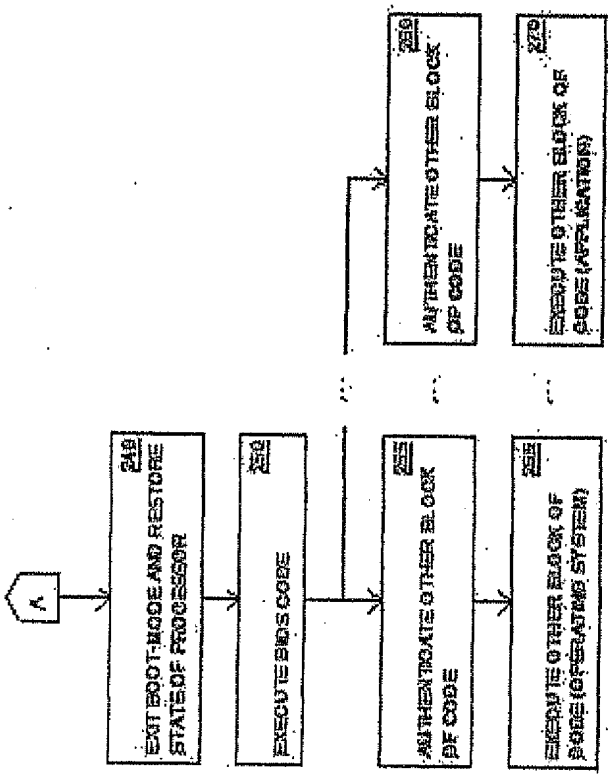


FIGURE 2B

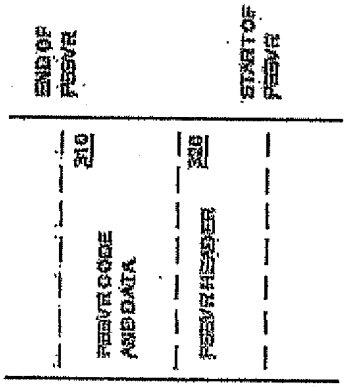


FIGURE 3

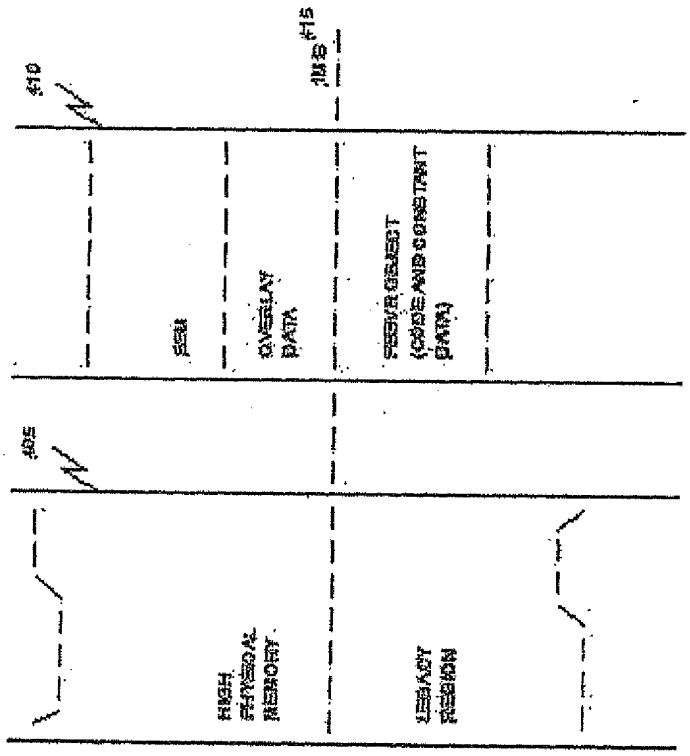

410
415
405
HIGH PHYSICAL MEMORY
SSA
OVERLAY DATA
RESERVED (CODE AND CONSTANT DATA)
LEGACY REGION

FIGURE 4

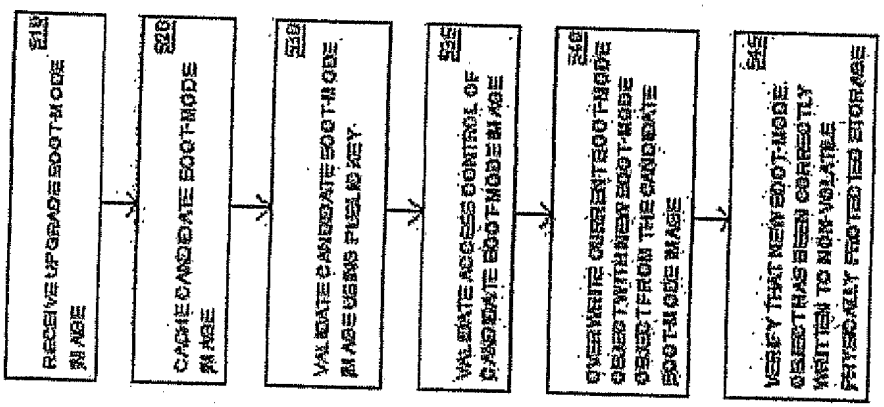

RECEIVE UPGRADE BOOT-MODE IMAGE
CACHE CANDIDATE BOOT-MODE IMAGE
VALIDATE CANDIDATE BOOT-MODE IMAGE USING PUBLIC KEY
VALIDATE ACCESS CONTROL OF CANDIDATE BOOT-MODE IMAGE
OVERWRITE CURRENT BOOT-MODE OBJECT WITH NEW BOOT-MODE OBJECT FROM THE CANDIDATE BOOT-MODE IMAGE
VERIFY THAT NEW BOOT-MODE OBJECT HAS BEEN CORRECTLY WRITTEN TO NON-VOLATILE PHYSICALLY PROTECTED STORAGE

FIGURE 5

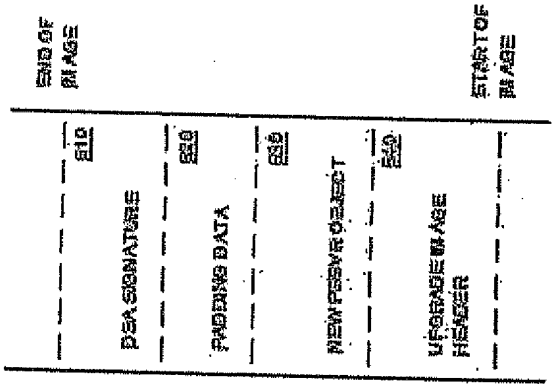

END OF IMAGE
810
DSA SIGNATURE
820
PADDING DATA
830
NEW FSSWR OBJECT
840
UPGRADE IMAGE HEADER
START OF IMAGE

FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2006/004094

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/02(2006.01)i, G06F 9/24(2006.01)i

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)

IPC8 : the entire class

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

Korean Patents and applications for inventions since 1975
Utility models and applications for Utility Models since 1975
Japanese Utility Models and application for Utility Models since 1975

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

eKIPASS(KIPO internal) , "boot", "authenticate"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,401,208 B2 (DAVIS, DEREK L. et al.) 4 June 2002 see column 1, lines 5 - 60.	1 - 33
A	US 6,356,529 B1 (RONY ZAROM) 12 March 2002 see the abstract	1 - 33

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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
16 JUNE 2006 (16.06.2006)	**19 JUNE 2006 (19.06.2006)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea	LEE, Young Su
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-8176

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2006/004094

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 06401208 B2	04.06.2002	US20020004905A1	10.01.2002
US 06356529 B1	12.03.2002	AU200064669A1	13.03.2001
		AU200064669A5	13.03.2001
		EP01203299A1	08.05.2002
		EP1203299A1	08.05.2002
		EP1203299A4	29.06.2005
		IL148054A0	12.09.2002
		US6356529BA	12.03.2002
		WO0113246A1	22.02.2001
		WO200113246A1	22.02.2001

Electronic Acknowledgement Receipt

EFS ID:	4656635
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	23720
Filer:	J. Mike Amerson/Mary Paul
Filer Authorized By:	J. Mike Amerson
Attorney Docket Number:	2000.162700/DE0892
Receipt Date:	22-JAN-2009
Filing Date:	
Time Stamp:	14:02:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	Information_Disclosure_Statement.pdf	200919 bdd51682777628706ff12a8eb1904b9366e635c4	no	3

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WO2006086301A1.pdf	981549 ba3ad228edff33e9bc224aba0d0adac8926d2f07	no	37
Warnings:					
Information:					
3	NPL Documents	German_Office_Action_Translation.pdf	273064 a14750697d2e474e1e53e8c0bc1dbee95fa37afc	no	8
Warnings:					
Information:					
			Total Files Size (in bytes):	1455532	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

OIPE IAP67
JAN 26 2009
PATENT & TRADEMARK OFFICE

IPW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Confirmation No.: 7735 Group Art Unit: Unknown
Serial No.: 12/355,900	Examiner: Unknown
Filed: January 19, 2009	Att'y Docket: 2000.162700/DE0892
For: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION	Customer No.: 23720

SUBMISSION OF PRIORITY DOCUMENT

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited with the United States Postal Service with sufficient postage as "FIRST CLASS MAIL" addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, this 21st day of January, 2009.

Mary Saul
Signature

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted for filing herewith is the certified copy of the priority document – German Patent Application No. 10 2008 021 567.8 filed on April 30, 2008.

If any fees under 37 C.F.R. §§ 1.16 to 1.21 are required for any reason relating to the enclosed materials, the Director is authorized to deduct said fees from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.162700.

Please date stamp and return the accompanying postcard to evidence receipt of this document.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON
CUSTOMER NO. 23720

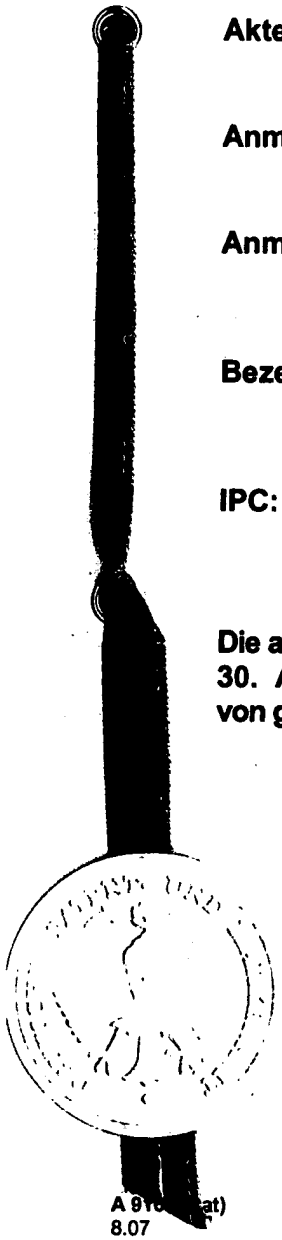
Date: January 20, 2009

J. Mike Amerson
Reg. No. 35,426
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4055
(713) 934-7011 (facsimile)

ATTORNEY FOR APPLICANTS

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung
DE 10 2008 021 567.8
über die Einreichung einer Patentanmeldung



Aktenzeichen:	10 2008 021 567.8
Anmeldetag:	30. April 2008
Anmelder/Inhaber:	ADVANCED MICRO DEVICES, INC., Sunnyvale, Calif./US
Bezeichnung:	A computer system comprising a secure boot mechanism on the basis of symmetric key encryption
IPC:	G 06 F 9/445, G 06 F 21/22

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der Teile der am 30. April 2008 eingereichten Unterlagen dieser Patentanmeldung unabhängig von gegebenenfalls durch das Kopierverfahren bedingten Farbabweichungen.

München, den 20. August 2008
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Dreer

A 9[illegible]at)
8.07

GRÜNECKER KINKELDEY STOCKMAIR & SCHWANHÄUSSER

ANWALTSSOZIETÄT

NEUE ADRESSE / NEW ADDRESS
LEOPOLDSTR. 4, D-80802 MÜNCHEN

GKS & S LEOPOLDSTRASSE 4 D-80802 MÜNCHEN GERMANY

RECHTSANWÄLTE
LAWYERS

MÜNCHEN
DR. HELMUT EICHMANN
GERHARD BARTH
DR. ULRICH BLUMENRÖDER, LL.M.
CHRISTA NIKLAS-FALTER
DR. MAXIMILIAN KINKELDEY, LL.M.
DR. KARSTEN BRANDT
ANJA FRANKE, LL.M.
UTE STEPHANI
DR. BERND ALLEKOTTE, LL.M.
DR. ELVIRA BERTRAM, LL.M.
KARIN LOCHNER
BABETT ERTLE
CHRISTINE NEUHIERL
SABINE PRÜCKNER
CORNELIA SCHMITT
PETRA LÜBBE
SONJA SCHÄFFLER
DR. HOLGER GAUSS
DR. NICOLÁS SCHMITZ
MARINA SCHLUMBERGER
KIRSTEN DRÖGE

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS

MÜNCHEN
DR. HERMANN KINKELDEY
PETER H. JAKOB
HANS HILGERS
ANNELIE EHNOLD
THOMAS SCHUSTER
DR. KLARA GOLDBACH
MARTIN AUFENANGER
GOTTFRIED KLITZSCH
DR. HEIKE VOGELSANG-WENKE
REINHARD KNAUER
DIETMAR KUHL
DR. FRANZ-JOSEF ZIMMER
BETTINA K. REICHELT
DR. ANTON K. PFAU
DR. UDO WEIGELT
RAINER BERTRAM
JENS KOCH, M.S. (U of PA) M.S.
BERND ROTHAEMEL
THOMAS W. LAUBENTHAL
DR. ANDREAS KAYSER
DR. JENS HAMMER

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS

DR. THOMAS EICKELKAMP
DR. CARLO TORTI*
DR. PETER MILTÉNYI
DR. MORITZ HÖFFE
GERO MAATZ-JANSEN
MICHAEL HEISE
CHRISTIAN MEISINGER
DR. MARTIN AHR
FELIX HERMANN
DR. WOLFGANG NEUBECK

BERLIN
DR. PATRICK ERK, M.S. (MIT)
DR. SVENJA SETHMANN

KÖLN
DR. MARTIN DROPMANN

DR. WILFRIED STOCKMAIR
(-1996)

*EUROPEAN PATENT ATTORNEY

IHR ZEICHEN / YOUR REF.

UNSER ZEICHEN / OUR REF.
P46953AP053jdc

DATUM / DATE
30.04.2008

Applicant: ADVANCED MICRO DEVICES, INC.
One AMD Place, Mail Stop 68,
Sunnyvale, CA 94088-3453
USA

A COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

GRÜNECKER KINKELDEY
STOCKMAIR & SCHWANHÄUSSER
LEOPOLDSTRASSE 4
D-80802 MÜNCHEN
GERMANY

TEL. +49 89 21 23 50
FAX +49 89 22 02 87
FAX +49 89 21 86 92 93
http://www.grunecker.de
e-mail: info@grunecker.de

Deutsche Bank München
Konto/Account: 175 1734
BLZ/Bank code: 700 700 10
SWIFT/BIC-code: DEUTDEMM
IBAN: DE47 7007 0010 0175 1734 00

A COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

FIELD OF THE PRESENT DISCLOSURE

The present disclosure generally relates to the field of computer systems of enhanced integrity and corresponding mechanisms implemented therein, which may enable the provision of enhanced security standards requiring a secure boot mechanism.

DESCRIPTION OF THE RELATED ART

The widespread use of computer systems has led to a significant increase of information processing on the basis of electronic computer systems, thereby involving the creation, distribution and processing of very large amounts of digital data. With the increasing capabilities of computer systems in view of data storage capacity and increased processing speed the reproduction of large data sets, such as audio data, movies, and the like, has become available for an increasing number of persons and is frequently practised despite any protective rights, which may be associated with many of the data provided in electronic form. Thus, significant economic damage may be created by the illegal copying, storage and redistribution of electronic data. Furthermore, the distribution of application programmes over widespread networks, such as the internet, may also provide the possibility of distributing malicious software applications, which may in turn be used for manipulating data and/or tampering with the configuration of a respective computer platform. For example, significant damage may be created in private environments, and in particular in the industry, by introducing software applications which may, for instance, manipulate software files such as stored data, communicate information via the internet without knowledge of the actual user of the platform, start a denial of service attack, thereby possibly rendering the platform to be no longer usable for a dedicated application requiring a specific status of the platform, and the like.

For these reasons, great efforts are being made in developing mechanisms for enhancing integrity of computer platforms so as to reduce the probability for "successful" external attacks, for instance in the form of malicious software, denial of service attacks, sniffing, spoofing and the like, and also to enhance data integrity with respect to internal manipulations of the computer platform. For example, a plurality of encryption techniques are available, such as symmetric or asymmetric encryption/decryption techniques which enable the exchange of data with a high degree of resistance against the tampering of data by a third party during the transmission and storage of data. In asymmetric encryption techniques a pair of a private key and a public key may be used for encrypting data by means of one of the keys and deciphering the data by using the other key, wherein one of the keys may be publicly accessible. In symmetric key encryption techniques a unique key is used for both the encryption and decryption of data, wherein access to the unique key may have to restricted to authorized parties. Although these techniques may provide for enhanced integrity in data communication and data storage, the actual configuration of a computer platform under consideration may still provide the possibility of a plurality of attacks, in particular, as many applications intended for increasing computer security may rely on a trusted platform configuration.

A trusted computer platform may be considered as a computer system in which the hardware configuration as well as the software applications may be assumed to be in a dedicated configuration. However, a secure platform configuration may be established only be establishing a "chain" of trusted platform levels, wherein each subsequent level may be initialized by the preceding level only, if the integrity of the subsequent level has been verified. Hence, the integrity at system level may be preserved through a chain of integrity verifications wherein a root of the chain of verification steps may have to be provided with a high degree of tamper resistance so as to also accomplish a high confidence with respect to integrity of the system after initializing the highest level, ie. the level of user applications.

In a typical computer platform the initialization of the system requires various degrees of abstraction, for example with respect to initializing the central processing unit (CPU), initializing the system memory, which is typically provided externally to the CPU, loading an operating system into the system memory from an

external mass storage device, and finally executing user applications. Thus, in view of enhancing the overall integrity of the system as a whole, it may not be sufficient to assume that the various system activities prior to loading the operating system can be considered to be secure so as to rely on the integrity of the operating system and the user application, since the operating system may be invoked by a "mistrusted" process, thereby providing the opportunity of manipulating the basic platform configuration by modifying hardware and software components. Hence, the process of initializing the various hardware components of the computer system, such as the system memory and the execution of the instructions contained therein for initializing the higher system levels, which may also be referred to as boot strapping or booting, may have to be incorporated into the chain of trust so as to provide for enhanced overall system integrity.

A typical start sequence for initializing a computer system after applying power or after a reset event causes a "power on self-test" of the CPU wherein also the processor starts execution of instructions at a dedicated entry address that is indicated by the processor's reset vector. That is, after an initial processor self-test the execution of instructions may start at the entry point which may typically be an address of a software routine, frequently referred to as BIOS (basic input/output system), which may be stored in a dedicated external non-volatile memory of the computer platform. Under the control of the BIOS the remaining self-test may be performed and the hardware configuration of the platform may be determined or measured". Thereafter a search for a bootable device may be performed, such as a mass storage device, for instance the hard disk of the computer system, a disk, a CD-ROM, an extension card, and the like, from which a primary boot block may be loaded into the system memory, wherein control is then past to the primary boot block, which may load an operating system into the system memory.

Although great efforts have been made in also enhancing security of the entire boot process, it is difficult to provide a reliable core root of trust for measurement (CRTM) for the boot process, for example in view of platform modifications such as replacement of the non-volatile memory chip including the BIOS software, since a corresponding chip replacement may therefore interrupt the chain of trust, thereby also rendering all subsequent verification steps as not trustworthy. Hence, great

efforts are made in providing a secure boot mechanism, wherein, however, frequently a trust center has to be used, thereby requiring comprehensive resources, whereas flexibility in updating the BIOS software may be reduced.

In view of the situation described above, the present disclosure relates to devices and methods for enhancing integrity of computer systems in combination with enhanced flexibility for BIOS upgrade capability, while avoiding or at least reducing one or more of the problems identified above.

SUMMARY OF THE DISCLOSURE

Generally, the present disclosure relates to devices and mechanisms for enhancing integrity of computer systems by establishing a static root of trust for measurement in that a certain set of data is provided that may include executable instructions and data values which, if a secure boot mechanism is enabled, will be accessed by the central processing unit without providing the possibility of circumventing access to the dedicated data set so that a defined root for the initialization of the platform is obtained. The set of data is implemented in such a manner that a high level of resistance against any attacks for manipulation may be achieved. During execution of instructions contained in the set of data the execution may not be changed or interrupted, thereby providing a high degree of integrity of the data which may thus be considered as a pre-boot set of instructions and data values. Since the processing of the instructions of the pre-boot data is mandatory at the start-up time of the system under consideration, a chain of trusted software may be started, thereby enabling a high degree of system integrity since the dedicated state of pre-boot data represents the static core root for the chain of subsequent verification steps. According to the principles disclosed herein, also an encryption key may be stored in the internal non-volatile memory, which may be accessed during the pre-boot phase on the basis of the secure instruction set in order to verify the integrity of at least a portion of signed boot data, the signature of which may also be generated on the basis of the encryption key stored in the non-volatile memory. Hence, prior to actually initializing the system memory, the boot data or at least a portion thereof may be verified by determining a signature of the boot data and

comparing the currently determined signature with the stored signature of the boot data. Consequently, using a unique symmetric encryption key for any desired platform results in a higher level of protection and also makes the BIOS non-interchangeable. This may be accomplished without involving a trust centre and may avoid general attacks which might concern a plurality of computer platforms, while at the same time a scaleable degree of security may be provided, wherein the "multiplicity", with which the unique symmetric encryption key is used, may determine the "granularity" of the degree of security. In some illustrative aspects disclosed herein, the unique encryption key stored in the non-volatile internal memory may also be used for creating a signature upon updating of the system BIOS, thereby further enhancing the overall flexibility of the trusted platform mechanism disclosed herein. Since the pre-boot data set and the unique symmetric encryption key may be maintained in a non-volatile internal memory, for instance in the CPU core itself, a high degree of integrity of the encryption key is achieved while substantially avoiding any attacks, for instance with respect to replacing BIOS chips and the like.

One illustrative method disclosed herein relates to a booting of a computer system. The method comprises, upon a power-on event or a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit wherein the internal non-volatile memory area contains an encryption key. The method further comprises determining a current signature of at least a signed portion of boot data, wherein the signed portion of boot data concerns a stored signature of the portion of boot data wherein the stored signature is created by applying the encryption key. The method further comprises executing boot instructions contained in the signed portion of boot data when the current signature and the stored signature are identical.

A further illustrative method disclosed herein relates to the booting of a computer system. The method comprises, upon a power-up event or a reset event, accessing an internal non-volatile memory of a central processing unit, wherein the internal non-volatile memory contains pre-boot instructions and data values for initializing an internal volatile memory of the central processing unit and for verifying the integrity of at least a portion of boot instructions and boot data values. The method

further comprises loading the at least a portion of the boot instructions and boot data values from a non-volatile memory into the internal volatile memory by executing the pre-boot instructions. Furthermore, the method comprises verifying an integrity of the at least a portion of the boot instructions and boot data values by using an encryption key stored in the internal non-volatile memory and using a signature associated with the at least a portion of the boot instructions and boot data values, wherein the signature is formed on the basis of the encryption key. Additionally, the method comprises determining whether an upgrade version of the boot instructions and boot data values is available when the integrity of the at least a portion of the boot instructions and boot data values has successfully been verified. Finally, the method comprises generating a signature of the upgrade version by using the encryption key when an upgrade version is available.

An illustrative central processing unit (CPU) disclosed herein comprises a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting the CPU core, the volatile random access memory and the non-volatile memory. The CPU further comprises pre-boot information stored in the non-volatile memory, wherein the pre-boot information includes instructions executable by the CPU core which also includes a symmetric encryption key for verifying at least a portion of a boot routine that is a signed by applying the symmetric encryption key.

One illustrative computer system disclosed herein comprises a central processing unit as specified above and a non-volatile boot memory configured to hold at least a boot routine and a second boot routine.

BRIEF DESCRIPTION OF THE DRAWINGS

Further embodiments of the present disclosure are defined in the appended claims and will become more apparent with the following detailed description when taken with reference to the accompanying drawings, in which:

Fig 1a schematically illustrates a central processing unit (CPU) including a random access memory (CACHE), a CPU core and a non-volatile memory including pre-boot information and a symmetric encryption key according to illustrative embodiments;

Fig 1b schematically illustrates a computer system including a CPU with pre-boot information and an encryption key according to still other illustrative embodiments;

Fig 1c schematically illustrates a process for verifying a portion of BIOS data, also referred to as initial BIOS loader (IBL) on the basis of a symmetric encryption mechanism according to illustrative embodiments;

Fig 1d schematically illustrates a flow diagram for a method of verifying integrity of boot data instructions and values according to still further illustrative embodiments;

Fig 1e schematically illustrates a flow diagram of a method for verifying integrity of BIOS data and generating a signature for an upgrade version of BIOS data according to still further illustrative embodiments; and

Figs 1f and 1g schematically illustrate flow diagrams of methods for performing verification of BIOS integrity and updating the BIOS data according to still other illustrative embodiments.

DETAILED DESCRIPTION

While the present disclosure is described with reference to the embodiments as illustrated in the following detailed description as well as in the drawings, it should be understood that the following detailed description as well as the drawings are not intended to limit the present disclosure to the particular illustrative embodiments disclosed, but rather the described illustrative embodiments merely exemplify the various aspects of the present disclosure, the scope of which is defined by the appended claims.

Generally, the present disclosure provides a system and a mechanism for executing – at start up or reset or any other operational state requiring an initialization of the system – instructions stored in a memory area that may not be accessed after completing a verification phase of at least a portion of boot instructions. For this purpose, the verification process may be based on a symmetric encryption key also stored in a memory area that may be locked in view of any operational state of the CPU except for start up or reset events. For example, the instructions and their symmetric encryption key may be stored in a non-volatile memory forming a part of a central processing unit, thereby significantly reducing the possibility of manipulating the data included in the non-volatile memory. Consequently, the contents of the non-volatile memory may be used as a static root of trust for measurement during the initialization of the CPU and the entire computer system by ensuring that upon power-up or reset of the CPU the first instruction is fetched from the non-volatile memory. Thus, the set of data contained therein may serve as a pre-boot or pre-BIOS component, which may enable the initialization of further system components, such as an internal random access memory, which may be used for storing operational data like variables and stack and instructions for running a portion of the BIOS software. For instance, the data cache as part of the random access memory area and an instruction cache may be initialized by the pre-boot data of the internal non-volatile memory, thereby substantially avoiding the possibility of external access to data contained therein during the initialization process. That is, the random access memory area, ie. the data cache and the instruction cache, are CPU internal components so that unwanted manipulation thereof may be very difficult, in particular as the external system memory is not initialized, as long as at least a portion of the BIOS software has been verified. Depending on the storage capacity of the random access memory, the BIOS routine may be divided into two or more portions such that verification of one or more signatures in view of BIOS integrity may be performed in the random access memory for a first portion that is configured to have a size so as to fit into the cache memory. Thus, this portion of the boot information may, after verification on the basis of the symmetric encryption key, be executed for instance directly from the random access memory, thereby substantially avoiding any manipulation process of verifying the first portion of the boot instructions. Thus, after verification of the signature of the first portion by applying the stored symmetric encryption key flow

control may be passed to the verified portion and the further boot process may be continued by initializing the system memory and copying the remaining boot information, while also verifying integrity of the further boot information, for instance on the basis of hash algorithms wherein, however, the generation of a signature may not be required due to the chain of trust created to the preceding verification on the basis of a signature and the stored metric encryption key. Consequently, the data, ie. the instructions and data values including the symmetric encryption key contained in a non-volatile internal memory area provided as an integral part of the CPU may be used as a static core root of trust for measurement, thereby providing a computer platform, in which a temporary system hardware and software configuration may be realized. In particular, in view of attacks, such as replacement of the BIOS chip, the mechanism of embodiments disclosed herein may provide enhanced security for typical practical applications, which use the platform in the context of financial transactions or digital rights management, which may be based on the requirement of a trustworthy computer platform. Additionally, using a symmetric encryption key mechanism provides for security without having to rely on a trust centre for handling private and public keys, as is the case asymmetric encryption techniques, thereby significantly reducing the overall complexity. At the same time, the desired degree of security may be determined by restricting the usage of the unique encryption key to a specified type of central processing unit so that manipulations or loss of secrecy for one unique encryption key may not affect other CPUs that have been fabricated on the basis of a different unique encryption key. Moreover, illustrative embodiments disclosed herein may provide for an efficient technique for updating the BIOS software using the stored encryption key for generating a respective signature, which may then be added to the upgrade version of the BIOS software, which may then be verified upon booting the computer system on the basis of the newly created signature and the stored encryption key.

With reference to the accompanying drawings further illustrative embodiments will now be described in more detail.

Fig 1a schematically illustrates a central processing unit (CPU) 100 according to illustrative embodiments in which a core root of trust for measurement (CRTM) may

be implemented with a high degree of tamper resistance. The CPU 100 may comprise a CPU core 102 which may include components for data processing, such as for performing arithmetic operations, logic operations and the like. The CPU core 102 may be functionally connected to a random access memory 101, which may comprise a plurality of static RAM cells and the like, corresponding to the overall configuration of the CPU 100. In one illustrative embodiment the RAM 101 may comprise a first memory portion, also indicated as data cache 101a, and a second portion indicated as instruction cache 101b. For example, the RAM 101 may be implemented in a fast memory technology so as to enhance the overall performance of the CPU 100, as is typically required in sophisticated applications. It should be appreciated, however, that any appropriate memory technology may be used for the memory 101, as long as direct control of the memory 101 via the CPU core 102 may be accomplished without the possibility of external access during the initialization of the CPU 100. The CPU 100 may further comprise a non-volatile memory 103, which may be provided in any appropriate memory technology, for instance in the form of a flash memory or a read-only memory technique, which may not enable external access for modifying the contents of the memory 103. Hence, the memory 103 may be considered as a secure memory area, the contents of which may therefore represent a static root of trust. For this purpose, a set of data 103a, which is to be understood as instructions executable by the CPU core 102 and data values representing operands and the like of the instructions, may be provided, at least in a portion of the memory 103, which may not be overwritten with new data once the respective portion of the memory 103 is programmed. Additionally, the memory 103 may contain a symmetric encryption key 103b, which may also be used for signing a portion of boot information that may initially be used for initializing a computer system comprising the CPU 100. It should be appreciated that the memory 103 may not necessarily represent a continuous memory area, a portion of which may contain the data set 103a and a portion of which may contain the encryption key 103b but may be implemented in any appropriate manner, for instance as substantially independent components of the CPU 100, as long as external access of the data set 103a and the encryption key 103b may be suppressed after a certain phase of the initialization process. Furthermore, the CPU 100 may comprise a lock mechanism 105, which may be configured such that access of the CPU core 102 to the memory 103, or at least the

encryption key 103b, may be enabled upon power-on or a reset event only, while disabling the memory 103 accomplished by instructing the lock mechanism 105 during the boot process after verification of at least a portion of the boot information. For instance, the lock mechanism 105 may comprise circuitry for shutting down supply energy for the memory 103 and also for the mechanism 105 itself, thereby locking the mechanism 105 and also the memory 103 non-responsive to any accesses performed after a request for "locking" the memory 103 or at least a portion thereof including the symmetric encryption key 103b. On the other hand, enabling the memory 103, for instance by providing power to the lock mechanism 105, may be associated with a power-up or a reset event only. It should be appreciated, however, that the lock mechanism 105 may have any other appropriate configuration in which external access to the encryption key 103b may be restricted, an operational status of the CPU 100 in which, after reset or power-on, a corresponding instruction for locking the encryption key 103b has not yet been executed.

The internal components of the CPU 100, that is, the memory 103, the CPU core 102, the internal RAM 101 and the lock mechanism 105, may be interconnected by means of a bus system 104 such that upon power-up or reset a jump to a specified address of the memory 103 is performed. Consequently, a "hard-wired" target for a reset vector of the CPU core 102 may be provided which ensures that execution of instructions may start from the memory 103, at least for a power-up event or a reset event.

It should be appreciated that the CPU 100 may be formed on the basis of sophisticated semiconductor manufacturing techniques in which an appropriate carrier material, such as a semiconductor substrate and the like, may receive a plurality of circuit elements formed on the basis of a technology under consideration, such as CMOS processes and the like, in which transistor elements, capacitors, resistors and the like, may be formed in accordance with specific device architecture for the CPU 100. In the embodiment illustrated herein the various components of the CPU 100 may therefore be formed on a common substrate during a common manufacturing process flow, thereby providing the memory 101 and 103 as an internal or integral component of the device 100. For example,

respective manufacturing techniques are well-established in which volatile and fast memory cells may be formed together with non-volatile memory cells and high performance logic gates, as may be required in the CPU core 102. Additionally, appropriate mechanisms may be provided such that after programming the memory 103 or at least a portion thereof including the data set 103a and the symmetric unique encryption key 103b, further access may be prevented so as to provide a protected environment for the data set 103a and the encryption key 103b.

Fig 1b schematically illustrates a computer system 150 comprising the CPU 100 providing for the protected environment for the data set 103a and the encryption key 103b, as previously explained, wherein in the embodiment shown the CPU 100 may comprise the random access memory 101 in the form of the data cache 101a and the instruction cache 101b, which may have a size of for example 64 bytes so as to accommodate a portion of boot information and to act as a "system RAM" when performing instructions to the data set 103a. Similarly, the instruction cache 101b may be provided with the size of 64 Kb, wherein it should be appreciated that any other appropriate memory size may be used that is compatible with the size of a respective portion of boot information that is to be performed from the memory 101 during a verification process. Also the internal non-volatile memory 103 may be provided with any appropriate size and configuration so as to be compatible with the requirements for the data 103a and the symmetric encryption key 103b. For example, the set of data 103a may comprise instructions and data values representing a secure load routine for loading a respective portion of boot information into the internal memory 101 for performing a verification process.

The computer system 150 may further comprise a system memory 110, for instance in the form of any appropriate memory device including random access memory cells, such as dynamic RAM cells and the like. The size of the system memory 110 may be adapted to the requirements of the system 150 in view of performance and storage capacity. Furthermore, the system 150 may comprise a non-volatile memory 121, such as a flash memory and the like, which may include information, also referred to as BIOS information, at least a portion of which may be a signed portion, that is, a signed portion may comprise a signature obtained on the basis of an appropriate hash algorithm in combination with an encryption mechanism using

the symmetric encryption key 103b as stored in the memory 103. In one illustrative embodiment, the non-volatile memory 120 may contain the boot information divided into two portions wherein a first portion may comprise data and instructions for initializing other system components, such as the system memory 110 for accommodating the second portion of boot information and executing the second portion once the first portion has been verified on the basis of the protected environment provided by the CPU 100. The first portion may also be referred to as an initial boot loader (IBL), which may represent the signed portion of the boot information contained in the memory 120.

In some illustrative embodiments the non-volatile memory 120 may comprise a first portion 120a for containing a first BIOS version that may be accessed upon initializing the system 150, which may be indicated as an enabled version of BIOS information contained in the memory 120. Moreover, a second portion 120b may be provided, which may contain a second BIOS version, such as an upgrade version, and which may be in a non-enabled state, thereby requiring validation and the creation of a signature on the basis of the stored encryption key 103b during an initialization phase, as will be described later on in more detail. Consequently, the memory 120 may have a sufficient capacity for holding at least two BIOS versions, thereby providing for the possibility of efficiently updating the BIOS information for the system 150 while nevertheless providing for enhanced security of the update process, as will be described later on.

The computer system 150 may further comprise an interface system 140 configured to operatively connect the system memory 110 and the non-volatile memory 120 with the CPU 100. In one illustrative embodiment the system 150 may further comprise a one-time programmable memory 130, which may include platform-specific information, for instance about boot sources and related parameters. For instance, as shown, the one-time programmable memory 130 may comprise information concerning boot options in order to indicate to the CPU 100 whether to boot from the internal memory 103 or not. For example, security bits may provided in the memory 130 including a respective bit that determines where the initial instruction fetch of the CPU 100 after reset is rooted to. For example, with this bit set to "1", execution may be passed to the internal memory 103 thereby enabling

the secure boot processing. It should be appreciated that in other illustrative embodiments the one-time programmable memory 130 may be omitted or may be provided so as to include other information controlling the secure boot processing during development and actual applications.

Fig 1c schematically illustrates the configuration of boot information 121 that may be stored in the non-volatile memory 120, for instance in one of the portions 120a, 120b as an "enabled" version of boot information contained therein. In the embodiment shown in Fig 1c, the boot information 121, which may also be referred to as BIOS, may comprise a first portion 121a which may represent a set of data including instructions and data values having a size so as to be compatible with the size of the memory 101, as previously explained. For example, for the above-given exemplary values of 64 Kb for each of the RAM areas 101a, 101b a maximum size of the portion 121a may be restricted to approximately 32 Kb. It should be appreciated, however, that any other appropriate size for the portion 121a may be applied, depending on the available amount of storage within the RAM 101. It should further be appreciated that providing the portion 121a may be necessary for boot information 121, which exceeds the size of the memory 101, so that the entire boot processing may not be performed on the basis of the memory 101, since typical boot routines may have a size of several hundred kilobytes and more. In other cases, when sufficient storage space may be available in the CPU 100, the boot information 121 as a whole may be used during the secure boot processing, as will be explained later on in more detail.

Thus, if the portion 121a may be provided, as shown in Fig 1c, this portion may serve as an initial BIOS loader (IBL) for a second portion 121b, wherein the first portion 121a may also contain a hash value obtained over the portion 121b. The hash value for the portion 121b may also be protected by a signature contained in the portion 121a obtained from a hash value generated over the first portion 121a, which may be encrypted by the encryption key 103b. Thus, an encryption of the hash value of the second portion may not be necessary. The signature of the hash value for the portion 121a may be used for verifying the portion 121a during a secure boot processing. The portion 121a may therefore be contained in instructions for performing necessary platform initialization actions, such as

initialization of a memory controller 141 and the like, followed by the shadowing of the portion 121b from the memory 120, ie. from one of the portions 120a, 120b, into the initialized system memory 110. Thus, after ??? the portion 121a, 121b the respective hash values may be created and may be added to the portion 121a, which may then, for an initial version of the BIOS information 121, be encrypted by a version of the symmetric encryption key 103b. The corresponding signature obtained by applying the key 103b may also be added to the portion 121a, as shown at the right-hand side of Fig 1c.

Fig 1d schematically illustrates a sequence for verifying the signature 121s contained in the portion 121a, which may be performed on the basis of the data set 103a and the encryption key 103b during start-up or reset of the system 150. The verification may be accomplished on the basis of any appropriate encryption algorithm used using the symmetric key 103b, wherein the initially created hash value such as hash 0, obtained over the portion 121a, which may include respective hash values for the portion 121b, may be used for generating the signature 121s by applying the key 103b. The initially created hash value for the portion 121a may then be compared to a respective hash value obtained by applying the appropriate hash algorithm over the portion 121a that is copied into the RAM memory 101. The portion 121a may be considered as verified if a signature generated by ???ing the key 103b to a calculated hash value match with the signature 121s contained in the portion 121a.

In view of implementing the system 150 as a secure platform a static root of trust may have to be implemented so as to enable a secure start-up of an operating system after power-up or reset of the computer system 150. For this purpose, a defined execution of the trusted BIOS information 121 may be accomplished by verifying at least the portion 121a on the basis of the trusted set of data 103a and the encryption key 103b, which are substantially resistant against any external manipulation. Thus, each time the system 150 may be activated by using a secure boot process, thereby enabling integrity of the entire boot process and trusted initialization of an operating system, which in turn may be used for performing security sensitive applications. On the other hand, if the integrity check may fail, for instance during verifying the portions 121a or 121b, an appropriate policy may

be applied, for instance the boot process may be terminated or surfaces provided by the system 150 may be limited. Thus, the secure boot architecture disclosed herein may protect against "class breaks", which are to be understood as attacks that will work against every instance of a given security system. For example, a piece of software generated by an external source may be considered as class break, which may be easy to install and enable circumvention of security measures, thereby enabling unauthorized use of the platform. In digital rights management (DRM) environments a class break may already be given when the DRM protected data file may be broken once, thereby enabling a redistribution of the unprotected file. Consequently, the mechanisms and systems disclosed herein may provide for enhanced security with respect to class breaks since a protected environment may be obtained on the basis of an integral portion within the CPU itself, thereby requiring manipulation of the CPU itself, wherein for instance the revealing of the encryption key 103b may only concern respective CPUs, into which this version of the encryption key 103b has been incorporated during the production process, while however other products manufactured on the basis of a different encryption key may nevertheless provide for a secure platform.

In step 161 the system may be reset or power may be supplied thereto or any other event may occur that may require a secure boot processing. Consequently, an appropriate self-test may be performed by the CPU core 102 and respective components, such as registers and the like, may be initialized. It should be appreciated that in some embodiments a secure boot processing may not be enabled in an operating state in which the operating system may stay in control of the system 150. In step 162 the first instruction is fetched from the internal non-volatile memory 103, which may be accomplished by mapping the internal memory 103 to the corresponding reset vector addressed. Consequently, the CPU 100 starts execution on the basis of the secure data set 103a in any instances in which a jump to the reset vector is caused by an external event. In step 163 the internal random access memory 101 may be initialized caused by the execution of the instructions contained in the data set 103a. In step 164 at least a portion of the boot information 121, for instance the portion 121a, including the signature 121s thereof, may be loaded into the internal random access memory 101. As previously explained, the signature 121s has been generated by applying the symmetric

encryption key 103b. In step 165 a signature of the boot data in the memory 101, for instance the portion 121a, is generated by, for instance, calculating a respective hash value, as previously explained, and applying the encryption key 103b by accessing the memory 103.

In step 166 the currently calculated signature is compared with the signature 121s and both values match, the process flow advances to step 167 in which the boot process may be continued, for instance by initializing the system memory and verifying the rest of the boot information 121. In the verification phase in step 166 the encryption key 103b is locked in step 168, for instance by disabling a respective portion of the memory 103 via the lock mechanism 105, as previously explained. Next, in step 169 the boot process may be terminated, which may include for instance an indication that an invalid BIOS information 121 is present in the internal memory 120.

Fig 1e schematically illustrates a sequence of steps for continuing the boot process after step 167 in Fig 1d. In step 167a, the system memory 110 may be initialized and in step 167b the BIOS information 121, or at least the portion 121b, may be loaded into the system memory 110. In step 167c the BIOS information 121, or at least the portion 121b, may be verified in the system memory 110, for instance by calculating one or more respective hash values and comparing the values with the corresponding hash values contained in the portion 121a, which has been verified in step 166, Fig 1d. In step 167d, the process flow branches into step 167e, when the remaining portion of the boot information has not been verified, or into step 167f wherein the boot process may be continued, for instance by loading the operating system, as previously explained.

In the above-described embodiment before passing execution to the boot information 121 or the portion 121a, the secure boot process, ie. the process flow represented by the steps 161 – 166, may not apply any reset procedures to any components of the system 150, thereby enabling reliable "measurement" of the hardware configuration of the system 150.

Fig 1f schematically illustrates a flow diagram for representing the operation of the system 150 when updating of a BIOS information may be possible.

In step 171 a reset event, such as power-on, may occur and the process flow may advance to step 172 in which it is determined whether the secure boot processing is enabled or not. If secure boot processing is not enabled, which may be advantageous during testing and debugging the system 150, an alternative process flow may be initiated. If secure boot processing is enabled the process flow may advance to step 173 in which execution of instructions may be started by accessing the internal non-volatile memory 103 and performing instructions of the set 103a, as previously explained. In step 174 integrity of at least a portion of the boot information, such as the portion 121a, may be checked, for instance in the same way as previously described with reference to the process flow in Fig 1d. If integrity of the boot information 121a is not verified in step 174, the process may advance to step 175 in which the encryption key 103b may be locked and the boot process may be terminated or booting may be continued, however with limited surfaces provided by the system 150. If integrity is validated in step 174, execution of instructions of the boot information 121a may be started in step 176. In step 177 it may be determined whether or not updating of the BIOS information 121 may be required. For this purpose, for instance, the internal memory 110 may be accessed so as to determine whether or not a non-enabled version of BIOS information is available or not. If a respective updating of the BIOS information is not required, the process flow advances to step 178 in which the encryption key 103b is locked, as previously explained. Thereafter, in step 179, the boot processing may be continued, as previously explained. When in step 177 updating of the BIOS information 121 is required, the process flow advances to step 180 in which the BIOS version contained in one of the memory areas 120a or 120b of the non-volatile memory 120 may be validated. For this purpose, any appropriate mechanism may be used, for instance using an asymmetric encryption mechanism, on which upon creating the BIOS version respective hash sums may have been calculated and have been encrypted by a secret key, which may now be validated on the basis of a public key, which may be contained in the new BIOS information.

When in step 181 a valid version of the new BIOS information is identified, a signature may be created by applying the encryption key 103b in that a respective hash sum may be calculated over the respective IBL portion of the new BIOS information, which may then be signed by applying the encryption key 103b. In step 182 the encryption key 103b may then be locked, as previously explained, and in step 183 the signature generated in step 181 may be added to the new BIOS information, for instance to the respective IBL portion 121a, when the BIOS information is provided in several parts. In step 184 the new BIOS information may be enabled, that is, an indication may be stored in the non-volatile memory 103 or any other appropriate storage that the new BIOS version is a BIOS information to be used for performing the boot process. In step 185 a reset event is generated so that the process flow returns to step 171. Consequently, upon enabling the upgrade version of the BIOS information in step 184, the steps 172 – 177 may be repeated on the basis of the upgrading of the BIOS information and the boot processing may be performed on the basis of the new BIOS information.

Fig 1g schematically illustrates a secure boot processing according to still other illustrative embodiments. As shown, in steps 181 and 182 reset events may be detected and it may be determined whether or not secure boot is enabled, as also previously explained. In step 183 instruction execution is performed from the internal data set 103a. In step 184 a CPU internal initialization may take place. In some illustrative embodiments, this may include steps 184a, ..., 184j. For example, in step 184a the memory 103 may be remapped. In step 184b a boot source may be detected and may be initialized in step 184c, followed by initialization of the data cache 101a and the instruction cache 101b according to steps 184d, 184e. In step 184f an unreal mode for the data cache may be set up and the image of the boot information 121 for the portion 121a may be copied into the data cache 101a, while in step 184h storage space may be assigned for variables in the data cache 101a. If required, in step 184i vendor identification may be retrieved and in step 184j a respective encryption engine may be initialized. Thereafter, in step 185 the hash sum over the signed BIOS data 121a, that is, the IBL, may be calculated. In step 186 the internal encryption key 103b may be applied to a previously calculated hash sum so as to generate a signature. In step 187 the signature determined in step 186 may be compared with the signature contained in the signed BIOS

information 121a. In step 189 the boot processing may be terminated if the signed BIOS information has been identified as an invalid information and the internal key 103b may be locked in step 189. In step 188 execution of the BIOS information may be started when a valid version of the BIOS information has been identified in step 187. In step 190 it may be determined whether updating of the BIOS information is required. If so, in step 191 the new BIOS information may be validated, for instance as previously indicated, and in step 192 it may be decided whether or not the new BIOS information is valid information or not. If a valid BIOS version is detected in step 192, in step 193 a hash sum may be calculated over the new BIOS information, ie. a respective portion thereof, such as an IBL portion, and in step 194 the internal encryption key 103b may be applied to the hash value so as to generate a new signature. In step 195 the internal key used in step 194 may be locked and in step 196 the newly created signature may be added to the new BIOS information. In step 197 the new BIOS information may be enabled, as also previously explained. If in step 192 the new BIOS information is identified as an invalid information or if in step 190 updating of the BIOS information is not required, the process flow advances to step 198, in which the encryption key 103b may be locked. Thereafter, the boot processing may continue in step 199, which in some illustrative embodiments may include the initialization of further system components of the system 150, such as the system memory 110 in step 199a. Thereafter, in step 199b the BIOS information, as presently enabled, may be loaded in to the system memory and in step 199c the BIOS information may be verified, for instance by calculating respective hash sums and comparing the hash sums with the values contained in the BIOS information, as previously explained. If in step 199d the BIOS information is identified as valid information the boot processing may be continued in step 199e, for instance by performing further steps for finally loading an operating system. If in step 199d the BIOS information is identified as an invalid BIOS information, in step 199f the boot process may be terminated or an indication may be given and the surfaces of the system 150 may be enabled in a re??ted form, as previously explained.

As a result, the systems and mechanisms disclosed herein provide for enhanced integrity of computer platforms by providing a secure boot processing on the basis of a pre-boot routine contained in a non-volatile memory and a symmetric

encryption key. Since the non-volatile memory is a part of the CPU itself, system initialization may be accomplished on the basis of the pre-boot information stored in the non-volatile internal memory and verification of the boot information may be accomplished by using the symmetric encryption key. Thus, enhanced security of the platform may be accomplished without requiring a trust centre, wherein an efficient protection against class breaks may be obtained, while the degree of security may be determined on the basis of the granularity of the symmetric encryption key, which may be incorporated into the non-volatile memory during fabrication of the CPU device.

Further modifications and variations of the present disclosure will be apparent to those skilled in the art in view of this description. Accordingly, the description is to be construed as illustrative only and is for the purpose of teaching those skilled in the art the general manner of carrying out the embodiments. It is to be understood that the forms shown and described herein are to be taken as the presently preferred embodiments.

CLAIMS

1. A method for booting a computer system, the method comprising:

upon one of a power on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key; and

executing boot instructions contained of said signed portion of boot data, when said current signature and said stored signature are identical.

2. The method of claim 1, wherein executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory.

3. The method of claim 2, wherein executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data.

4. The method of claim 2, wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache.

5. The method of claim 1, further comprising locking said encryption key for external access prior to executing said boot instructions.

6. The method of claim 5, further comprising determining whether an upgrade version of said boot data is available.

7. The method of claim 6, wherein determining whether an upgrade version of said boot data is available is performed prior to locking said encryption key.

8. The method of claim 7, further comprising verifying said upgrade version of said boot data.

9. The method of claim 8, further comprising calculating a new signature over a hash sum of said upgrade version of the boot data using said encryption key and adding said new signature to said upgrade version of the boot data.

10. The method of claim 9, further comprising enabling said upgrade version of said boot data.

11. The method of claim 10, further comprising generating a reset event.

12. The method of claim 10, further comprising locking said encryption key prior to enabling said upgrade version of the boot data.

13. A method for booting a computer system, the method comprising:

upon at least one of a power up event and a reset event, accessing an internal non-volatile memory of a central processing unit, said internal non-volatile memory containing pre-boot instructions and data values for initializing an internal volatile memory of said central processing unit and verifying an integrity of at least a portion of boot instructions and boot data values;

loading said at least a portion of said boot instructions and boot data values from a non-volatile memory into said internal volatile memory by executing said pre-boot instructions;

verifying integrity of said at least a portion of said boot instructions and boot data values by using an encryption key stored in said internal non-volatile memory and a signature associated with said at least a portion of said boot instructions and boot data values, said signature being formed on the basis of said encryption key;

after successfully verifying integrity of said at least a portion of said boot instructions and boot data values, determining whether an upgrade version of said boot instructions and boot data values is available; and

when an upgrade version is available, generating a signature of said upgrade version by using said encryption key.

14. The method of claim 13, wherein executing said boot instructions comprises initializing a system memory of said computer system and loading a second portion of boot instructions and boot data values into said system memory.

15. The method of claim 14, further comprising verifying integrity of said second portion and continuing booting of said computer system on the basis of said second portion when verification of said second portion is successful.

16. The method of claim 13, wherein initializing said volatile internal memory comprises initializing a data cache of said central processing unit and wherein said at least a portion is loaded into said data cache and is verified therein.

17. The method of claim 13, further comprising locking said encryption key prior to executing said boot instructions when an upgrade version is not available.

18. The method of claim 13, further comprising verifying said upgrade version of the boot instructions and boot data prior to generating said new signature.

19. A central processing unit (CPU) comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key.

20. The central processing unit of claim 19, further comprising a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power on event only.

21. A computer system comprising:

a central processing unit comprising

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory, and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key; and

a non-volatile boot memory configured to hold at least said boot routine and a second boot routine.

ABSTRACT

A CPU, a computer system and a secure boot mechanism are provided in which a symmetric encryption key may be incorporated into a non-volatile memory area of the CPU core, thereby substantially avoiding any tampering of the encryption key by external sources. Moreover, pre-boot information may internally be stored in the CPU and may be retrieved upon a reset or power-on event in order to verify a signed boot information on the basis of the internal symmetric encryption key. Furthermore, the BIOS information may efficiently be updated by generating a signature using the internal encryption key.





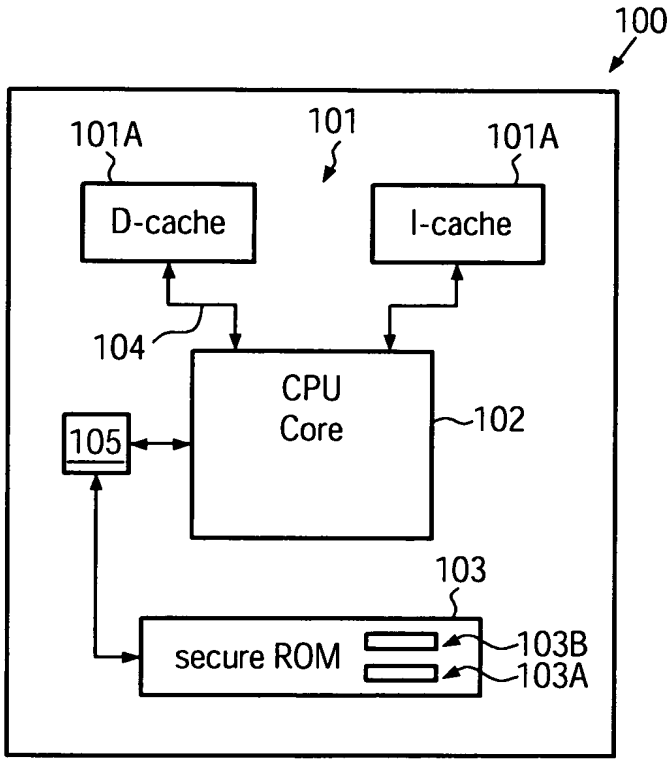

100
101A
101
101A
D-cache
I-cache
104
CPU
Core
102
105
103
secure ROM
103B
103A

FIG. 1a

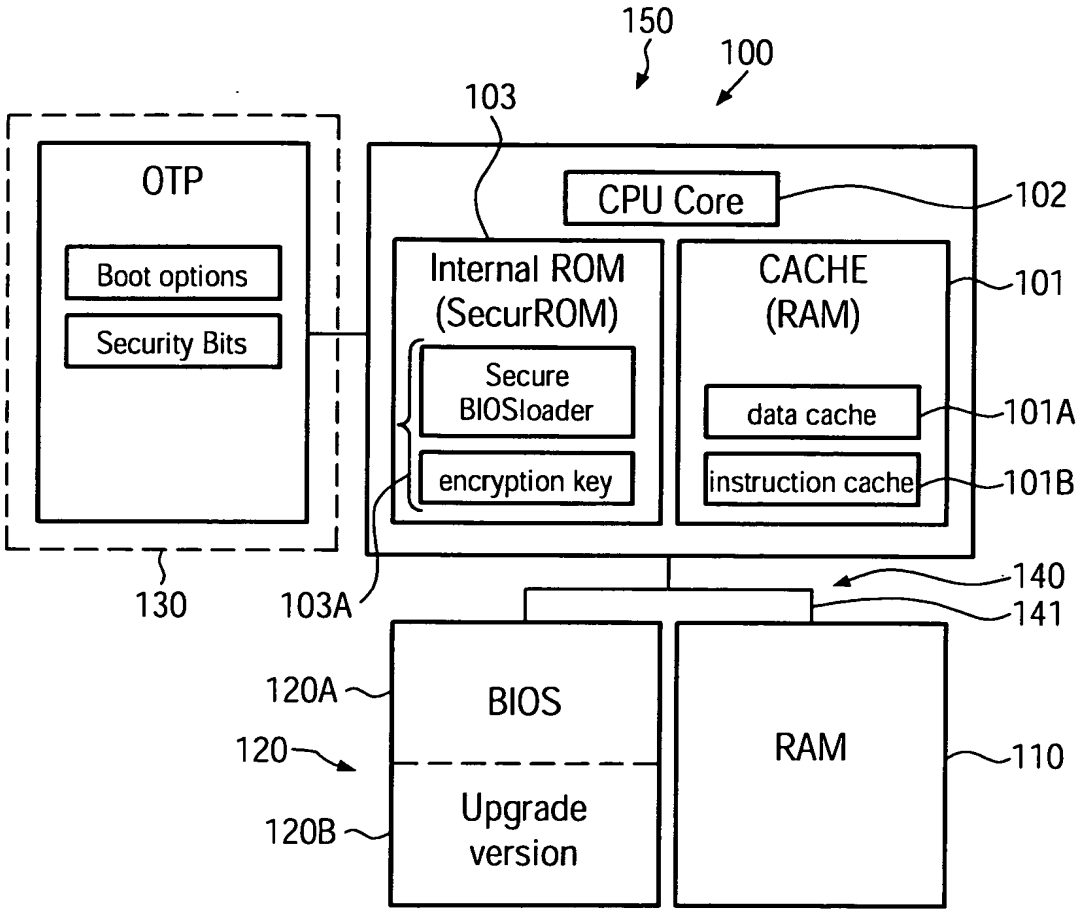

150
100
103
OTP
Boot options
Security Bits
CPU Core
102
Internal ROM
(SecurROM)
Secure
BIOSloader
encryption key
CACHE
(RAM)
101
data cache
101A
instruction cache
101B
130
103A
140
141
120A
BIOS
120
120B
Upgrade
version
RAM
110

FIG. 1b

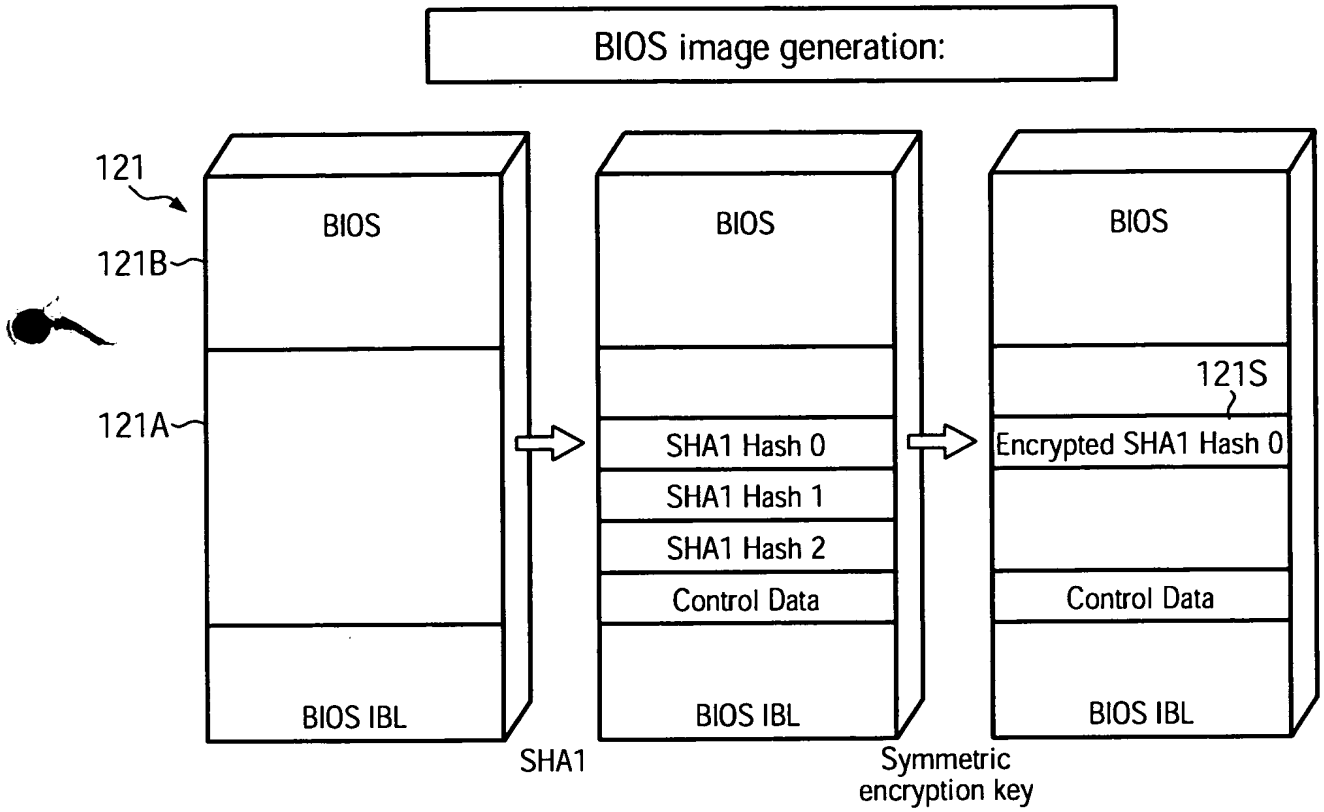

BIOS image generation:
121
121B
121A
BIOS
BIOS IBL
SHA1
SHA1 Hash 0
SHA1 Hash 1
SHA1 Hash 2
Control Data
Symmetric encryption key
121S
Encrypted SHA1 Hash 0

FIG. 1c

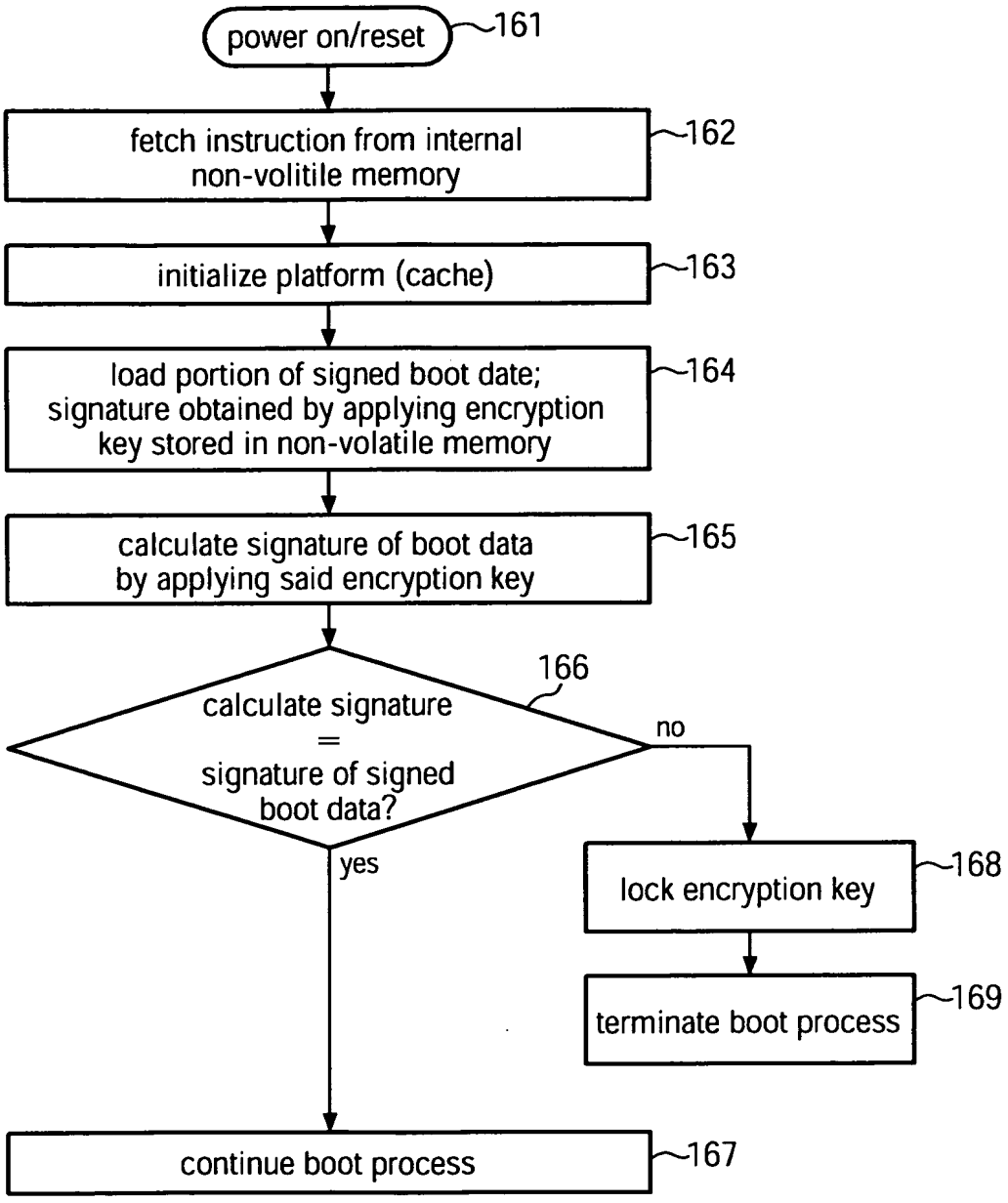

power on/reset
161
fetch instruction from internal non-volitile memory
162
initialize platform (cache)
163
load portion of signed boot date; signature obtained by applying encryption key stored in non-volatile memory
164
calculate signature of boot data by applying said encryption key
165
166
calculate signature = signature of signed boot data?
no
yes
lock encryption key
168
terminate boot process
169
continue boot process
167

FIG. 1d

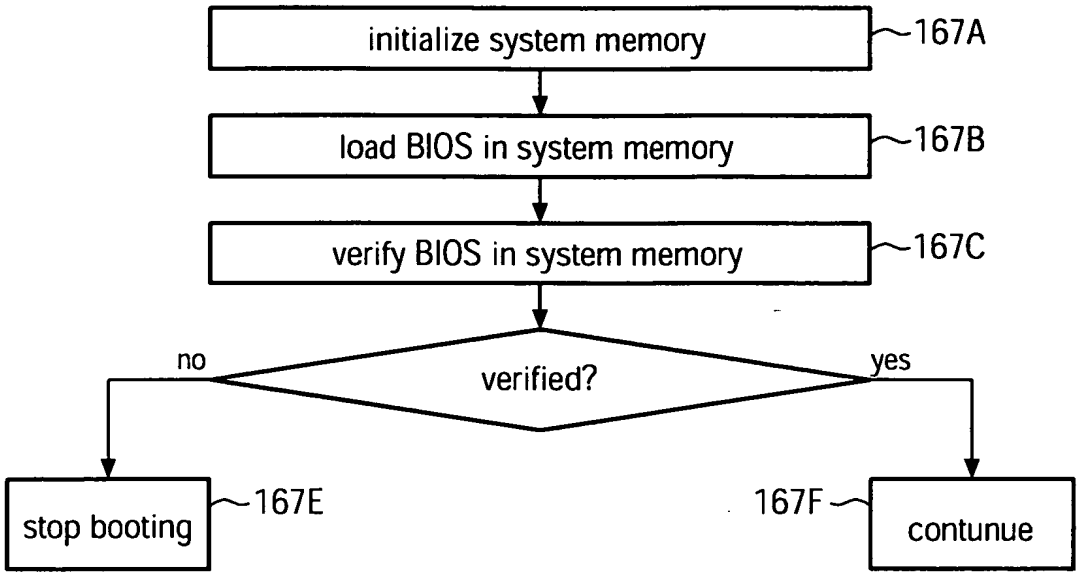

initialize system memory
167A
load BIOS in system memory
167B
verify BIOS in system memory
167C
verified?
no
yes
stop booting
167E
167F
contunue

FIG. 1e

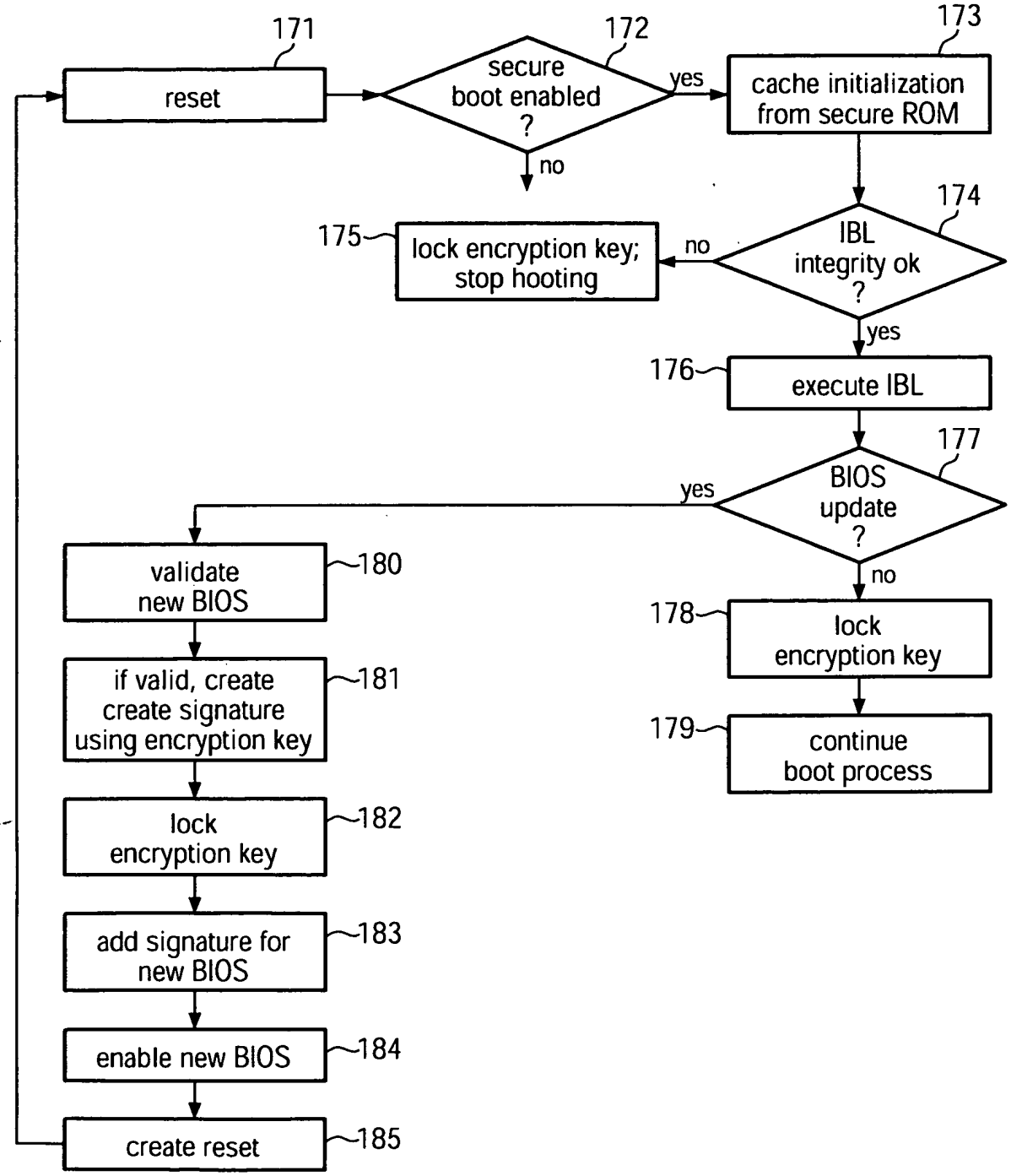

171
reset
172
secure boot enabled ?
yes
no
173
cache initialization from secure ROM
174
IBL integrity ok ?
no
175
lock encryption key; stop hooting
yes
176
execute IBL
177
BIOS update ?
yes
no
178
lock encryption key
179
continue boot process
180
validate new BIOS
181
if valid, create create signature using encryption key
182
lock encryption key
183
add signature for new BIOS
184
enable new BIOS
185
create reset

FIG. 1f

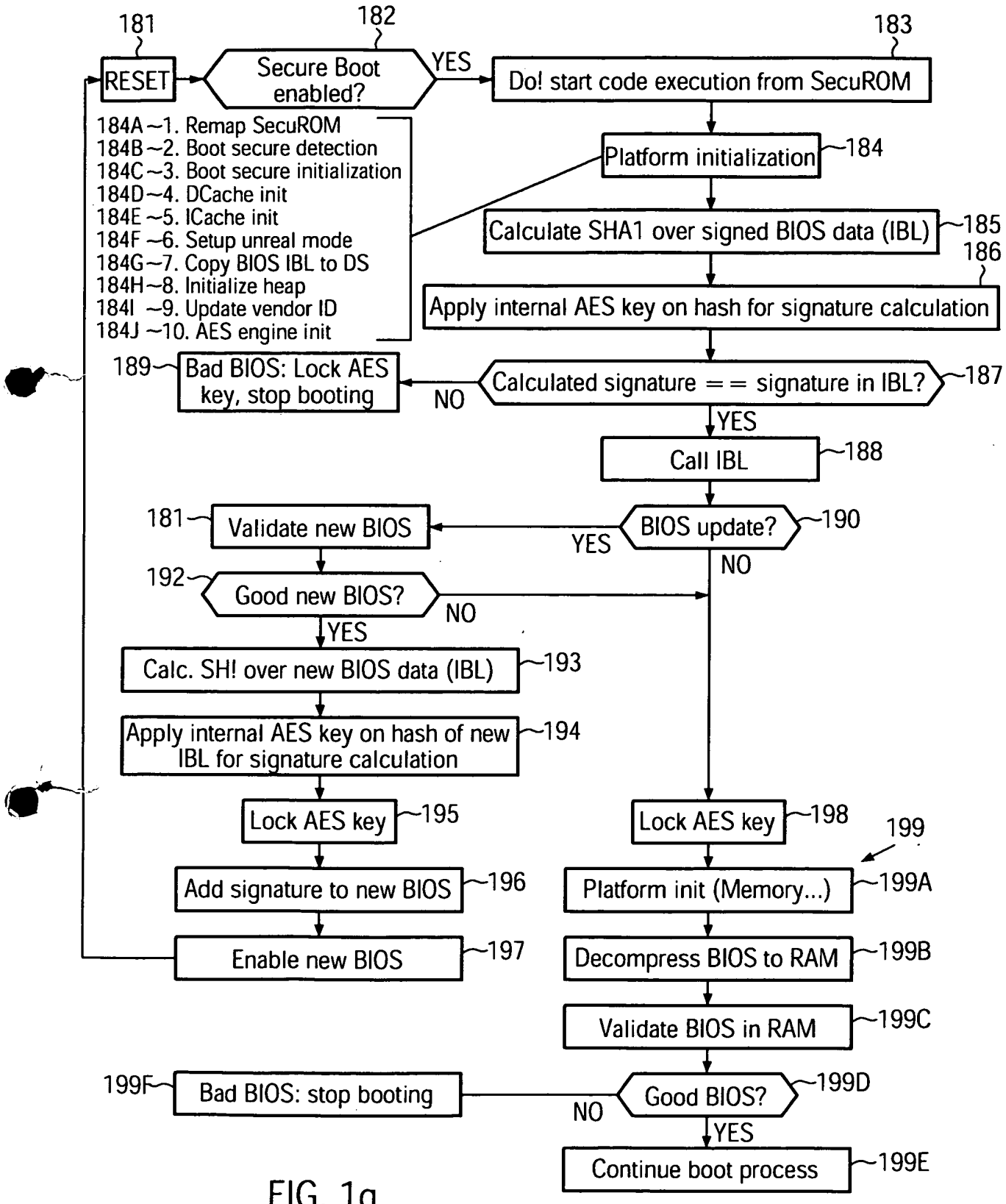

181
RESET
182
Secure Boot enabled?
YES
183
Do! start code execution from SecuROM
184A ~1. Remap SecuROM
184B ~2. Boot secure detection
184C ~3. Boot secure initialization
184D ~4. DCache init
184E ~5. ICache init
184F ~6. Setup unreal mode
184G ~7. Copy BIOS IBL to DS
184H ~8. Initialize heap
184I ~9. Update vendor ID
184J ~10. AES engine init
Platform initialization
184
Calculate SHA1 over signed BIOS data (IBL)
185
186
Apply internal AES key on hash for signature calculation
189
Bad BIOS: Lock AES key, stop booting
NO
Calculated signature == signature in IBL?
187
YES
Call IBL
188
181
Validate new BIOS
YES
BIOS update?
190
NO
192
Good new BIOS?
NO
YES
Calc. SHI over new BIOS data (IBL)
193
Apply internal AES key on hash of new IBL for signature calculation
194
Lock AES key
195
Lock AES key
198
199
Add signature to new BIOS
196
Platform init (Memory...)
199A
Enable new BIOS
197
Decompress BIOS to RAM
199B
Validate BIOS in RAM
199C
199F
Bad BIOS: stop booting
NO
Good BIOS?
199D
YES
Continue boot process
199E

FIG. 1g

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/355,900	01/19/2009	2115	1362	2000.162700/DE0892	21	4

CONFIRMATION NO. 7735

23720
WILLIAMS, MORGAN & AMERSON
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

FILING RECEIPT

OC000000034378375

Date Mailed: 02/09/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Michael Grell, Dresden, GERMANY;
Ralf Findeisen, Dresden, GERMANY;
Frank Schuecke, Dresden, GERMANY;

Power of Attorney:

Terry Morgan--31181
Paul Drake--33491
Jeffrey Pyle--34904
Scott Diring--35119
J Amerson--35426
Kent Cooper--37296
Barry Newberger--41527
Rubendra Bains--46532
Jaison John--50737
Mark Sincell--52226

Domestic Priority data as claimed by applicant

Foreign Applications

GERMANY 10 2008 021 567.8 04/30/2008

If Required, Foreign Filing License Granted: 02/03/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/355,900**

Projected Publication Date: 11/05/2009

Non-Publication Request: No

Early Publication Request: No

Title

COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/355,900	01/19/2009	Michael Grell	2000.162700/DE0892

CONFIRMATION NO. 7735

23720
WILLIAMS, MORGAN & AMERSON
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

POA ACCEPTANCE LETTER

OC000000034378409

Date Mailed: 02/09/2009

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/19/2009.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ebekeli/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/355,900	01/19/2009	Michael Grell	2000.162700/DE0892

CONFIRMATION NO. 7735

23720
WILLIAMS, MORGAN & AMERSON
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

PUBLICATION NOTICE

OC000000038630200

Title:COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

Publication No.US-2009-0276617-A1
Publication Date:11/05/2009

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
12/355,900		2115	

OC000000046355449

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 10742 on 11/01/2010

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 10742 is:

10742
GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

10742 7590 10/17/2011

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

EXAMINER	
ABBASZADEH, JAWEED A	
ART UNIT	PAPER NUMBER
2115	

MAIL DATE	DELIVERY MODE
10/17/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	12/355,900	GRELL ET AL.	
	Examiner	Art Unit	
	JAWEED A. ABBASZADEH	2115	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *13-18* is/are allowed.

7)☒ Claim(s) *1-6 and 19-21* is/are rejected.

8)☒ Claim(s) *7-12* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *1/19/2009* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/22/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 -21 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 19, and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Little et al. (hereinafter 'Little') US 20060112266.

As to claim 1, Little teaches a method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit [0030—"***After the processor 18 receives the reset signal***, rather than fetching instructions from an untrusted source (e.g. off-chip memory such as NOR flash 116)***, the processor 18 executes code read directly from its internal ROM 19***"], said internal non-volatile memory area containing an encryption key [0031—"a public key stored in the internal ROM 19"];

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data[Fig. 2, Signed code 118], said stored signature created by applying said encryption key [0031—"The program software residing in external memory 116 may be

authenticated in any conventional fashion, for example using a digital signature verification system such as "RSA," or any other suitable system, and preferably using a public key stored in the internal ROM 19" A digital signature verification system compares a current signature with a stored signature.]; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical [0032—"If the processor 18 determines that the program software in the external memory 116 has been authenticated successfully, the processor 18 begins to fetch and execute program code stored in the external memory 116 to initiate the basic functions of the device 10" Successful authentication means that the current signature and the stored signature are identical.].

As to claim 2, Little teaches executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory [0032—"the processor 18 begins to fetch and execute program code stored in the external memory 116" and Fig. 2, SRAM]. Although not specifically stated, when the processor fetches the code, it inherently gets stored in a RAM in order to be executed. As shown in Fig. 2 an internal SRAM is present for the program code to be executed from after it is fetched. Little further reinforces the inherency by previously mentioning that data is moved from a non-volatile memory to a volatile memory for processing [0016—"a memory controller

interface caches sectors out of non-volatile memory into volatile memory for processing"].

As to claim 3, Little teaches executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data [0032—"the processor 18 begins to fetch and execute program code stored in the external memory 116" and Fig. 2, SRAM and 0031—"The program software residing in external memory 116 may be authenticated"]. Although not specifically stated, when the processor fetches the code, it inherently gets stored in a system memory in order to be executed. As shown in Fig. 2 an internal SRAM is a system memory that is present for the program code to be loaded into. Little further reinforces the inherency by previously mentioning that data is moved from a non-volatile memory to a volatile memory for processing [0016—"a memory controller interface caches sectors out of non-volatile memory into volatile memory for processing"].

As to claim 4, Little teaches wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache Little further reinforces the inherency by previously mentioning that data is moved from a non-volatile memory to a volatile memory for processing [0016—"a memory controller interface caches sectors out of non-volatile memory into volatile memory for processing"]. It is well known in the art that a processor further uses a cache to load data that is to be executed.

As to claim 19, Little teaches a central processing unit (CPU), comprising:

a substrate having formed thereon circuit elements defining a CPU core [Fig. 2, MCU/DSP], a volatile random access memory [Fig. 2, Internal SRAM], a non-volatile memory [Fig. 2, 19] and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory [Fig. 2, The connections between the MCU/DSP, BootROM, External memory interface, and Internal SRAM make up the bus system]; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core [0030—The authentication code is the instructions executable by said CPU core] and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key [0030—"The internal ROM 19 contains the authentication code, includes one or more ***public keys***"].

As to claim 21, Little teaches a computer system, comprising:

a central processing unit comprising:

a substrate having formed thereon circuit elements defining a CPU core [Fig. 2, MCU/DSP], a volatile random access memory [Fig. 2, Internal SRAM], a non-volatile memory [Fig. 2, 19] and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core [0030—The authentication code is the instructions executable by said CPU core] and a symmetric encryption key for verifying at least a portion of a boot routine signed

by using said symmetric encryption key [0030—"The internal ROM 19 contains the authentication code, includes one or more ***public keys***"];

a non-volatile boot memory configured to hold at least said boot routine [Fig. 2, 116] and a second boot routine [Fig. 2, 118].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Little et al. (hereinafter 'Little') US 20060112266 in view of Chen et al. (hereinafter 'Chen') US 7,546,447.

As to claim 5, Little teaches the method of claim 1, but does not teach locking said encryption key for external access prior to executing said boot instructions.

Chen is cited to teach a similar secure boot method. Chen further teaches locking said encryption key for external access prior to executing said boot instructions [col. 6, lines 32-36-—"The secure store may be unlocked only when the platform is reset"]. Therefore, the secure store is locked after reset which would be prior to executing the boot instructions. It would have been obvious to one of ordinary skill in the art to have combined the teachings of Little and Chen because they are both

directed towards booting securely. Chen further improves upon Litlle by locking the encryption key to deter virus attacks [col. 4, lines 40-41].

As to claim 20, Little teaches the method of claim 1, but does not teach enabling a portion of non-volatile memory upon one of a reset event and a power on event. Chen is cited to teach a similar secure boot method. Chen further teaches a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power-on event only [col. 6, lines 32-36-—"The secure store may be unlocked only when the platform is reset"].

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Little et al. (hereinafter 'Little') US 20060112266 in view of Chen et al. (hereinafter 'Chen') US 7,546,447 as applied to claim 5 above, and further in view of Dailey et al. (hereinafter 'Dailey') US 2005/0216753.

As to claim 6, Little and Chen teach the method of claim 5, but do not teach determining whether an upgrade version of said boot data is available.

Dailey is cited to teach a method involving upgrading firmware. Dailey further teaches determining whether an upgrade version of said boot data is available [Fig. 5, 104 "Firmware update available flag set to yes?"]. It would have been obvious to one of ordinary skill in the art to have combined the teachings of Little and Chen with Dailey because they are all directed towards booting a computer system. Dailey introduces an improvement that allows for a BIOS to be upgraded. This would be advantageous because according to Dailey, it may be necessary to upgrade the firmware of a device to correct errors or improve performance [0003].

Allowable Subject Matter

Claims 13-18 are allowed.

Claims 7-12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAWEED A. ABBASZADEH whose telephone number is (571)270-1640. The examiner can normally be reached on Mon-Fri: 7:30 a.m.-5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas C. Lee can be reached on (571) 272-3667. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAWEED A ABBASZADEH/
Examiner, Art Unit 2115
10/10/11

Notice of References Cited	Application/Control No. 12/355,900	Applicant(s)/Patent Under Reexamination GRELL ET AL.	
	Examiner JAWEED A. ABBASZADEH	Art Unit 2115	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,389,532 B1	05-2002	Gupta et al.	713/163
*	B	US-2002/0099949 A1	07-2002	Fries et al.	713/200
*	C	US-2003/0014663 A1	01-2003	Sormunen et al.	713/200
*	D	US-2003/0229777 A1	12-2003	Morais et al.	713/2
*	E	US-2005/0021968 A1	01-2005	Zimmer et al.	713/176
*	F	US-2005/0138270 A1	06-2005	Morais et al.	711/102
*	G	US-2005/0138409 A1	06-2005	Sheriff et al.	713/200
*	H	US-2006/0015748 A1	01-2006	Goto et al.	713/190
*	I	US-2006/0026693 A1	02-2006	Bade et al.	726/034
*	J	US-7,036,023 B2	04-2006	Fries et al.	726/21
*	K	US-2006/0112266 A1	05-2006	Little et al.	713/161
*	L	US-7,073,064 B1	07-2006	Angelo et al.	713/176
*	M	US-7,174,457 B1	02-2007	England et al.	713/168

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 12/355,900	Applicant(s)/Patent Under Reexamination GRELL ET AL.	
	Examiner JAWEED A. ABBASZADEH	Art Unit 2115	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0055872 A1	03-2007	Soga et al.	713/168
*	B	US-2007/0113067 A1	05-2007	Oh et al.	713/002
*	C	US-2007/0198851 A1	08-2007	GOTO, Seiji	713/187
*	D	US-7,343,496 B1	03-2008	Hsiang et al.	713/194
*	E	US-2008/0108325 A1	05-2008	AHN et al.	455/411
*	F	US-7,457,412 B2	11-2008	England et al.	380/44
*	G	US-2009/0063865 A1	03-2009	Berenbaum et al.	713/180
*	H	US-2009/0086981 A1	04-2009	Kumar et al.	380/285
*	I	US-7,546,447 B2	06-2009	Chen et al.	713/1
*	J	US-2009/0172639 A1	07-2009	Natu et al.	717/120
*	K	US-2009/0193211 A1	07-2009	Hu et al.	711/163
*	L	US-2009/0241103 A1	09-2009	Pennisi et al.	717/173
*	M	US-7,676,840 B2	03-2010	Morais et al.	726/21

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 12/355,900	Applicant(s)/Patent Under Reexamination GRELL ET AL.	
	Examiner JAWEED A. ABBASZADEH	Art Unit 2115	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2010/0082955 A1	04-2010	Chhabra et al.	713/1
*	B	US-7,770,165 B2	08-2010	Olson et al.	717/168
*	C	US-7,937,575 B2	05-2011	Hajji et al.	713/1
*	D	US-7,962,737 B2	06-2011	Lo, Yuan-Chang	713/2
*	E	US-8,006,095 B2	08-2011	Berenbaum et al.	713/180
*	F	US-2005/0216753	09-2005	Dailey et al.	713/191
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	**Art Unit**
	JAWEED A ABBASZADEH	2115

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/10/2011								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	O								
	8	O								
	9	O								
	10	O								
	11	O								
	12	O								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	✓								
	20	✓								
	21	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

SEARCHED			
Class	Subclass	Date	Examiner
713	1, 2	10/10/2011	JA
713	176	10/10/2011	JA

SEARCH NOTES		
Search Notes	Date	Examiner
Performed EAST search, see results attached	8/29/2011	JA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4703	(713/176).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 21:40
L2	447	(boot$3 and 1)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 21:42
L3	109	(boot$3 with (bios or firmware)) and 1	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 21:42
S1	22	(michael near2 grell) or (findeisen near2 ralf) or (frank near2 schuecke)	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 10:23
S2	149	(cpu or processor) near4 key with boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 10:29
S3	119	S2 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 10:29
S4	579	boot$3 near4 signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 16:07
S5	91	boot$3 near4 signature with (processor or cpu)	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 16:07
S6	82	S5 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/08/29 16:08
S7	451	(cpu or processor) near4 key with signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 14:34
S8	15	S7.ab.	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 14:35
S9	586	signature near4 (processor or cpu) with (match$3 or compar$3)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 15:06

S10	397	signature near4 (processor or cpu) near5 (match$3 or compar$3)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 15:07
S11	3	signature near4 (processor or cpu) near5 (match$3 or compar$3) same boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 15:07
S12	53	secure$2 near3 boot$3 with signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 15:11
S13	32	S12 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 15:12
S14	101	signature near4 (match$3 or compar$3) with boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 17:33
S15	85	S14 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/01 17:33
S16	678	key near3 stored near3 (processor or cpu)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 13:55
S17	237	key near3 stored near3 (processor or cpu) and signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 13:56
S18	24	key near3 stored near3 (processor or cpu) and signature.ab.	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 13:56
S19	21	S18 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 13:56
S20	41	key near3 stored near3 (processor or cpu) same signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 14:09
S21	31	S20 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 14:09
S22	78	key near4 stored near4 (processor or cpu) same signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 14:09
S23	63	S22 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 14:09
S24	18	restrict$3 near4 key with (boot$3 or initializ$5)	US-PGPUB; USPAT;	OR	OFF	2011/09/02 15:24

			EPO			
S25	13	S24 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:24
S26	259	lock$3 near4 key with (boot$3 or initializ$5)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:30
S27	21	access$3 near4 key with (boot$3 or initializ$5) near3 (before or after)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:38
S28	1	restrict$3 near4 key near4 compromis$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:43
S29	140	restrict$3 near4 key same signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:44
S30	116	S29 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:44
S31	79	(before or prior) adj3 (boot$3 or initializ$5) near4 key	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:58
S32	66	S31 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:58
S33	4	(before or prior) adj3 (boot$3 or initializ$5) near4 (encryption adj key)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 15:59
S34	8	(before or prior) adj3 (boot$3 or initializ$5) with (encryption adj key)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 16:14
S35	4	S34 not S33	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/02 16:14
S36	1431	(updat$3 or upgrad$3) with (encryption adj key)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/08 17:21
S37	113	S36.ab.	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/08 17:21
S38	89	S37 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/08 17:21
S39	58	prevent$3 near2 access near3 (encryption	US-	OR	OFF	2011/09/08

		adj key)	PGPUB; USPAT; EPO			17:42
S40	46	S39 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/08 17:43
S41	3	(symmetric adj encryption adj key) with boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:14
S42	4	encryption adj key near3 lock$3 near4 (before or after)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:18
S43	3	encryption adj key near3 lock$3 near4 (boot$3)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:22
S44	3	encryption adj key near3 lock$3 with (boot$3)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:22
S45	3	encryption adj key near5 lock$3 with (boot$3)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:22
S46	37	encryption adj key near3 secure near4 (after or before)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:23
S47	27	S46 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:23
S48	1	("20090086981").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 09:46
S49	26	(updat$3 or upgrad$3) near3 bios with signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 11:27
S50	579	(updat$3 or upgrad$3) with ((creat$3 or generat$3) near2 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 11:39
S51	4	(updat$3 or upgrad$3) with ((creat$3 or generat$3) near2 signature) same boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 11:40
S52	21	(updat$3 or upgrad$3) with ((creat$3 or generat$3) near2 signature) same initializ$5	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 11:46
S53	562	(updat$3 or upgrad$3) with ((new) near2 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:41

S54	202	(updat$3 or upgrad$3) with ((new) adj signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:41
S55	171	S54 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:43
S56	86	(updated or upgraded) with (determin$3 near3 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:50
S57	68	S56 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:50
S58	132	(updated or upgraded) with (calculat$3 near3 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:52
S59	56	(updated or upgraded) with (calculat$3 near2 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:52
S60	47	S59 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 16:52
S61	24	(upgrad$3 or updat$3) near2 (firmware or bios) same ((calculat$3 or generat$3) near2 signature)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/09 17:25
S62	1	(11/467432).APP.	USPAT; USOCR	OR	OFF	2011/09/10 12:17
S63	31	("20020091807" | "20050132351" | "20050235015" | "20060136517" | "20070073747" | "5588143" | "5623604" | "5909689" | "6094684" | "6324544" | "6343315" | "6356949" | "6357021" | "6622302" | "6640334" | "6708231" | "6742176" | "6754895" | "6907602" | "7043664" | "7085957" | "7093244" | "7146609" | "7281132" | "7421468" | "7434216" | "7437405" | "7480907" | "7600224" | "7614098" | "7676803").PN. OR ("7770165").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/09/10 12:17
S64	192	(upgrad$3 or updat$3) near2 (firmware or bios) same signature	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/10 12:37
S65	75	(upgrad$3 or updat$3) near2 (firmware or bios) same signature same key	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/10 12:37
S66	59	S65 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/10 12:37
S67	1166	(protect$3) near3 (encryption adj key)	US-	OR	OFF	2011/09/11

			PGPUB; USPAT; EPO			14:37
S68	14	(protect$3) near3 (encryption adj key) near3 (cpu or processor)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/11 14:38
S69	20	(protect$3) near3 (encryption adj key) near6 (cpu or processor)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/11 14:38
S70	20	(protect$3) near3 (encryption adj key) near6 (cpu or processor)	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/11 14:39
S71	4	encryption adj key near4 tamper$3 with boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 09:53
S72	40	("20010033012" | "20020166061" | "20020199111" | "20030005323" | "20030018892" | "20030046238" | "20040243797" | "20050005108" | "20050081048" | "20070079043" | "4593384" | "5022077" | "5150412" | "5325532" | "5457748" | "5877547" | "5880523" | "5930110" | "5935242" | "6105136" | "6128694" | "6181803" | "6237098" | "6246967" | "6292899" | "6473861" | "6567787" | "6775778" | "6782479" | "6836847" | "6942573" | "6975204" | "7188282" | "7228440").PN. OR ("7343496").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/09/12 09:54
S73	78	key near4 tamper$3 with boot$3	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 10:19
S74	76	S73 not S71	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 10:19
S75	72	S74 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 10:19
S76	6	("20030028761" | "20040003288" | "20050149729" | "6185678" | "6745329").PN. OR ("7546447").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/09/12 10:58
S77	496	(updated or upgraded) with (signature) with key	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 11:21
S78	19	S77.ab.	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 11:21
S79	49	S77.clm.	US-PGPUB; USPAT;	OR	OFF	2011/09/12 11:55

			EPO			
S80	42	S79 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/09/12 11:55
S81	1	("20090276617").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 13:35
S82	1	("20090086981").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 13:54
S83	0	(11/864887).APP.	USPAT; USOCR	OR	ON	2011/10/10 15:57
S84	1	("7073064").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 15:57
S85	62	boot adj code near3 internal	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 15:59
S86	55	S85 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 15:59
S87	36	authentication adj code near3 internal	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 16:21
S88	1	("20090063799").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:18
S89	1	("7917176").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:19
S90	1	("7546447").PN.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:20
S91	197	(updat$3 or upgrad$3) near3 firmware near4 reset$4	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:32
S92	150	S91 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:32
S93	382	(updat$3 or upgrad$3) near3 firmware near4 check$3	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:32
S94	4471	(713/1).CCLS.	US-PGPUB; USPAT;	OR	OFF	2011/10/10 17:33

			EPO			
S95	4479	(713/2).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:33
S96	7375	S94 or S95	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:33
S97	35	S96 and S93	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:33
S98	5	(updat$3 or upgrad$3) near3 firmware with preboot	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:42
S99	612	(updat$3 or upgrad$3) near3 firmware with boot$3	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:45
S100	42	S99.ab.	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:45
S101	37	S100 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:45
S102	152	(updat$3 or upgrad$3) near3 firmware with lock$3	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 17:59
S103	140	S102 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 17:59
S104	3	(updat$3 or upgrad$3) near3 firmware with lock$3 near3 key	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 18:08
S105	12	(updat$3 or upgrad$3) near3 firmware same lock$3 near3 key	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 18:09
S106	28	(updat$3 or upgrad$3) near3 firmware with pre-boot	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 18:11
S107	22	updated near2 (firmware or bios) with signature	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:18
S108	15	S107 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 20:18
S109	68	updated near2 (firmware or bios) with	US-	OR	ON	2011/10/10

		sign$3	PGPUB; USPAT; EPO			20:20
S110	54	S109 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	OFF	2011/10/10 20:20
S111	54	S109 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:20
S112	0	updat$3 near2 (firmware or bios) with (new adj2 signature)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:23
S113	0	(updat$3 or upgrad$3) near2 (firmware or bios) with (new adj2 signature)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:24
S114	100	(updat$3 or upgrad$3) near2 (firmware or bios) with (signed or signing)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:24
S115	77	S114 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:24
S116	504	updat$3 near4 (digital adj signature)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:26
S117	26	S116.ab.	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:26
S118	37	updat$3 near4 (digital adj signature) with (firmware or bios)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:33
S119	2433	internal near3 (volatile adj memory)	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:53
S120	98	internal near3 (volatile adj memory) with cpu	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:53
S121	66	S120 and @ad<"20080430"	US-PGPUB; USPAT; EPO	OR	ON	2011/10/10 20:53

EAST Search History (Interference)

<This search history is empty>

10/10/2011 9:44:15 PM
C:\Users\jabbaszadeh\Documents\CASES\12355900\search.wsp

Form PTO-1449 (modified)	Atty. Docket No. 2000.162700/DE0892	Serial No. 12/355,900
List of Patents and Publications for Applicant's INFORMATION DISCLOSURE STATEMENT (Use several sheets if necessary)	**Applicant** Michael Grell, Ralf Findeisen and Frank Schuecke	
	Filing Date: January 19, 2009	**Group:** Unknown

U.S. Patent Documents	Foreign Patent Documents	Other Art
See Page 1	*See Page 1*	*See Page 1*

U.S. Patent Documents

Exam. Init.	Ref. Des.	Document Number	Date	Name	Class	Sub Class	Filing Date of App.
	A1						
	A2						
	A3						
	A4						
	A5						

Foreign Patent Documents

Exam. Init.	Ref. Des.	Document Number	Date	Country	Class	Sub Class	Translation Yes/No
	B1	WO 2006/086301 A1	8/17/06	PCT	G06F	12/02	Yes
	B2						
	B3						

Other Art (Including Author, Title, Date Pertinent Pages, Etc.)

Exam. Init.	Ref. Des.	Citation
	C1	Translation of Official Communication from German Patent Office for German Patent Application No. 10 2008 021 567.8-53 dated November 12, 2008.
	C2	
	C3	

EXAMINER:	/Jaweed Abbaszadeh/	DATE CONSIDERED:	08/29/2011

EXAMINER: INITIAL IF REFERENCE CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED. INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7735

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/355,900	01/19/2009	713	2115	2162.162700/DE0892

APPLICANTS

Michael Grell, Dresden, GERMANY;
Ralf Findeisen, Dresden, GERMANY;
Frank Schuecke, Dresden, GERMANY;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

GERMANY 10 2008 021 567.8 04/30/2008

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

02/03/2009

Foreign Priority claimed ☑ Yes ☐ No 35 USC 119(a-d) conditions met ☑ Yes ☐ No Verified and Acknowledged /JAWEED A ABBASZADEH/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		GERMANY	7	21	4

ADDRESS

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042
UNITED STATES

TITLE

COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

FILING FEE RECEIVED		
1362	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Group Art Unit: 2115 Examiner: JAWEED A. ABBASZADEH
Serial No.: 12/355,900	Conf. No.: 7735
Filed: January 19, 2009	Atty. Docket: 2162.162700/DE0892
For: **METAL CAP LAYER OF INCREASED ELECTRODE POTENTIAL FOR COPPER-BASED METAL REGIONS IN SEMICONDUCTOR DEVICES**	CUSTOMER NO.: 10742

RESPONSE TO OFFICE ACTION DATED OCTOBER 17, 2011

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is submitted in response to the Office Action mailed October 17, 2011, for which the shortened three-month statutory response date is January 17, 2012. This response is being filed on or before the due date, therefore, it is timely filed.

If an extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, this paper is to be construed as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

The Commissioner is authorized to deduct the fee ($250) for one additional independent claim (Claim 7, as amended) from Williams, Morgan & Amerson, P.C.'s Deposit Account No. 50-0786/2162.162700. No other fee is believed due as a result of the response contained herein. However, should any other fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason, the

Commissioner is authorized to deduct said fees from Williams, Morgan & Amerson, P.C.'s Deposit Account No. 50-0786/2162.162700.

IN THE CLAIMS

1. (Original) A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

2. (Original) The method of claim 1, wherein executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory.

3. (Original) The method of claim 2, wherein executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data.

4. (Original) The method of claim 2, wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache.

5. (Original) The method of claim 1, further comprising locking said encryption key for external access prior to executing said boot instructions.

6. (Original) The method of claim 5, further comprising determining whether an upgrade version of said boot data is available.

7. (Currently Amended) A method for booting a computer system, the method comprising: ~~The method of claim 6~~

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key;

locking said encryption key for external access prior to executing said boot instructions;

determining whether an upgrade version of said boot data is available, wherein determining whether an upgrade version of said boot data is available is performed prior to locking said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

8. (Original) The method of claim 7, further comprising verifying said upgrade version of said boot data.

9. (Original) The method of claim 8, further comprising calculating a new signature over a hash sum of said upgrade version of the boot data using said encryption key and adding said new signature to said upgrade version of the boot data.

10. (Original) The method of claim 9, further comprising enabling said upgrade version of said boot data.

11. (Original) The method of claim 10, further comprising generating a reset event.

12. (Original) The method of claim 10, further comprising locking said encryption key prior to enabling said upgrade version of the boot data.

13. (Original) A method for booting a computer system, the method comprising:

upon at least one of a power-up event and a reset event, accessing an internal non-volatile memory of a central processing unit, said internal non-volatile memory containing pre-boot instructions and data values for initializing an internal volatile memory

of said central processing unit and verifying an integrity of at least a portion of boot instructions and boot data values;

loading said at least a portion of said boot instructions and boot data values from a non-volatile memory into said internal volatile memory by executing said pre-boot instructions;

verifying integrity of said at least a portion of said boot instructions and boot data values by using an encryption key stored in said internal non-volatile memory and a signature associated with said at least a portion of said boot instructions and boot data values, said signature being formed on the basis of said encryption key;

after successfully verifying integrity of said at least a portion of said boot instructions and boot data values, determining whether an upgrade version of said boot instructions and boot data values is available; and

when an upgrade version is available, generating a signature of said upgrade version by using said encryption key.

14. (Original) The method of claim 13, wherein executing said boot instructions comprises initializing a system memory of said computer system and loading a second portion of boot instructions and boot data values into said system memory.

15. (Original) The method of claim 14, further comprising verifying integrity of said second portion and continuing booting of said computer system on the basis of said second portion when verification of said second portion is successful.

16. (Original) The method of claim 13, wherein initializing said volatile internal memory comprises initializing a data cache of said central processing unit and wherein said at least a portion is loaded into said data cache and is verified therein.

17. (Original) The method of claim 13, further comprising locking said encryption key prior to executing said boot instructions when an upgrade version is not available.

18. (Original) The method of claim 13, further comprising verifying said upgrade version of the boot instructions and boot data prior to generating said new signature.

19. (Original) A central processing unit (CPU), comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key.

20. (Original) The central processing unit of claim 19, further comprising a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power-on event only.

21. (Original) A computer system, comprising:

a central processing unit comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory, and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key; and

a non-volatile boot memory configured to hold at least said boot routine and a second boot routine.

REMARKS

Pursuant to the present response, claim 7 has been amended. Thus, claims 1-21 are pending in the present application. No new matter has been introduced by way of the present response and amendment. Reconsideration of the present application is respectfully requested in view of the arguments and amendments set forth herein.

Allowable Subject Matter

Applicants acknowledge and appreciate the Examiner's indication of allowable subject matter. In the Office Action, the Examiner indicated that claims 13-18 were allowable, and that claims 7-12 were objected to, but would be allowable if rewritten in independent form. Applicants have rewritten claim 7 in independent form and respectfully submit that claim 7, and its dependent claims, are allowable.

Prior Art Rejections

In the Office Action, the Examiner rejected claims 1-4, 19 and 21 under 35 U.S.C. §102(b) as being anticipated by US 2006/0112266 ***(Little)***. The Examiner rejected claims 5 and 20 under 35 U.S.C. §103(a) as being unpatentable over ***Little*** in view of US 7,546,447 ***(Chen)***. The Examiner rejected claim 6 under 35 U.S.C. §103(a) as being unpatentable over ***Little*** in view of ***Chen*** as applied to claim 5, and further in view of US 2005/0216753 ***(Dailey)***. Applicants respectfully traverse the Examiner's rejections.

Legal Standards

As the Examiner well knows, an anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). To the extent the Examiner relies on principles of inherency in making the anticipation rejections in the Office Action, inherency

requires that the asserted proposition necessarily flow from the disclosure. *In re Oelrich*, 212 U.S.P.Q. 323, 326 (C.C.P.A. 1981); *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1463-64 (Bd. Pat. App. & Int. 1990); *Ex parte Skinner*, 2 U.S.P.Q.2d 1788, 1789 (Bd. Pat. App. & Int. 1987); *In re King*, 231 U.S.P.Q. 136, 138 (Fed. Cir. 1986). It is not enough that a reference could have, should have, or would have been used as the claimed invention. "The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Oelrich*, at 326, quoting *Hansgirg v. Kemmer*, 40 U.S.P.Q. 665, 667 (C.C.P.A. 1939); *In re Rijckaert*, 28 U.S.P.Q.2d 1955, 1957 (Fed. Cir. 1993), quoting *Oelrich*, at 326; see also *Skinner*, at 1789. "Inherency … may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Skinner*, at 1789, citing *Oelrich*. Where anticipation is found through inherency, the Office's burden of establishing prima facie anticipation includes the burden of providing "…some evidence or scientific reasoning to establish the reasonableness of the examiner's belief that the functional limitation is an inherent characteristic of the prior art." *Skinner* at 1789.

Moreover, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination must not be based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). With respect to alleged obviousness, it is necessary for the Examiner to identify the reason why a person of ordinary skill in the art would have combined the prior art in the manner claimed. The mere fact

that the prior art can be combined or modified does not make the resultant combination obvious. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990).

The Federal Circuit has made it clear that, in an obviousness analysis, conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1434 (Fed. Cir. 2002). Under this controlling legal standard, it is respectfully submitted that any attempt to assert that the inventions defined by the presently pending claims would have been obvious in view of the prior art of record constitutes an impermissible use of hindsight using Applicants' disclosure as a roadmap.

Analysis and Argument

Claim 1

Applicants respectfully disagree with the Examiner's reading of ***Little*** and submit that ***Little*** fails to teach at least one of the features of pending claim 1. More specifically, relative to pending claim 1, Applicants respectfully submit that ***Little*** fails to disclose, at least, the claimed feature of determining a current signature of at least a signed portion of boot data, where the signed portion of boot data contains a stored signature of the portion of boot data, where the stored signature is created by applying the encryption key (hereinafter referred to as the "Created Signature" limitation). As discussed more fully below, Applicants believe that all pending claims are in condition for allowance.

In the Office Action, the Examiner argued that ***Little*** teaches the Created Signature limitation because ***Little*** allegedly describes a public key used to authenticate a program stored externally to a processor. *See* Office Action, pp. 2-3. That is, the Examiner argued that the public key described in ***Little*** corresponds to the encryption key, as recited in claim 1. Applicants respectfully disagree. ***Little*** teaches that a public key may be stored in a ROM that is

internal to a processor, and that the public key may be used to authenticate external programs. ***Little***, ¶¶[0030]-[0033]. ***Little***, however, is silent with respect to the stored signature being created by applying the encryption key. ***Little*** neither teaches nor suggests that a digital signature residing in an externally stored program is created by applying the shared key. ***Little*** teaches that "[t]he program software residing in external memory **116** may be authenticated in any conventional fashion, for example using a digital signature verification system such as 'RSA,' or any other suitable system, and preferably using a public key stored in the internal ROM 19." ***Little***, ¶[0032]. In other words, ***Little*** describes *authenticating* the digital signature using the public key, but not *creating* the digital signature using the public key. In fact, as understood by the undersigned, ***Little*** does not describe the creation of digital signatures at all. As is known in the art, digital signature verification uses public keys for *authenticating*, but uses private keys for *creating* digital signatures. The Examiner argued that the public key of ***Little*** corresponds to the claimed feature of the encryption key used to create the stored signature of claim 1. Such a position, however, is untenable for at least the reasons given above. As such, ***Little*** does not teach at least the claimed Created Signature feature described above.

For at least the aforementioned reasons, claim 1 and its dependent claims are allowable. These arguments may be similarly applied to independent claims 19 and 21, thus for similar reasons, the remaining rejected claims are also allowable.

As to any remaining anticipation and/or obviousness rejections in the Office Action, none of the additional arguments or prior art identified by the Examiner cures the fundamental deficiencies in ***Little***, as noted above. Accordingly, Applicants respectfully request that all of the rejections set forth in the Office Action should be withdrawn for claims 1, 19 and 21 (and their respective dependent claims).

CONCLUSION

Applicants respectfully assert that in light of the amendments and arguments provided throughout the prosecution of the present application, all claims of the present application are now allowable and, therefore, request that a Notice of Allowance be issued. Reconsideration of the present application is respectfully requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is respectfully requested to call the undersigned attorney at the Houston, Texas telephone number (713) 934-4093 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 10742

Date: January 17, 2012

By: /Nathan E. Black/
Nathan E. Black Reg. No. 66,191
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4093
(713) 934-7011 (facsimile)

ATTORNEY FOR APPLICANT(S)

Electronic Patent Application Fee Transmittal

Application Number:	12355900
Filing Date:	19-Jan-2009
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Filer:	Nathan Eldon Black/Nancy Nolan
Attorney Docket Number:	2162.162700/DE0892

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Independent claims in excess of 3	1201	1	250	250
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**250**

Electronic Acknowledgement Receipt

EFS ID:	11850964
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	Nathan Eldon Black/Nancy Nolan
Filer Authorized By:	Nathan Eldon Black
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	17-JAN-2012
Filing Date:	19-JAN-2009
Time Stamp:	15:21:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$250
RAM confirmation Number	2183
Deposit Account	500786
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Amendment.pdf	135899 29f0c1aab8f843434ad79826539eac96209cfb48	no	13
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30501 976b4d3365ec3d0deff32f4977942d75e9510b31	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	166400		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/355,900	01/19/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT	01/17/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $ =		OR	X $60=	0
	Independent (37 CFR 1.16(h))	* 5	Minus	***4	= 1	X $ =		OR	X $250=	250
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	250

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/LAJUAN HICKSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

10742 7590 03/20/2012

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

EXAMINER	
ABBASZADEH, JAWEED A	
ART UNIT	PAPER NUMBER
2115	

MAIL DATE	DELIVERY MODE
03/20/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	12/355,900	GRELL ET AL.	
	Examiner	Art Unit	
	JAWEED A. ABBASZADEH	2115	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/17/2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-12 and 19-21* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-21 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 and 19-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320.

As to claim 1, Bhatt teaches a method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit [Fig. 2, execute verification code on reset 205, 0024—"verification code from boot storage 130" Boot storage 130 is located on the processor package as shown in Fig. 1], said internal non-volatile memory area containing an encryption key [0025—"Any now known or later developed hashing…or similar algorithm...may be stored in boot storage 130" A signature is determined using the key in boot storage. Once again, boot storage 130 is located on the processor package.];

determining a current signature of at least a signed portion of boot data [0027—"the verification code executed by processor 120 may compute a signature of the boot code 180"], said signed portion of boot data containing a stored signature of said portion

of boot data [0027—"signature value from ID storage"], said stored signature created by applying said encryption key [0025—"Any now known or later developed hashing…or similar algorithm...may be stored in boot storage 130 and used in act 225" Act 225 initially computed the signature of the boot code and stored it.]; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical [0028—"If the computed signature from act 245 matches the corresponding signature value from ID storage 140 [act 250], processor 120 the verification code executed by processor 120 may permit further booting from boot code 180 in external memory 160 [act 255]."

As to claim 2, Bhatt teaches executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory [0028—It is well known in the art that booting involves loading data from non-volatile memory into RAM].

As to claim 3, Bhatt teaches executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data [0028].

As to claim 4, Bhatt teaches teaches wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into

said data cache [0028—It is well known in the art that booting involves loading boot data into cache in order for it to be executed by the processor].

As to claim 19, Bhatt teaches this claim according to the reasoning set forth in claim 1 supra.

As to claim 21, Bhatt teaches this claim according to the reasoning set forth in claim 1 supra.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320 in view of Tugenberg et al. (hereinafter 'Tugenberg') US 7,103,782.

As to claims 5, Bhatt teaches the method of claim 1, but does not teach locking said encryption key for external access prior to executing said boot instructions.

Tugenberg is cited to teach a method that utilizes an encryption key stored in secure memory. Tugenberg further teaches locking said encryption key for external access prior to executing said boot instructions [Fig. 3]. When blocking gates are enabled in step 314, the encryption key is "locked." It would have been obvious to one

of ordinary skill in the art to have combined the teachings of Bhatt and Tugenberg because they are both directed towards utilizing an encryption key. Tugenberg improves upon Bhatt because Tugenberg's system is more secure. It prevents access to the encryption key when access is not needed [col. 8, lines 4-5].

As to claim 20, Tugenberg teaches this claim according to the reasoning set forth in claim 5 supra.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320 in view of Tugenberg et al. (hereinafter 'Tugenberg') US 7,103,782 as applied to claim 5 above, and further in view of Aguilar et al. (hereinafter 'Aguilar') US 6,892,297.

As to claim 6, Bhatt and Tugenberg teach the method of claim 5, but do not teach determining whether an upgrade version of said boot data is available.

Aguilar teaches determining whether an upgrade version of said boot data is available [col. 4, lines 19-27]. It would have been obvious to one of ordinary skill in the art to have combined the teachings of Aguilar with those of Bhatt and Tugenberg because Aguilar improves upon Bhatt and Tugenberg. By checking for an update of the boot code, Aguilar's teachings ensure that the version of the boot code is the correct version required by the operating system [col. 1, lines 52-55]

Claim 7-12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320 in view of Tugenberg et al. (hereinafter 'Tugenberg') US 7,103,782 and Aguilar et al. (hereinafter 'Aguilar') US 6,892,297.

As to claim 7, Bhatt, Tugenberg, and Aguilar teach this claim according to the reasoning set forth in claims 1 and 6-7 supra.

As to claims 8-12, Bhatt, Tugenberg, and Aguilar teach these claims according to the reasoning set forth supra.

Allowable Subject Matter

Claims 13-18 are allowed.

Response to Arguments

Applicant's arguments with respect to claims 1-12 and 19-21 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAWEED A. ABBASZADEH whose telephone number is (571)270-1640. The examiner can normally be reached on Mon-Fri: 8:30 a.m.-6:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas C. Lee can be reached on (571) 272-3667. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAWEED A ABBASZADEH/
Examiner, Art Unit 2115
3/18/12

Notice of References Cited	Application/Control No. 12/355,900	Applicant(s)/Patent Under Reexamination GRELL ET AL.	
	Examiner JAWEED A. ABBASZADEH	Art Unit 2115	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0078338 A1	06-2002	Lay et al.	713/2
*	B	US-6,539,456 B2	03-2003	Stewart, David C.	711/113
*	C	US-6,892,297 B1	05-2005	Aguilar et al.	713/2
*	D	US-6,959,331 B1	10-2005	Traversat et al.	709/222
*	E	US-7,036,040 B2	04-2006	Nicholson et al.	714/6.31
*	F	US-7,103,782 B1	09-2006	Tugenberg et al.	713/194
*	G	US-7,454,653 B2	11-2008	Nicholson et al.	714/47.2
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

SEARCHED			
Class	Subclass	Date	Examiner
713	1, 2	10/10/2011	JA
713	176	10/10/2011	JA

SEARCH NOTES		
Search Notes	Date	Examiner
Performed EAST search, see results attached	8/29/2011	JA
Updated EAST search, see results attached	3/13/2012	JA
Performed Google Patents search, see results attached	3/13/2012	JA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

+You Search Images Maps YouTube News Gmail Documents Calendar More

boot compute signature

Sign in

Search About 13,600 results (0.33 seconds)

Did you mean: boot *computer* signature

Everything
Images
Maps
Videos
News
Shopping
Patents
More

Any date
Restrict by filing date
Restrict by issue date

Any filing status
Applications
Issued patents

Any patent type
Utility
Design
Plant
Defensive Publication
Additional Improvement
Statutory Invention Registration

List view
Grid view

Sorted by relevance
Filing date: latest
Filing date: oldest

SYSTEM AND METHOD FOR OPERATING SYSTEM INSTALLATION ON A DISKLESS ...



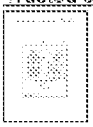
www.google.com/patents/US20080028052
US Pat. App 11456850 - Filed Jul 25, 2006
Amethod for performing a **boot** operation for a diskless **computing** device, the method comprising: **computing** a **signature** value that indicates a hardware ...
Overview - Abstract - Drawing - Description - Claims

Secure **boot** scheme from external memory using internal memory



www.google.com/patents/US20060107320
US Pat. App 10988913 - Filed Nov 15, 2004
[0025] Optionally, if processor 120 has retrieved a portion of **boot** code 180 in act 210, processor 120 may **compute** a cryptographic hash or digital **signature** ...
Overview - Abstract - Drawing - Description - Claims

Trusted component update system and method



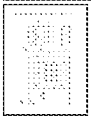
www.google.com/patents/US20080256363
US Pat. App 11780874 - Filed Apr 13, 2007
Hash logic 104 and hash value 105 are stored in **boot** block 102, ... verify logic 111 to independently **calculate** certain portions of a digital **signature** 115 ...
Overview - Abstract - Drawing - Description - Claims

Updating A Basic Input/Output System ('BIOS') **Boot** Block Security ...



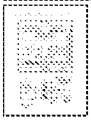
www.google.com/patents/US20090327686
US Pat. App 12116633 - Filed May 9, 2008 - INTERNATIONAL BUSINESS MACHINES CORPORATION
[0031] For each **compute** node in such a multinode computer, ... area (210) of flash memory (134) of the **compute** node and verifying a digital **signature** (214) ...
Overview - Abstract - Drawing - Description - Claims

ELECTRONIC DEVICE **BOOTED** UP WITH SECURITY, A HASH **COMPUTING** ...



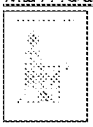
www.google.com/patents/US20090144559
US Pat. App 12249295 - Filed Oct 10, 2008 - Samsung Electronics Co., Ltd
[0025] The **boot** code of the first memory includes command codes that enable the processor to **calculate** a hash value of the **boot** code of the first memory if ...
Overview - Abstract - Drawing - Description - Claims

Master **boot** record management



www.google.com/patents/US20080184022
US Pat. App 11699252 - Filed Jan 29, 2007
The method of claim 1, wherein comparing a first identifier derived from a master **boot** record of the **computing** device with a second identifier stored in a ...
Overview - Abstract - Drawing - Description - Claims

METHODS AND SYSTEMS FOR PROVIDING SECURE IMAGE MOBILITY



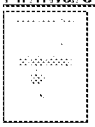
www.google.com/patents/US20100235833
US Pat. App 12403742 - Filed Mar 13, 2009 - LIQUID COMPUTING CORPORATION
[0110] Secure Virtual Server **Boot** [0111] Each of the set of virtual server ... and the Secure **Compute** Host 102 may be protected by a digital **signature** based ...
Overview - Abstract - Drawing - Description - Claims

Systems and methods for detecting tampering of a computer system ...



www.google.com/patents/US20050039049
US Pat. App 9765342 - Filed Jan 19, 2001
In one example, the **boot signature** checker monitors the bus connecting the ... SIGNAL SEQUENCER III **CALCULATE BOOT SIGNATURE BOOT SIGNATURE** IS EXPECTED **BOOT** ...
Overview - Abstract - Drawing - Description - Claims

Firmware Verified **Boot**



www.google.com/patents/US20110087872
US Pat. App. 12/903,202 - Filed Oct 12, 2010
In the **boot** process of the second general aspect, the **computing** system halts the **boot** process if the verification of the encrypted **signature** corresponding ...
Overview - Abstract - Drawing - Description - Claims

Multi-level **boot** hierarchy for software development on an ...



www.google.com/patents/US7783886
US Pat. 7783886 - Filed Jan 13, 2004 - Issued Aug 24, 2010 - Silverbrook Research Pty Ltd
The time taken to **calculate** and compare **signatures** must be independent of data content. 35 To update ChipU' s Pw: a. System calls ChipU's Random function; ...
Overview - Abstract - Drawing - Description - Claims

1 2 3 4 5 6 7 8 9 10 Next

Advanced search Search Help Give us feedback

Google Home Advertising Programs Business Solutions Privacy About Google

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/10/2011	03/18/2012							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	O	✓							
	8	O	✓							
	9	O	✓							
	10	O	✓							
	11	O	✓							
	12	O	✓							
	13	=	=							
	14	=	=							
	15	=	=							
	16	=	=							
	17	=	=							
	18	=	=							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("7836293").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/13 17:08
S2	1	(boot adj sector) near3 cached	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/13 17:35
S3	0	(boot adj sector) near4 caching	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/13 17:41
S4	4	(boot adj sector) near4 cach$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/13 17:41
S5	59	("5307497" | "6061788" | "6073232" | "6172936" | "6189100" | "6226740").PN. OR ("6539456").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/13 17:46
S6	0	(boot adj block) near3 cached	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:08
S7	0	(boot adj block) near3 caching	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:08
S8	0	(boot adj block) near4 caching	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:08
S9	6	(boot adj code) near4 caching	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:08

S10	3	(boot adj sector) near4 cache	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:09
S11	53	("6539456").URPN.	USPAT	OR	OFF	2012/03/14 10:12
S12	541	("20010031092" | "20010032128" | "20010047473" | "20010052038" | "20010054131" | "20020037035" | "20020069354" | "20020080871" | "20020097172" | "20020101367" | "20020104891" | "20020126755" | "20020191692" | "20030030575" | "20030034905" | "20030084238" | "20030090397" | "20030142874" | "20030191876" | "20040042506" | "20040056783" | "20040073710" | "20040073746" | "20060015650" | "20060181441" | "20060181442" | "20060184687" | "20060184696" | "20060190644" | "20060195601" | "20070043939" | "20070050514" | "20070050515" | "20070067483" | "20070083746" | "20070109154" | "20070109155" | "20070109156" | "20070174209" | "20080232457" | "20090154545" | "20090287839" | "20100316114" | "20100318684" | "20100332700" | "20110037626" | "20110199243" | "20110208833" | "3394352" | "3490690" | "4021782" | "4032893" | "4054951" | "4127518" | "4302775" | "4325085" | "4360840" | "4386416" | "4394774" | "4464650" | "4494108" | "4499499" | "4574351" | "4593324" | "4626829" | "4646061" | "4682150" | "4701745" | "4729020" | "4730348" | "4745559" | "4748638" | "4750135" | "4754351" | "4804959" | "4813040" | "4814746" | "4862167" | "4866601" | "4870415" | "4872009" | "4876541" | "4888812" | "4890282" | "4897717" | "4906991" | "4906995" | "4929946" | "4953324" | "4956808" | "4965675" | "4988998" | "5003307" | "5016009" | "5027376" | "5028922" | "5045848" | "5045852" | "5046027" | "5049881" | "5079630" | "5091782" | "5097261" | "5103306" | "5109226" | "5109433" | "5113522" | "5115309" | "5121342").PN. OR ("5126739" | "5128963" | "5132992" | "5146221" | "5150430" | "5155484" | "5159336" | "5167034" | "5175543" | "5179651" | "5187793" | "5191431" | "5204756" | "5209220" | "5212742" | "5226176" | "5227893" | "5231492" | "5237460" | "5237675" | "5243341" | "5243348" | "5247638" | "5247646" | "5249053" | "5263168" | "5267333" | "5270832" | "5280600" | "5287420" | "5289580" | "5293379" | "5293576" | "5307497" | "5309555" |	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/14 10:12

"5319682" | "5341440" | "5347600" |
"5353132" | "5354315" | "5355498" |
"5357614" | "5367629" | "5373290" |
"5374916" | "5379036" | "5379757" |
"5381145" | "5389922" | "5394534" |
"5396228" | "5400401" | "5403639" |
"5406278" | "5406279" | "5410671" |
"5412384" | "5414850" | "5420639" |
"5434983" | "5437020" | "5452287" |
"5454079" | "5454107" | "5455576" |
"5455578" | "5455680" | "5461679" |
"5463390" | "5467087" | "5471206" |
"5479587" | "5479633" | "5483470" |
"5486826" | "5488364" | "5488365" |
"5495244" | "5504842" | "5506844" |
"5506872" | "5506944" | "5521940" |
"5528628" | "5530845" | "5533051" |
"5535311" | "5535356" | "5535369" |
"5537658" | "5539865" | "5542031" |
"5544290" | "5546395" | "5546475" |
"5553160" | "5557551" | "5557668" |
"5557749" | "5561421" | "5561824" |
"5563961" | "5574952" | "5574953" |
"5576953" | "5577248" | "5581715" |
"5583500" | "5586264" | "5586285" |
"5590306" | "5596674" | "5598388" |
"5604824" | "5606706" | "5610657" |
"5611024" | "5612788" | "5613069" |
"5615017" | "5615287" | "5619995" |
"5621820" | "5623623" | "5623701").PN. OR
("5627534" | "5627995" | "5629732" |
"5630092" | "5635632" | "5635932" |
"5638498" | "5640158" | "5642506" |
"5649032" | "5652795" | "5652857" |
"5652917" | "5654703" | "5655138" |
"5666560" | "5668737" | "5671355" |
"5671389" | "5671413" | "5673370" |
"5675333" | "5675789" | "5686916" |
"5692159" | "5694619" | "5696927" |
"5703793" | "5708511" | "5715477" |
"5717393" | "5717394" | "5719862" |
"5721958" | "5724475" | "5729228" |
"5740395" | "5742773" | "5748904" |
"5757852" | "5764774" | "5765027" |
"5768445" | "5768525" | "5771340" |
"5774715" | "5778411" | "5781767" |
"5784572" | "5787487" | "5794229" |
"5796864" | "5799110" | "5805834" |
"5805932" | "5808660" | "5809176" |
"5809299" | "5809337" | "5812195" |
"5812789" | "5818368" | "5818369" |
"5818530" | "5819215" | "5822781" |
"5825424" | "5825830" | "5832037" |
"5832126" | "5832443" | "5835788" |
"5836003" | "5838821" | "5838927" |
"5838996" | "5839100" | "5841979" |
"5847762" | "5850565" | "5861824" |
"5861920" | "5864342" | "5864678" |
"5867167" | "5867602" | "5870036" |
"5870087" | "5872530" | "5874907" |
"5883975" | "5884269" | "5886655" |
"5887165" | "5889961" | "5892847" |
"5907801" | "5909557" | "5909559" |
"5915079" | "5917438" | "5918068" |

"5918225" | "5920326" | "5923860" |
"5930358" | "5936616" | "5938737" |
"5943692" | "5945933" | "5949355" |
"5949968" | "5951623" | "5955976" |
"5956490" | "5960465" | "5964842" |
"5968149" | "5969927" | "5973630" |
"5974235" | "5974387" | "5974471" |
"5978483" | "5982360").PN. OR ("5982723" |
"5982937" | "5987022" | "5987590" |
"5990884" | "5991515" | "5996033" |
"6000009" | "6002411" | "6003115" |
"6008743" | "6011901" | "6014694" |
"6021433" | "6023755" | "6026217" |
"6028725" | "6031939" | "6032148" |
"6032197" | "6058459" | "6061398" |
"6061473" | "6070179" | "6073232" |
"6075470" | "6078958" | "6091777" |
"6092123" | "6094634" | "6097520" |
"6098114" | "6104389" | "6105130" |
"6115384" | "6128412" | "6134631" |
"6141053" | "6145020" | "6145069" |
"6169241" | "6170007" | "6170047" |
"6170049" | "6172936" | "6173381" |
"6175650" | "6175856" | "6182125" |
"6185625" | "6185659" | "6192082" |
"6192155" | "6195024" | "6195465" |
"6198842" | "6198850" | "6208273" |
"6215904" | "6219754" | "6222886" |
"6225922" | "6226667" | "6226740" |
"6230223" | "6237054" | "6243829" |
"6253264" | "6272178" | "6272627" |
"6272628" | "6282641" | "6285458" |
"6298408" | "6308311" | "6309424" |
"6310563" | "6317714" | "6317818" |
"6330622" | "6333745" | "6345307" |
"6356589" | "6356937" | "6388584" |
"6392567" | "6404931" | "6421387" |
"6434168" | "6434695" | "6442659" |
"6449658" | "6449682" | "6452602" |
"6452933" | "6459429" | "6463509" |
"6487640" | "6489902" | "6505239" |
"6513113" | "6523102" | "6526174" |
"6529633" | "6532121" | "6539438" |
"6539456" | "6542644" | "6577254" |
"6590609" | "6597812" | "6601104" |
"6604040" | "6604158" | "6606040" |
"6606413" | "6609223" | "6618728" |
"6624761" | "6633244" | "6633968" |
"6650261" | "6661839" | "6661845" |
"6704840").PN. OR ("6708220" | "6711709" |
"6717534" | "6731814" | "6745282" |
"6748457" | "6756922" | "6768749" |
"6792151" | "6810434" | "6813689" |
"6819271" | "6822589" | "6856651" |
"6862278" | "6879266" | "6885316" |
"6885319" | "6888893" | "6909383" |
"6944740" | "6952409" | "6959359" |
"6963608" | "6990247" | "6993597" |
"7007099" | "7024460" | "7054493" |
"7069342" | "7089391" | "7102544" |
"7127518" | "7129860" | "7130913" |
"7161506" | "7181608" | "7190284" |
"7319667" | "7321937" | "7330912" |
"7352300" | "7358867" | "7376772" |

		"7378992" | "7386046" | "7395345" | "7400274" | "7415530" | "7417568" | "7552069" | "7565441" | "7714747" | "7777651" | "RE40092").PN. OR ("8090936").URPN.				
S13	6	(fast adj2 boot$3) near6 cach$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/14 10:29
S14	12	("20060288202" | "20080184038" | "5450576" | "5867702" | "6058475" | "6336185" | "6584560" | "6842857" | "7007161" | "7010678").PN. OR ("7836293").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/14 13:46
S15	1	("20060069769").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/15 09:07
S16	1	("20020078338").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/16 11:25
S17	0	cache near3 corrupt with boot$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/16 11:36
S18	85969	("714").CLAS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/16 11:37
S19	206	cache with boot$3 and S18	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/16 11:37
S20	0	(cache near3 corrupt).ab. with boot$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/16 11:37
S21	8	(cache with boot$3).ab. and S18	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/16 11:37
S22	20	("20030037020" | "20030140220" | "5452454" | "5842011" | "5978912" | "6167567" | "6175918" | "6301710" | "6345308" | "6553037" | "6578054").PN. OR ("6959331").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/16 12:17
S23	1	("20100268928").PN.	US-PGPUB; USPAT;	OR	OFF	2012/03/16 12:40

			USOCR			
S24	34	abbaszadeh.xa. and key	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/17 15:18
S25	7	abbaszadeh.xa. and key and encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/17 15:18
S26	279	(update or upgrade) near4 after near3 (verif$6 or authenticat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/17 15:34
S27	162	(update or upgrade) near4 after adj3 (verif$6 or authenticat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/17 15:34
S28	1	("20090276617").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/17 16:02
S29	1	("7103782").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/03/17 16:19
S30	226	(updat$3 near3 (operating adj system)) with boot$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/18 13:43
S31	23	S30.ab.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	OFF	2012/03/18 13:43

EAST Search History (Interference)

< This search history is empty>

3/ 18/ 2012 3:33:25 PM
C:\ Users\ jabbaszadeh\ Documents\ CASES\ 12427052\ amen1.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Group Art Unit: 2115 Examiner: JAWEED A. ABBASZADEH
Serial No.: 12/355,900	Conf. No.: 7735
Filed: January 19, 2009	Atty. Docket: 2162.162700/DE0892 CUSTOMER NO.: 10742

For: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

RESPONSE TO OFFICE ACTION DATED MARCH 20, 2012

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is submitted in response to the Office Action mailed March 20, 2012, for which the shortened three-month statutory response date is June 20, 2012. This response is being filed on or before the due date, therefore, it is timely filed.

If an extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, this paper is to be construed as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

No fee is believed due as a result of the response contained herein. However, should any other fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason, the Commissioner is authorized to deduct said fees from Williams, Morgan & Amerson, P.C.'s Deposit Account No. 50-0786/2162.162700.

AMENDMENT TO THE CLAIMS

1. (Original) A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

2. (Original) The method of claim 1, wherein executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory.

3. (Original) The method of claim 2, wherein executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data.

4. (Original) The method of claim 2, wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache.

5. (Original) The method of claim 1, further comprising locking said encryption key for external access prior to executing said boot instructions.

6. (Original) The method of claim 5, further comprising determining whether an upgrade version of said boot data is available.

7. (Previously Presented) A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key;

locking said encryption key for external access prior to executing said boot instructions;

determining whether an upgrade version of said boot data is available, wherein determining whether an upgrade version of said boot data is available is performed prior to locking said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

8. (Original) The method of claim 7, further comprising verifying said upgrade version of said boot data.

9. (Original) The method of claim 8, further comprising calculating a new signature over a hash sum of said upgrade version of the boot data using said encryption key and adding said new signature to said upgrade version of the boot data.

10. (Original) The method of claim 9, further comprising enabling said upgrade version of said boot data.

11. (Original) The method of claim 10, further comprising generating a reset event.

12. (Original) The method of claim 10, further comprising locking said encryption key prior to enabling said upgrade version of the boot data.

13. (Original) A method for booting a computer system, the method comprising:

upon at least one of a power-up event and a reset event, accessing an internal non-volatile memory of a central processing unit, said internal non-volatile memory containing pre-boot instructions and data values for initializing an internal volatile memory of said central processing unit and verifying an integrity of at least a portion of boot instructions and boot data values;

loading said at least a portion of said boot instructions and boot data values from a non-volatile memory into said internal volatile memory by executing said pre-boot instructions;

verifying integrity of said at least a portion of said boot instructions and boot data values by using an encryption key stored in said internal non-volatile memory and a signature associated with said at least a portion of said boot instructions and boot data values, said signature being formed on the basis of said encryption key;

after successfully verifying integrity of said at least a portion of said boot instructions and boot data values, determining whether an upgrade version of said boot instructions and boot data values is available; and

when an upgrade version is available, generating a signature of said upgrade version by using said encryption key.

14. (Original) The method of claim 13, wherein executing said boot instructions comprises initializing a system memory of said computer system and loading a second portion of boot instructions and boot data values into said system memory.

15. (Original) The method of claim 14, further comprising verifying integrity of said second portion and continuing booting of said computer system on the basis of said second portion when verification of said second portion is successful.

16. (Original) The method of claim 13, wherein initializing said volatile internal memory comprises initializing a data cache of said central processing unit and wherein said at least a portion is loaded into said data cache and is verified therein.

17. (Original) The method of claim 13, further comprising locking said encryption key prior to executing said boot instructions when an upgrade version is not available.

18. (Original) The method of claim 13, further comprising verifying said upgrade version of the boot instructions and boot data prior to generating said new signature.

19. (Original) A central processing unit (CPU), comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key.

20. (Original) The central processing unit of claim 19, further comprising a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power-on event only.

21. (Original) A computer system, comprising:

a central processing unit comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory, and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key; and

a non-volatile boot memory configured to hold at least said boot routine and a second boot routine.

REMARKS

Claims 1-21 are pending in the present application. No new matter has been introduced by way of the present response. Reconsideration of the present application is respectfully requested in view of the arguments set forth herein.

Allowable Subject Matter

Applicants acknowledge and appreciate the Examiner's indication of allowable subject matter. In the Office Action, the Examiner indicated that claims 13-18 were allowable.

Prior Art Rejections

In the Office Action, the Examiner rejected claims 1-4, 19-21 under 35 U.S.C. §102(b) as being anticipated by US 2006/0107320 ***(Bhatt)***. The Examiner rejected claims 5 and 20 under 35 U.S.C. §103(a) as being unpatentable over ***Bhatt*** in view of US 7,103,782 ***(Tugenberg)***. The Examiner rejected claim 6 under 35 U.S.C. §103(a) as being unpatentable over ***Bhatt*** in view of ***Tugenberg,*** as applied to claim 5, and further in view of US 6,892,297 ***(Aguilar)***. Claims 7-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over ***Bhatt*** in view of ***Tugenberg*** and ***Aguilar***. Applicants respectfully traverse the Examiner's rejections.

Analysis and Argument

Claim 1

Applicants respectfully disagree with the Examiner's reading of ***Bhatt*** and submit that ***Bhatt*** fails to teach at least one of the features of pending claim 1. More specifically, relative to pending claim 1, Applicants respectfully submit that ***Bhatt*** fails to disclose, at least, the claimed feature of determining a current signature of at least a signed portion of boot data, where the signed portion of boot data contains a stored signature of the portion of boot data, where the stored signature is created by applying the encryption key (hereinafter referred to as the "Created

Signature" limitation). As discussed more fully below, Applicants believe that all pending claims are in condition for allowance.

In the Office Action, the Examiner argued that ***Bhatt*** teaches the Created Signature limitation because ***Bhatt*** allegedly describes computing a signature of boot code 180 using a hashing or similar algorithm. *See* Office Action, pp. 2-3. That is, the Examiner argued that the secret key *used by* the hashing or similar algorithm in ***Bhatt*** corresponds to the encryption key, as recited in claim 1. Applicants respectfully disagree with the Examiner's reasoning and analysis. ***Bhatt*** teaches that a signature of the boot code 180 can be computed using a hashing or similar algorithm, and that such an algorithm may be stored internally to the processor. *See* ***Bhatt***, ¶[0025]. ***Bhatt***, however, is silent with respect to the secret key (*i.e.*, the claimed encryption key, according to the Examiner) being stored internally to the processor. ***Bhatt*** neither teaches nor suggests that the secret key is stored internally to the processor—***Bhatt*** teaches that the hashing or similar algorithm may be stored internally, and that the algorithm *uses* a secret key, but ***Bhatt*** is silent regarding the secret key being stored internally to the processor. *See* ***Bhatt***, ¶[0025]. In other words, ***Bhatt*** describes *using* a secret key, but not *internally storing* the secret key. To the extent the Examiner relies upon inherency to show such a feature, Applicants respectfully submit that such a position is untenable at least because *internally storing* the secret key does not necessarily flow from the disclosure in ***Bhatt***. *See* Legal Standards section of Applicants January 17, 2012 response. As such, ***Bhatt*** does not teach at least the Created Signature claim feature described above; thus ***Bhatt*** does not anticipate claim 1.

For at least the aforementioned reasons, claim 1 and its dependent claims are allowable. These arguments may be similarly applied to independent claims 19 and 21, thus for similar reasons, the remaining rejected claims are also allowable.

Claim 2

Applicants respectfully disagree with the Examiner's reading of ***Bhatt*** and submit that ***Bhatt*** fails to teach at least one of the features of pending claim 2. More specifically, relative to pending claim 2, Applicants respectfully submit that ***Bhatt*** fails to disclose, at least, the claimed feature of an internal random access memory. In the Office Action, the Examiner argued that ***Bhatt*** allegedly teaches this claimed feature because ***Bhatt*** describes executing instructions and that "it is well known in the art that booting involves loading data from non-volatile memory into RAM." *See* Office Action, p.3. Applicants, however, respectfully submit that regardless of whether booting involves loading data from non-volatile memory into RAM, ***Bhatt*** is completely silent with respect to the claimed feature of an ***internal*** random access memory. In fact, ***Bhatt*** explicitly discloses, in the paragraph cited by the Examiner (¶[0028]), executing boot code 180 in *external memory* 160. Further, ***Bhatt*** only describes internal memory 130 as being *non-volitile*, read-only memory (ROM), not RAM as recited in claim 2. *See* ***Bhatt***, ¶[0013]. Clearly the Examiner's position (i.e., that "it is well known in the art that booting involves loading data from non-volatile memory into RAM") is in direct contrast to the claim 2 feature of an internal random access memory. As such, ***Bhatt*** does not teach this feature, and therefore, ***Bhatt*** does not anticipate claim 2.

As to any remaining anticipation and/or obviousness rejections in the Office Action, none of the additional arguments or prior art identified by the Examiner cures the fundamental deficiencies in ***Bhatt***, as noted above. Accordingly, Applicants respectfully request that all of the rejections set forth in the Office Action should be withdrawn for claims 1, 19 and 21 (and their respective dependent claims).

Conclusion

Applicants respectfully assert that in light of the amendments and arguments provided throughout the prosecution of the present application, all claims of the present application are now allowable and, therefore, request that a Notice of Allowance be issued. Reconsideration of the present application is respectfully requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is respectfully requested to call the undersigned attorney at the Houston, Texas telephone number (713) 934-4093 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 10742

Date: June 22, 2012

By: /Nathan E. Black/
Nathan E. Black Reg. No. 66,191
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4093
(713) 934-7011 (facsimile)
ATTORNEY FOR APPLICANT(S)

Electronic Acknowledgement Receipt

EFS ID:	13081733
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	Nathan Eldon Black/Nancy Nolan
Filer Authorized By:	Nathan Eldon Black
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	22-JUN-2012
Filing Date:	19-JAN-2009
Time Stamp:	12:56:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Response_to_NF_OfficeAction.pdf	137251 81cfa89daf81dc37594178763decb5e8f0e53fc9	no	10

Warnings:	
Information:	

Total Files Size (in bytes):	137251

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12355900
Filing Date	2009-01-19
First Named Inventor	Michael Grell
Art Unit	2115
Examiner Name	Jaweed A. Abbaszadeh
Attorney Docket Number	2162.162700/DE0892

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010007131	A1	2001-05-01	Galasso et al.	
	2	20050076226	A1	2005-04-07	Boivie et al.	
	3	20070192610	A1	2007-08-16	Chun et al.	
	4	20060112266	A1	2006-05-25	Little et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12355900
	Filing Date	2009-01-19
	First Named Inventor	Michael Grell
	Art Unit	2115
	Examiner Name	Jaweed A. Abbaszadeh
	Attorney Docket Number	2162.162700/DE0892

	1	1659472	EP	A1	2006-05-24			☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	PCT Search Report and Written Opinion from PCT/US2009/001289 dated August 3, 2009	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12355900
	Filing Date	2009-01-19
	First Named Inventor	Michael Grell
	Art Unit	2115
	Examiner Name	Jaweed A. Abbaszadeh
	Attorney Docket Number	2162.162700/DE0892

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Nathan E. Black/	Date (YYYY-MM-DD)	2012-06-22
Name/Print	Nathan E. Black	Registration Number	66191

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

AMD

From the INTERNATIONAL SEARCHING AUTHORITY

To:

Advanced Micro Devices, Inc.
Attn. Drake, Paul S.
7171 Southwest Parkway Mail Stop B100. 3.341
Austin TX 78735
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 03/08/2009
Applicant's or agent's file reference DE0904-PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2009/001289	International filing date *(day/month/year)* 27/02/2009
Applicant ADVANCED MICRO DEVICES, INC.	

1. [x] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Eva Hehn

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped),whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1–10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

If a demand for international preliminary examination is made, the written opinion of the International Searching Authority will, except in certain cases where the International Preliminary Examining Authority did not act as International Searching Authority and where it has notified the International Bureau under Rule 66.1*bis*(b), be considered to be a written opinion of the International Preliminary Examining Authority. If a demand is made, the applicant may submit to the International Preliminary Examining Authority a reply to the written opinion together, where appropriate, with amendments before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later (Rule 43*bis*.1(c)).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
DE0904-PCT		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2009/001289	27/02/2009	29/02/2008
Applicant		
ADVANCED MICRO DEVICES, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1b
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/001289

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F21/02

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)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 659 472 A (RES IN MOTION LTD [CA]) 24 May 2006 (2006-05-24)	1-10
X	the whole document	11,12
A	US 2001/007131 A1 (GALASSO LEONARD J [US] ET AL) 5 July 2001 (2001-07-05) the whole document	1-12
A	US 2005/076226 A1 (BOIVIE RICHARD H [US] ET AL) 7 April 2005 (2005-04-07) paragraph [0021] - paragraph [0022] paragraph [0043]	1-12

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document 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
24 July 2009	03/08/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Meis, Marc

3

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/001289

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1659472 A	24-05-2006	US 2006112266 A1	25-05-2006
US 2001007131 A1	05-07-2001	NONE	
US 2005076226 A1	07-04-2005	CN 1655087 A	17-08-2005

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2009/001289	27.02.2009	29.02.2008

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00 G06F21/02

Applicant
ADVANCED MICRO DEVICES, INC.

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

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

2. **FURTHER ACTION**

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

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

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

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

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Meis, Marc Telephone No. +49 89 2399-2505

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

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

1. Statement

Novelty (N)	Yes:	Claims	1-12
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-10
	No:	Claims	11-12
Industrial applicability (IA)	Yes:	Claims	1-12
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

SECTION V

1. Reference is made to the following documents:

   D1: EP-A-1 659 472 (RES IN MOTION LTD [CA]) 24 May 2006 (2006-05-24)
   D2: US 2001/007131 A1 (GALASSO LEONARD J [US] ET AL) 5 July 2001 (2001-07-05)
   D3: US 2005/076226 A1 (BOIVIE RICHARD H [US] ET AL) 7 April 2005 (2005-04-07)

2. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 11 - 12 does not involve an inventive step in the sense of Article 33(3) PCT.

   (a) Cl. 11

   Document D1 (par. 26 - 28 and fig. 2) discloses a CPU (processor 18) comprising
   - a substrate (technically implicit from the circuit elements being part of a processor) having formed thereon circuit elements defining a CPU core (MCU/DSP), a volatile RAM (internal SRAM), a non volatile memory (ROM 19) and a bus system for connecting said CPU core, said volatile RAM and said non-volatile memory; and
   - pre-boot information stored in said non-volatile memory, said pre-boot information including instructions (par. 27: authentication code) executable by said CPU core ~~and data values for initializing said volatile RAM~~ and verifying at least a portion of a boot routine (par. 17 and 27: OS software from memory 116).

   The subject-matter of cl. 11 differs therefrom in that
   (i) the pre-boot information comprises data values for initializing said volatile RAM.

   The subject-matter of claim 11 is therefore new (Article 33(2) PCT) with

respect to the disclosure of D1.

Feature (i) solves the problem of initializing the CPU for further operation.

Initialization of CPU elements prior after reset normally is required to ensure proper operation of CPUs. Provision of feature (ii) does not go beyond such initialization.

(b) Cl. 12

In the CPU known from D1, said pre-boot information includes one or more ~~decryption~~ keys (par. 27) configured to enable ~~deciphering~~ *verifying* of a signature of said at least a portion of said boot routine.

The subject-matter of cl. 12 further differs therefrom in that
(i) the keys are decryption keys for deciphering a signature.

The problem to be solved by the present invention may therefore be regarded as providing for authentication using encrypted signatures.

Authentication using encrypted signatures merely is one known authentication method (see e.g. document D2) of several known alternatives the skilled person may chose from within his normal skills.

3. Document D1 is regarded as being the closest prior art to the subject-matter of claim 1 and discloses a method for starting a computer system (device 10), the method comprising:
   - accessing a first set of data stored in non-volatile memory (ROM 19) of a CPU (processor 18), said first set of data including first instructions (par. 27: authentication code) ~~causing a core circuit (MCU/DSP) of said CPU to initialize an internal volatile memory of said CPU~~;
   - ~~loading~~ *reading* (par. 28) an image of a second set of data (par. 17: OS) from a non-volatile memory (par. 17 and 28: external flash memory 116) ~~into said initialized internal volatile memory~~, said second set of data comprising a signature for verifying integrity of said second set of data (fig. 2: "signed code"), said second set of data further comprising second instructions

causing said CPU to initialize a system memory of said computer system (technically implicit from the software in memory 116 being an OS);
- verifying said integrity of said second set of data by using said signature and a ~~decryption~~ key included in said first set of data (par. 27); and
- initializing said system memory using said second instructions when verification of said second set of data is unsuccessful (par. 27, 3): execute OS stored in external memory 116).

The subject-matter of cl. 1 differs therefrom in that
(i) the first set of data includes first instructions causing a core circuit of said CPU to initialize an internal volatile memory of said CPU;
(ii) an image of the second set of data is loaded into non-volatile memory of the CPU for verification and initializing the system memory.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

- Provision of feature (i) does not imply an inventive step for the reasons of lack of an inventive step given against cl. 10.

- In D1, the OS (second set of data comprising the second instructions) is read and verified and executed from external memory 116. This allows for tampering with the data and instructions when they are read again for execution even though they have been verified.

  The problem to be solved by feature (ii) the present invention may therefore be regarded as ensuring that the second instructions, once verified, cannot be tampered with for execution.

  This problem is solved by features (ii), i.e. by verifying and executing the second instructions from the internal memory, execution of the verified second instructions is ensured.

  The solution (ii) proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) because it is not obviously derivable from the available prior art.

Though document D3 (par. 21, 22 and 43) mentions use of a physically protected memory for loading, verifying and executing signed code, it is not obvious from document D3 to include such protected memory into the CPU itself.

Cl. 2 - 10 are dependent on claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

4. The claimed subject-matter is industrially applicable.

SECTION VIII

1. The vague and imprecise statement in the description on p. 6, l. 20 implies that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity (Article 6 PCT) when used to interpret them.

2. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the document D1 is not mentioned in the description, nor is this document identified therein.

—

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

BNSDOCID: <XS_____200704010CK_I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 659 472 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.05.2006 Bulletin 2006/21

(51) Int Cl.:
G06F 1/00 *(2006.01)* ***G06F 12/14*** *(2006.01)*

(21) Application number: **04105984.1**

(22) Date of filing: **22.11.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK YU

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Little, Herbert A.**
  N2T 2V8, Waterloo, (CA)
- **Hickey, Ryan J.**
  N2L 6M2, Waterloo, (CA)

(74) Representative: **Rickard, David John et al**
26 Mallinson Road
London SW11 1BP (GB)

(54) Method and Device for Authenticating Software

(57) A method and device for authenticating software stored in non-volatile memory in a data processing device. The processor comprises an internal immutable memory, preferably a read only memory (ROM), and during the boot up procedure the software in external memory is authenticated using code that is stored in the internal ROM. The on-chip ROM is physically integrated with the processor itself, so the code stored in ROM can neither be tampered with nor replaced, and can therefore be assumed at all times to be authentic. Thus, in the method and device of the invention known good code is used to authenticate the untrusted code in external memory, so the integrity of the system is significantly improved.

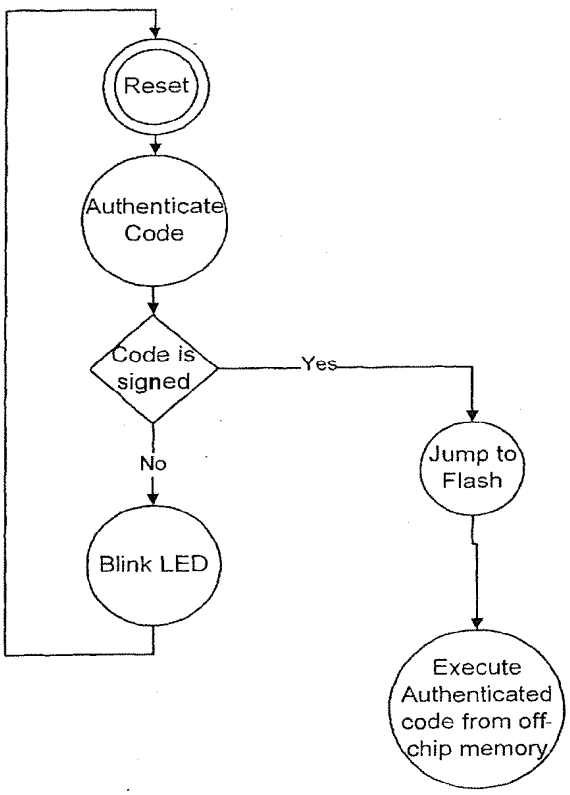


FIG. 3

EP 1 659 472 A1

internal memory being immutable once programmed and comprising authentication code and a public key for authenticating program software in at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

Brief Description of the Drawings

[0012] In drawings which illustrate by way of example only a preferred embodiment of the invention,

Figure 1 is a block diagram of a system overview of a conventional hand-held data processing device.
Figure 2 is a block diagram of a processor chip in the data processing device of Figure 1.

Figure 3 is a flow chart showing the boot procedure in the data processing device of Figure 1.

Detailed Description of the Invention

[0013] The invention will be described in detail below, by way of example only, in the context of a hand-held data processing device having wireless communications capabilities and a battery, as illustrated in Figure 1, in which a memory controller interface caches sectors out of non-volatile memory into volatile memory for processing, and writes modified data from volatile memory into non-volatile memory for more permanent storage. However, although the invention is particularly advantageous in the hand-held data processing device 10 of Figure 1, it will be appreciated that the principles of the system apply to other data processing devices and the system is not intended to be limited thereby.

[0014] The hand-held data processing devices 10 include a housing, a keyboard 14 and an output device 16. The output device shown is a display 16, which is preferably a full graphic LCD. Other types of output devices may alternatively be utilized. A processor 18, which is shown schematically in Figure 1, is contained within the housing and is coupled between the keyboard 14 and the display 16. The processor 18 controls the operation of the display 16, as well as the overall operation of the data processing device 10, in response to actuation of keys on the keyboard 14 by the user.

[0015] The housing may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keyboard may include a mode selection key, or other hardware or software for switching between text entry and telephony entry. The housing contains the primary power supply, in the embodiment shown a battery 170 , a secondary power supply 180 (illustrated in Figure 2), which may be a small rechargeable battery or capacitor capable of sustaining power to the processor 18, NAND flash 116 and SDRAM 118 for the duration of an AutoSave interval and a Power Manager 190.

[0016] In addition to the processor 18, other parts of the data processing device 10 are shown schematically in Fig. 1. These include a communications subsystem 100; a short-range communications subsystem 102; the keyboard 14 and the display 16, along with other input/output devices 106, 108, 110 and 112; as well as memory devices 116, 118 and various other device subsystems 120. The data processing device 10 is preferably a two-way RF communication device having voice and data communication capabilities. In addition, the data processing device 10 preferably has the capability to communicate with other computer systems via the Internet.

[0017] Operating system software executed by the processor 18 is preferably stored in a persistent store, such as a flash memory 116, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as a random access memory (RAM including also DRAM and SDRAM) 118. Communication signals received by the data processing device 10 may also be stored to the RAM 118.

[0018] The processor 18, in addition to its operating system functions, enables execution of software applications 130A-130N on the device 10. A predetermined set of applications that control basic device operations, such as data and voice communications 130A and 130B, may be installed on the device 10 during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM is preferably capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also preferably capable of sending and receiving data items via a wireless network 140. Preferably, the PIM data items are seamlessly integrated, synchronized and updated via the wireless network 140 with the device user's corresponding data items stored or associated with a host computer system.

[0019] Communication functions, including data and voice communications, are performed through the communication subsystem 100, and possibly through the short-range communications subsystem. The communication subsystem 100 includes a receiver 150, a transmitter 152, and one or more antennas 154 and 156. In addition, the communication subsystem 100 also includes a processing module, such as a digital signal processor (DSP) 158, and local oscillators (LOs) 160. The specific design and implementation of the communication subsystem 100 is dependent upon the communication network in which the data processing device 10 is intended to operate. For example, a data processing device 10 may include a communication subsystem 100

BNSDOCID: <EP_____1659472A1_I_>

device 10.

4) If the processor 18 determines that the program software in the external memory 116 has not been authenticated successfully, the boot program causes another reset signal to be sent the processor 18. The boot routine thus repeats and again tries to authenticate the program software in the external memory 116. If the unsuccessful authentication attempt was merely due to an execution error, the program software will likely be authenticated on a subsequent execution of the authentication code. However, if the unsuccessful authentication attempt occurred because the external memory 116 had been tampered with, an endless resetting loop will result, thereby preventing malicious code from being executed by the processor 18.

[0028] The method and device of the invention thus ensures that the boot code performing the authentication process is guaranteed to be authentic. As an alternative, it is possible to stack the non-volatile memory 116 in the same package as the processor 18, on the assumption that there is no way for an attacker to modify the boot code stored in on-chip flash. However, authenticating the device's code using internal ROM 19 is more secure, since it is impossible to change the code stored in ROM without re-fabricating the silicon die itself. Accordingly, in the method and device of the invention trusted code is always used to authenticate the untrustworthy code in external memory, so the integrity of the system is significantly improved.

[0029] When authenticating the code in external memory such as flash memory 116, it is important to ensure the code is signed correctly. Several algorithms can be used to accomplish this. By way of example only, RSA is a good candidate since it runs quickly and has a small memory footprint. However, other authentication algorithms are available for this and the invention is not intended to be limited to any particular authentication means.

[0030] Although internal ROM 19 is preferred, other internal memory technologies that are immutable when in operation (i.e. once programmed), such as one time programmable flash could be used to hold the bootROM and public key(s). However, whatever type of memory is used, the internal bootROM code and public key(s) should be immutable once the device has been deployed so that they cannot be changed. Regular flash can be used if protected by hardware that secures a regular programmable flash memory to render it immutable once it has been written to, and a programmable flash memory so equipped would be immutable for purposes of the invention and thus suitable for use in the invention.

[0031] Various embodiments of the present invention having been thus described in detail by way of example, it will be apparent to those skilled in the art that variations and modifications may be made without departing from the invention. The invention includes all such variations and modifications as fall within the scope of the appended claims.

Claims

1. A method of authenticating software in a data processing device comprising a data processor comprising at least one internal memory, the internal memory being immutable once programmed, and at least one external memory containing program software, comprising the steps of:

   issuing a reset signal to the processor;
   reading authentication code from the internal memory;
   executing the authentication code to authenticate at least a portion of the software in the external memory using a public key stored in the internal memory; and

   (i) if the software is authenticated successfully, reading and executing code stored in external memory; or
   (ii) if the software is not authenticated successfully, sending a reset signal to the processor.

2. The method of claim 1 wherein the internal memory comprises a read only memory.

3. A data processing device, comprising
   at least one external memory containing program software, and
   a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code means and a public key for authenticating the program software in the at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code means stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

4. The device of claim 3 wherein the internal memory comprises a read only memory.

5. A data processor for the device of claim 3, wherein the internal memory comprises a one time programmable flash memory.

6. A computer readable medium comprising code means executable by the data processor of the device of claims 3 or 4 for implementing the method of

BNSDOCID: <EP_____1659472A1_I_>

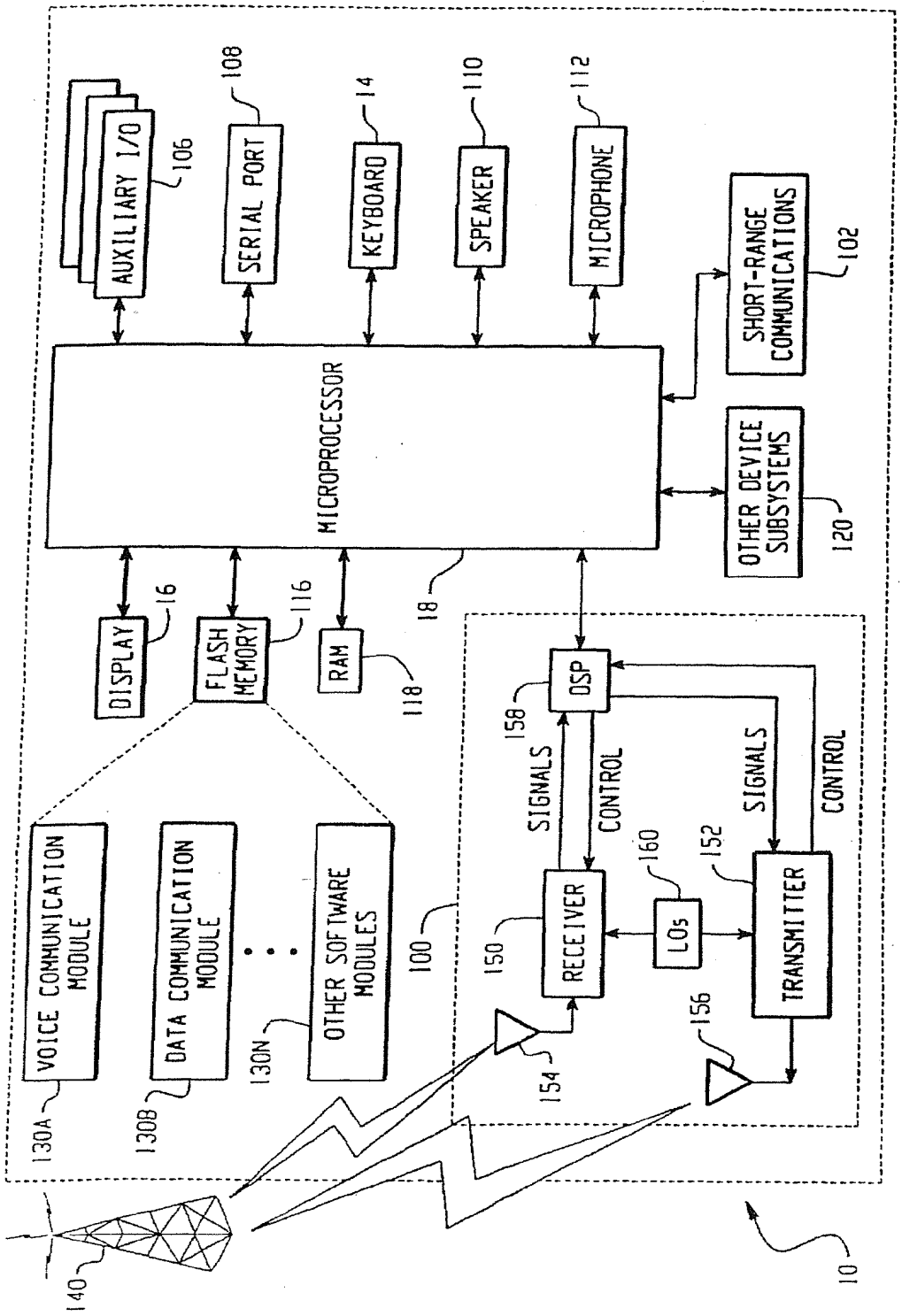


FIG. 1

BNSDOCID: <EP_____1659472A1_I_>

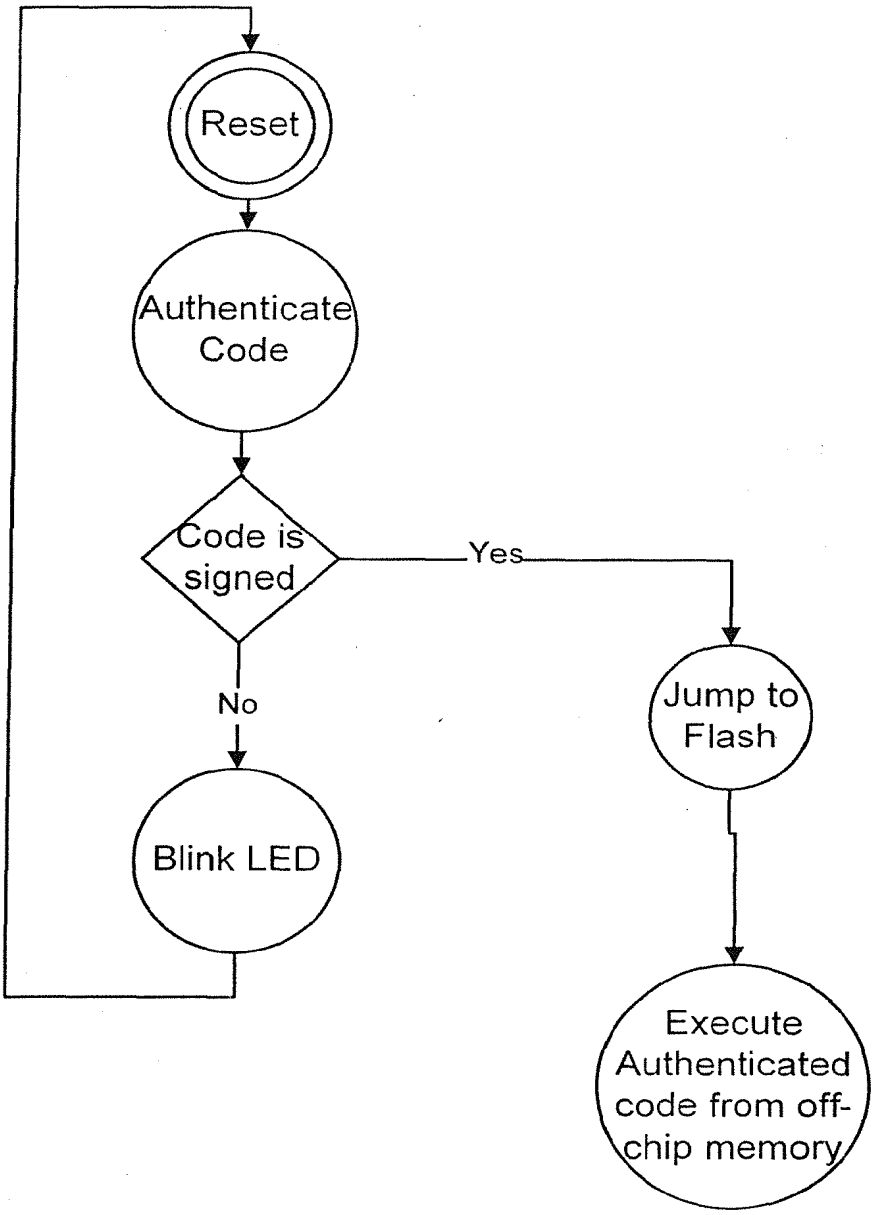


FIG. 3

BNSDOCID: <EP_____1659472A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 10 5984

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	SMITH S W ET AL: "Building a high-performance, programmable secure coprocessor" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 31, no. 8, 23 April 1999 (1999-04-23), pages 831-860, XP004304521 ISSN: 1389-1286 * page 833, right-hand column, line 22 - line 25 * * page 835, right-hand column, line 9 - page 836, left-hand column, line 35 * * page 839, left-hand column, line 8 * * page 844, left-hand column, line 29 - right-hand column, line 24; figure 8 * * page 846, right-hand column, line 16 - line 19 * * page 850, left-hand column, line 30 - right-hand column, line 4 *	1-6	
A	WO 03/060670 A (RESEARCH IN MOTION LIMITED; MADTER, RICHARD, C; HICKEY, RYAN, J; PATTE) 24 July 2003 (2003-07-24) * page 8, line 3 - line 9; figure 2 *	1-6	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	US 2002/144104 A1 (SPRINGFIELD RANDALL SCOTT ET AL) 3 October 2002 (2002-10-03) * paragraph [0022] *	1-6	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	12 July 2005	Preuss, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1659472A1_I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 659 472 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.05.2006 Bulletin 2006/21

(51) Int Cl.:
G06F 1/00 *(2006.01)* ***G06F 12/14*** *(2006.01)*

(21) Application number: **04105984.1**

(22) Date of filing: **22.11.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK YU

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Little, Herbert A.**
  N2T 2V8, Waterloo, (CA)
- **Hickey, Ryan J.**
  N2L 6M2, Waterloo, (CA)

(74) Representative: **Rickard, David John et al**
26 Mallinson Road
London SW11 1BP (GB)

(54) Method and Device for Authenticating Software

(57) A method and device for authenticating software stored in non-volatile memory in a data processing device. The processor comprises an internal immutable memory, preferably a read only memory (ROM), and during the boot up procedure the software in external memory is authenticated using code that is stored in the internal ROM. The on-chip ROM is physically integrated with the processor itself, so the code stored in ROM can neither be tampered with nor replaced, and can therefore be assumed at all times to be authentic. Thus, in the method and device of the invention known good code is used to authenticate the untrusted code in external memory, so the integrity of the system is significantly improved.

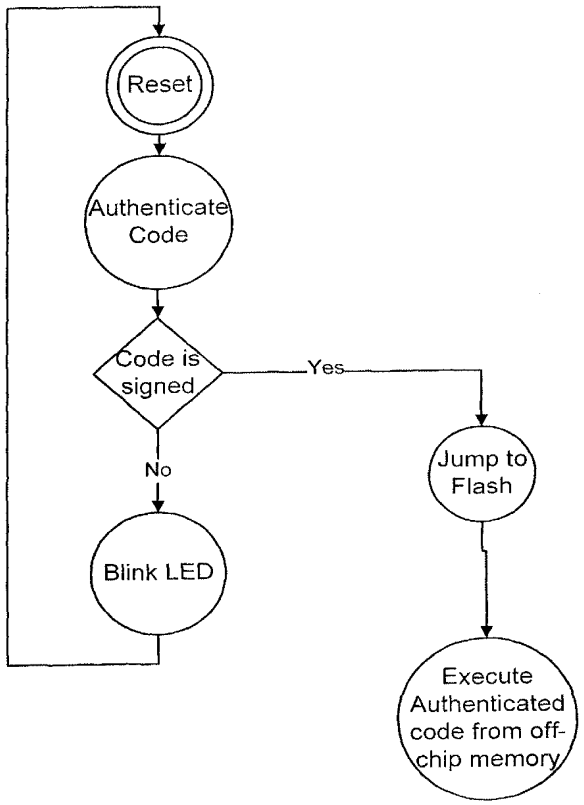


FIG. 3

EP 1 659 472 A1

Description

[0001] This invention relates to security in data processing systems. In particular, this invention relates to a method and device for the authentication of software stored in non-volatile memory.

[0002] The use of portable data processing systems has increased significantly in recent years. In addition to so called "laptop" and "tablet" computers, there is a growing popularity in handheld data processing devices, often called a "personal digital assistant" or "PDA." All of these devices are capable of storing a significant amount of user data, including calendar, address book, tasks and numerous other types of data for business and personal use. Most handheld data processing devices have the ability to connect to a personal computer for data exchange, and many are equipped for wireless communications using, for example, conventional email messaging systems.

[0003] Depending upon the user's needs much of this data can be highly sensitive in nature, especially for example in a government, military or commercial context. Accordingly, protection of the data in such a device is an important consideration. The integrity of a secure system relies entirely on the authenticity of its program code. It is possible to attack these types of systems by replacing the device's program code with malicious code. Thus, in any system that values security, when the embedded system boots up and the processor begins executing boot code, the boot code will immediately authenticate the software before executing any program code.

[0004] The fundamental deficiency in this method of software authentication is that the initial boot code is usually stored in off chip non-volatile memory and therefore cannot itself be trusted, because it is possible for an attacker to replace the non-volatile memory chip with another compatible chip containing malicious code.

[0005] It would accordingly be advantageous to provide a method of authenticating software in which the boot code that performs the authentication process can be guaranteed to be authentic. The authentication process itself can then be trusted, and the program code can be determined with certainty not to have been tampered with.

Summary of the Invention

[0006] The present invention accordingly provides a method and apparatus for authenticating software stored in external non-volatile memory using a hardware mechanism before the software is allowed to run on the processor.

[0007] According to the method and apparatus of the invention, in the preferred embodiment of the invention, during the boot up procedure the code in external memory is authenticated using code that is stored in on-chip (internal) immutable memory, preferably a read only memory (ROM). The internal memory is physically integrated into the processor itself, so the code stored in the internal memory can neither be tampered with nor replaced, and can therefore be assumed at all times to be authentic. The public key needed for the authentication process is also stored in the internal memory.

[0008] In the preferred embodiment of the invention the boot procedure is as follows:

1) Following a reset signal (e.g. when the device is activated), rather than fetching instructions from an untrustworthy source such as an external NOR or NAND flash memory chip, the processor executes code read directly from the internal memory.
2) The code in the internal memory first runs a program that authenticates all or a portion of the external memory.
3) If the code is authenticated successfully using the public key stored in the internal memory, the authentication program jumps to code stored in external memory.
4) If the code authentication is unsuccessful, the program resets the processor. Where the external memory has been tampered with, this results in an endless resetting loop, thereby preventing malicious code from being executed.

[0009] The present invention thus provides a method of authenticating software in a data processing device comprising a data processor comprising at least one internal memory, the internal memory being immutable once programmed, and at least one external memory containing program software, comprising the steps of: a. issuing a reset signal to the processor; b. reading authentication code from the internal memory; c. executing the authentication code to authenticate at least a portion of the software in the external memory using a public key stored in the internal memory; and d. (i) if the software is authenticated successfully, reading and executing code stored in external memory; or (ii) if the software is not authenticated successfully, sending a reset signal to the processor.

[0010] The present invention further provides data processing device, comprising at least one external memory containing program software, and a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code and a public key for authenticating the program software in the at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

[0011] The present invention further provides a data processor comprising at least one internal memory, the

internal memory being immutable once programmed and comprising authentication code and a public key for authenticating program software in at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

Brief Description of the Drawings

[0012] In drawings which illustrate by way of example only a preferred embodiment of the invention,

Figure 1 is a block diagram of a system overview of a conventional hand-held data processing device.
Figure 2 is a block diagram of a processor chip in the data processing device of Figure 1.

Figure 3 is a flow chart showing the boot procedure in the data processing device of Figure 1.

Detailed Description of the Invention

[0013] The invention will be described in detail below, by way of example only, in the context of a hand-held data processing device having wireless communications capabilities and a battery, as illustrated in Figure 1, in which a memory controller interface caches sectors out of non-volatile memory into volatile memory for processing, and writes modified data from volatile memory into non-volatile memory for more permanent storage. However, although the invention is particularly advantageous in the hand-held data processing device 10 of Figure 1, it will be appreciated that the principles of the system apply to other data processing devices and the system is not intended to be limited thereby.

[0014] The hand-held data processing devices 10 include a housing, a keyboard 14 and an output device 16. The output device shown is a display 16, which is preferably a full graphic LCD. Other types of output devices may alternatively be utilized. A processor 18, which is shown schematically in Figure 1, is contained within the housing and is coupled between the keyboard 14 and the display 16. The processor 18 controls the operation of the display 16, as well as the overall operation of the data processing device 10, in response to actuation of keys on the keyboard 14 by the user.

[0015] The housing may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keyboard may include a mode selection key, or other hardware or software for switching between text entry and telephony entry. The housing contains the primary power supply, in the embodiment shown a battery 170 , a secondary power supply 180 (illustrated in Figure 2), which may be a small rechargeable battery or capacitor capable of sustaining power to the processor 18, NAND flash 116 and SDRAM 118 for the duration of an AutoSave interval and a Power Manager 190.

[0016] In addition to the processor 18, other parts of the data processing device 10 are shown schematically in Fig. 1. These include a communications subsystem 100; a short-range communications subsystem 102; the keyboard 14 and the display 16, along with other input/output devices 106, 108, 110 and 112; as well as memory devices 116, 118 and various other device subsystems 120. The data processing device 10 is preferably a two-way RF communication device having voice and data communication capabilities. In addition, the data processing device 10 preferably has the capability to communicate with other computer systems via the Internet.

[0017] Operating system software executed by the processor 18 is preferably stored in a persistent store, such as a flash memory 116, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as a random access memory (RAM including also DRAM and SDRAM) 118. Communication signals received by the data processing device 10 may also be stored to the RAM 118.

[0018] The processor 18, in addition to its operating system functions, enables execution of software applications 130A-130N on the device 10. A predetermined set of applications that control basic device operations, such as data and voice communications 130A and 130B, may be installed on the device 10 during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM is preferably capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also preferably capable of sending and receiving data items via a wireless network 140. Preferably, the PIM data items are seamlessly integrated, synchronized and updated via the wireless network 140 with the device user's corresponding data items stored or associated with a host computer system.

[0019] Communication functions, including data and voice communications, are performed through the communication subsystem 100, and possibly through the short-range communications subsystem. The communication subsystem 100 includes a receiver 150, a transmitter 152, and one or more antennas 154 and 156. In addition, the communication subsystem 100 also includes a processing module, such as a digital signal processor (DSP) 158, and local oscillators (LOs) 160. The specific design and implementation of the communication subsystem 100 is dependent upon the communication network in which the data processing device 10 is intended to operate. For example, a data processing device 10 may include a communication subsystem 100

designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, GSM, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the data processing device 10.

[0020] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore requires a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0021] When required network registration or activation procedures have been completed, the data processing device 10 may send and receive communication signals over the communication network 140. Signals received from the communication network 140 by the antenna 154 are routed to the receiver 150, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP 158 to perform more complex communication functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network 140 are processed (e.g. modulated and encoded) by the DSP 158 and are then provided to the transmitter 152 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 140 (or networks) via the antenna 156.

[0022] In addition to processing communication signals, the DSP 158 provides for control of the receiver 150 and the transmitter 152. For example, gains applied to communication signals in the receiver 150 and transmitter 152 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 158.

[0023] In a data communication mode, a received signal, such as a text message or web page download, is processed by the communication subsystem 100 and is input to the processor 18. The received signal is then further processed by the processor 18 for an output to the display 16, or alternatively to some other auxiliary I/O device 106. A device user may also compose data items, such as e-mail messages, using the keyboard 14 and/or some other auxiliary I/O device 106, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communication network 140 via the communication subsystem 100.

[0024] In a voice communication mode, overall operation of the device is substantially similar to the data communication mode, except that received signals are output to a speaker 110, and signals for transmission are generated by a microphone 112. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device 10. In addition, the display 16 may also be utilized in voice communication mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[0025] The short-range communications subsystem enables communication between the data processing device 10 and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth™ communication module to provide for communication with similarly-enabled systems and devices.

[0026] The device 10 embodying the invention, illustrated in Figure 2, authenticates software stored in an external memory such as non-volatile memory 116 (for example a NOR or NAND flash memory chip) using a internal authentication program, before any software from the memory 116 is executed by the processor 18. The processor comprises an internal immutable memory, preferably a read only memory (ROM) 19, which is physically integrated into the processor 18 when the processor's silicon die is fabricated.

[0027] The internal ROM 19 contains the authentication code, including one or more public keys, required for authenticating the program software residing in external memory 116 in known fashion. The authentication process is initiated when a reset signal is sent to the processor 18 (for example when the device 10 is activated or restarted). This initiates the boot up procedure, illustrated in Figure 3, which in the preferred embodiment of the invention is as follows:

1) After the processor 18 receives the reset signal, rather than fetching instructions from an untrusted source (e.g. off-chip memory such as NOR flash 116), the processor 18 executes code read directly from its internal ROM 19.

2) The code in the processor's internal ROM 19 comprises a conventional software authentication program that authenticates all or a portion of the external memory 116 containing the program software for the device 10, which is executed by the processor 18 before any code from the external memory 116 is executed. The program software residing in external memory 116 may be authenticated in any conventional fashion, for example using a digital signature verification system such as "RSA," or any other suitable system, and preferably using a public key stored in the internal ROM 19.

3) If the processor 18 determines that the program software in the external memory 116 has been authenticated successfully, the processor 18 begins to fetch and execute program code stored in the external memory 116 to initiate the basic functions of the

device 10.

4) If the processor 18 determines that the program software in the external memory 116 has not been authenticated successfully, the boot program causes another reset signal to be sent the processor 18. The boot routine thus repeats and again tries to authenticate the program software in the external memory 116. If the unsuccessful authentication attempt was merely due to an execution error, the program software will likely be authenticated on a subsequent execution of the authentication code. However, if the unsuccessful authentication attempt occurred because the external memory 116 had been tampered with, an endless resetting loop will result, thereby preventing malicious code from being executed by the processor 18.

[0028] The method and device of the invention thus ensures that the boot code performing the authentication process is guaranteed to be authentic. As an alternative, it is possible to stack the non-volatile memory 116 in the same package as the processor 18, on the assumption that there is no way for an attacker to modify the boot code stored in on-chip flash. However, authenticating the device's code using internal ROM 19 is more secure, since it is impossible to change the code stored in ROM without re-fabricating the silicon die itself. Accordingly, in the method and device of the invention trusted code is always used to authenticate the untrustworthy code in external memory, so the integrity of the system is significantly improved.

[0029] When authenticating the code in external memory such as flash memory 116, it is important to ensure the code is signed correctly. Several algorithms can be used to accomplish this. By way of example only, RSA is a good candidate since it runs quickly and has a small memory footprint. However, other authentication algorithms are available for this and the invention is not intended to be limited to any particular authentication means.

[0030] Although internal ROM 19 is preferred, other internal memory technologies that are immutable when in operation (i.e. once programmed), such as one time programmable flash could be used to hold the bootROM and public key(s). However, whatever type of memory is used, the internal bootROM code and public key(s) should be immutable once the device has been deployed so that they cannot be changed. Regular flash can be used if protected by hardware that secures a regular programmable flash memory to render it immutable once it has been written to, and a programmable flash memory so equipped would be immutable for purposes of the invention and thus suitable for use in the invention.

[0031] Various embodiments of the present invention having been thus described in detail by way of example, it will be apparent to those skilled in the art that variations and modifications may be made without departing from the invention. The invention includes all such variations and modifications as fall within the scope of the appended claims.

Claims

1. A method of authenticating software in a data processing device comprising a data processor comprising at least one internal memory, the internal memory being immutable once programmed, and at least one external memory containing program software, comprising the steps of:

   issuing a reset signal to the processor;
   reading authentication code from the internal memory;
   executing the authentication code to authenticate at least a portion of the software in the external memory using a public key stored in the internal memory; and

   (i) if the software is authenticated successfully, reading and executing code stored in external memory; or
   (ii) if the software is not authenticated successfully, sending a reset signal to the processor.

2. The method of claim 1 wherein the internal memory comprises a read only memory.

3. A data processing device, comprising
   at least one external memory containing program software, and
   a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code means and a public key for authenticating the program software in the at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code means stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

4. The device of claim 3 wherein the internal memory comprises a read only memory.

5. A data processor for the device of claim 3, wherein the internal memory comprises a one time programmable flash memory.

6. A computer readable medium comprising code means executable by the data processor of the device of claims 3 or 4 for implementing the method of

claims 1 or 2.

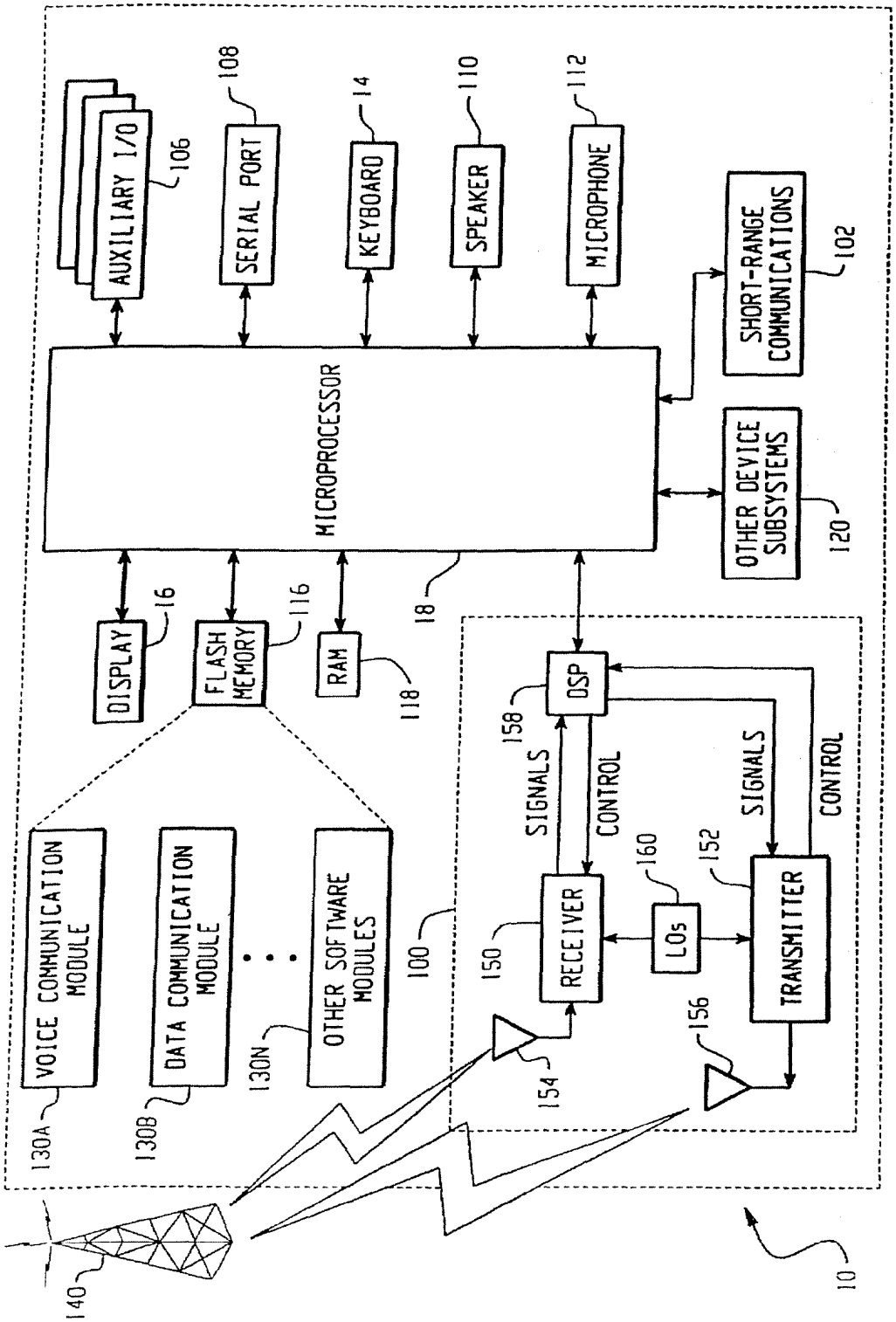

AUXILIARY I/O
106
SERIAL PORT
108
KEYBOARD
14
SPEAKER
110
MICROPHONE
112
SHORT-RANGE COMMUNICATIONS
102
MICROPROCESSOR
OTHER DEVICE SUBSYSTEMS
120
DISPLAY
16
FLASH MEMORY
116
RAM
118
18
DSP
158
SIGNALS
CONTROL
SIGNALS
CONTROL
160
152
RECEIVER
LOs
TRANSMITTER
150
154
156
100
VOICE COMMUNICATION MODULE
130A
DATA COMMUNICATION MODULE
130B
OTHER SOFTWARE MODULES
130N
140
10

FIG. 1

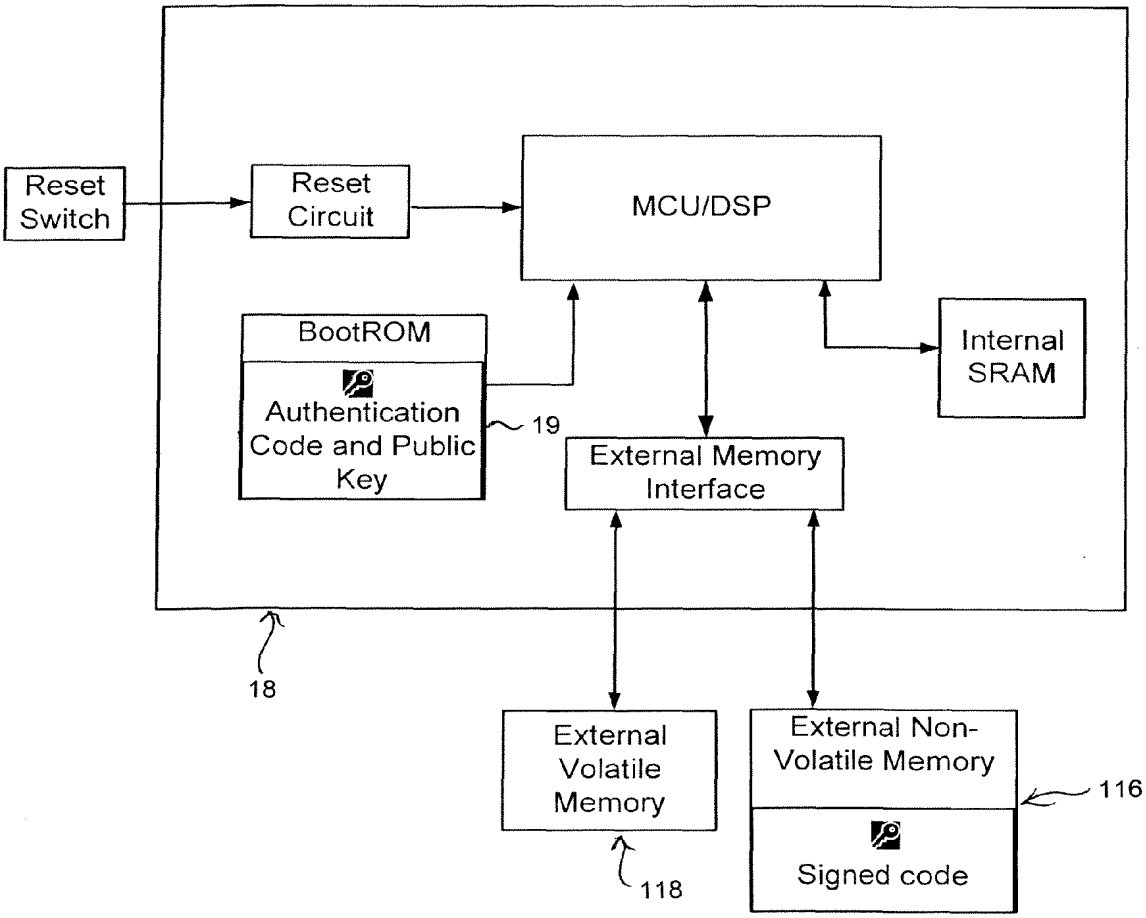

Reset Switch
Reset Circuit
MCU/DSP
BootROM
Authentication Code and Public Key
19
Internal SRAM
External Memory Interface
18
External Volatile Memory
118
External Non-Volatile Memory
116
Signed code

FIG. 2

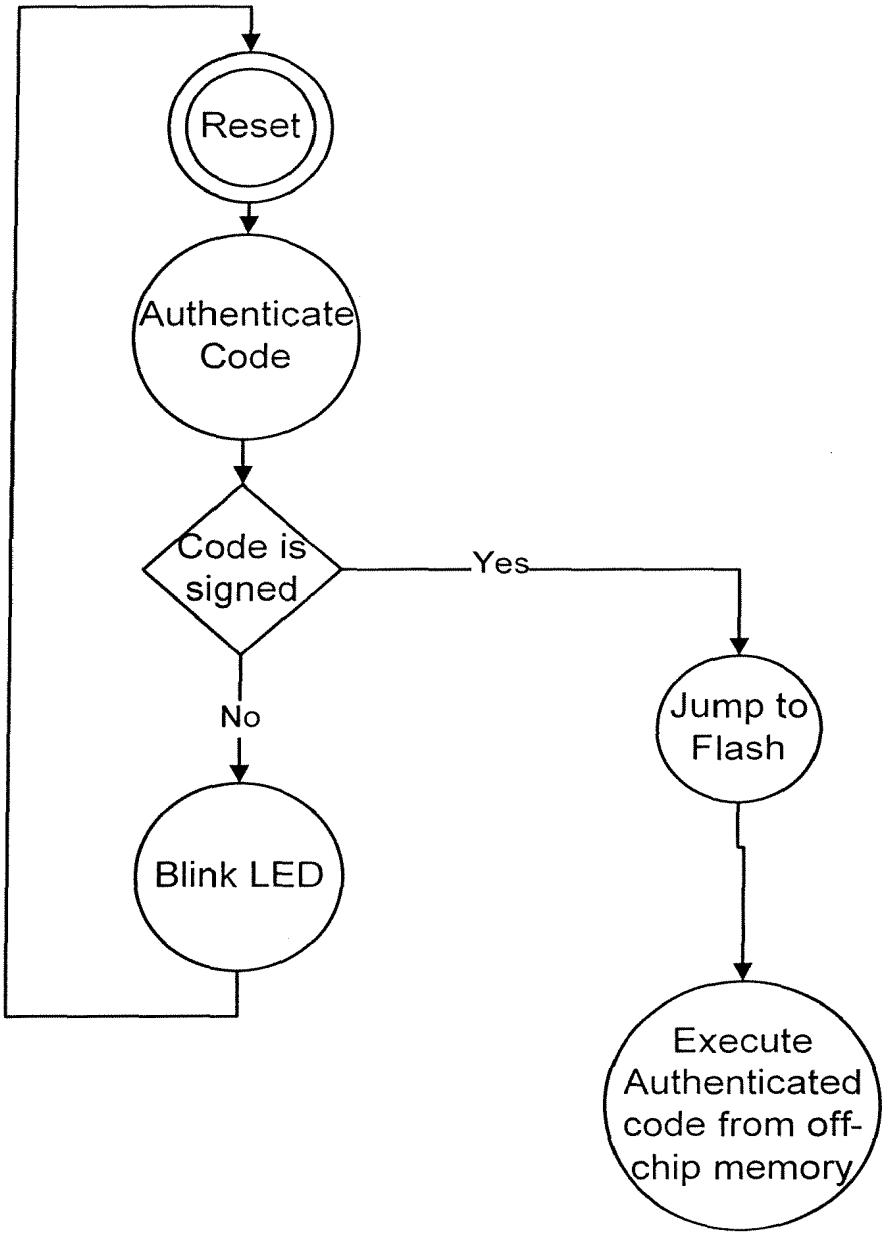

Reset
Authenticate Code
Code is signed
Yes
No
Jump to Flash
Blink LED
Execute Authenticated code from off-chip memory

FIG. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 10 5984

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 6 587 947 B1 (O'DONNELL AMY ET AL) 1 July 2003 (2003-07-01) * column 2, line 8 - line 20 * * column 4, line 36 - line 42 * * column 4, line 56 - line 59 * * column 5, line 22 - line 26 * * figures 2,4,6 *	1-6	G06F1/00 G06F12/14
Y	ANDREW "BUNNIE" HUANG: "Hacking the Xbox" 2003, NO STARCH PRESS INC. , SAN FRANCISCO, CA, USA , XP002335696 * page 104, paragraph 2 * * page 142 - page 143 *	1-6	
Y	EP 0 961 193 A (TEXAS INSTRUMENTS INCORPORATED) 1 December 1999 (1999-12-01) * page 6, column 9, line 29, paragraph 28 - column 10, line 43, paragraph 31; figure 5 *	1-6	
A	EP 0 816 970 A (SUN MICROSYSTEMS, INC) 7 January 1998 (1998-01-07) * claim 9 *	1,3,5	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
Y	* claim 15 *	2,4	G06F

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	12 July 2005	Preuss, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 10 5984

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	SMITH S W ET AL: "Building a high-performance, programmable secure coprocessor" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 31, no. 8, 23 April 1999 (1999-04-23), pages 831-860, XP004304521 ISSN: 1389-1286 * page 833, right-hand column, line 22 - line 25 * * page 835, right-hand column, line 9 - page 836, left-hand column, line 35 * * page 839, left-hand column, line 8 * * page 844, left-hand column, line 29 - right-hand column, line 24; figure 8 * * page 846, right-hand column, line 16 - line 19 * * page 850, left-hand column, line 30 - right-hand column, line 4 *	1-6	
A	WO 03/060670 A (RESEARCH IN MOTION LIMITED; MADTER, RICHARD, C; HICKEY, RYAN, J; PATTE) 24 July 2003 (2003-07-24) * page 8, line 3 - line 9; figure 2 *	1-6	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	US 2002/144104 A1 (SPRINGFIELD RANDALL SCOTT ET AL) 3 October 2002 (2002-10-03) * paragraph [0022] *	1-6	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	12 July 2005	Preuss, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 10 5984

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-07-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6587947 B1	01-07-2003	NONE	
EP 0961193 A	01-12-1999	US 5974495 A	26-10-1999
		EP 0961193 A2	01-12-1999
		JP 2000138917 A	16-05-2000
		US 6266754 B1	24-07-2001
		US 2001018745 A1	30-08-2001
		US 6411106 B1	25-06-2002
		CA 2334276 A1	02-12-1999
		EP 1082453 A1	14-03-2001
		US 6030802 A	29-02-2000
		WO 9961657 A1	02-12-1999
EP 0816970 A	07-01-1998	US 6138236 A	24-10-2000
		EP 0816970 A2	07-01-1998
WO 03060670 A	24-07-2003	AU 2002350339 A1	30-07-2003
		WO 03060670 A2	24-07-2003
		CA 2471835 A1	24-07-2003
		EP 1459153 A2	22-09-2004
		US 2005033951 A1	10-02-2005
US 2002144104 A1	03-10-2002	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

US 20070192610A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0192610 A1

Chun et al. (43) Pub. Date: Aug. 16, 2007

(54) METHOD AND APPARATUS FOR SECURELY BOOTING FROM AN EXTERNAL STORAGE DEVICE

(76) Inventors: **Dexter Tamio Chun**, San Diego, CA (US); **Ajit B. Patil**, San Diego, CA (US); **Cuneyt Fitoz**, San Diego, CA (US); **Dwight Gordon**, San Diego, CA (US); **Yu-Hsiang Huang**, San Diego, CA (US); **Oliver Michaelis**, San Diego, CA (US)

Correspondence Address:
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121 (US)

(21) Appl. No.: **11/351,966**

(22) Filed: **Feb. 10, 2006**

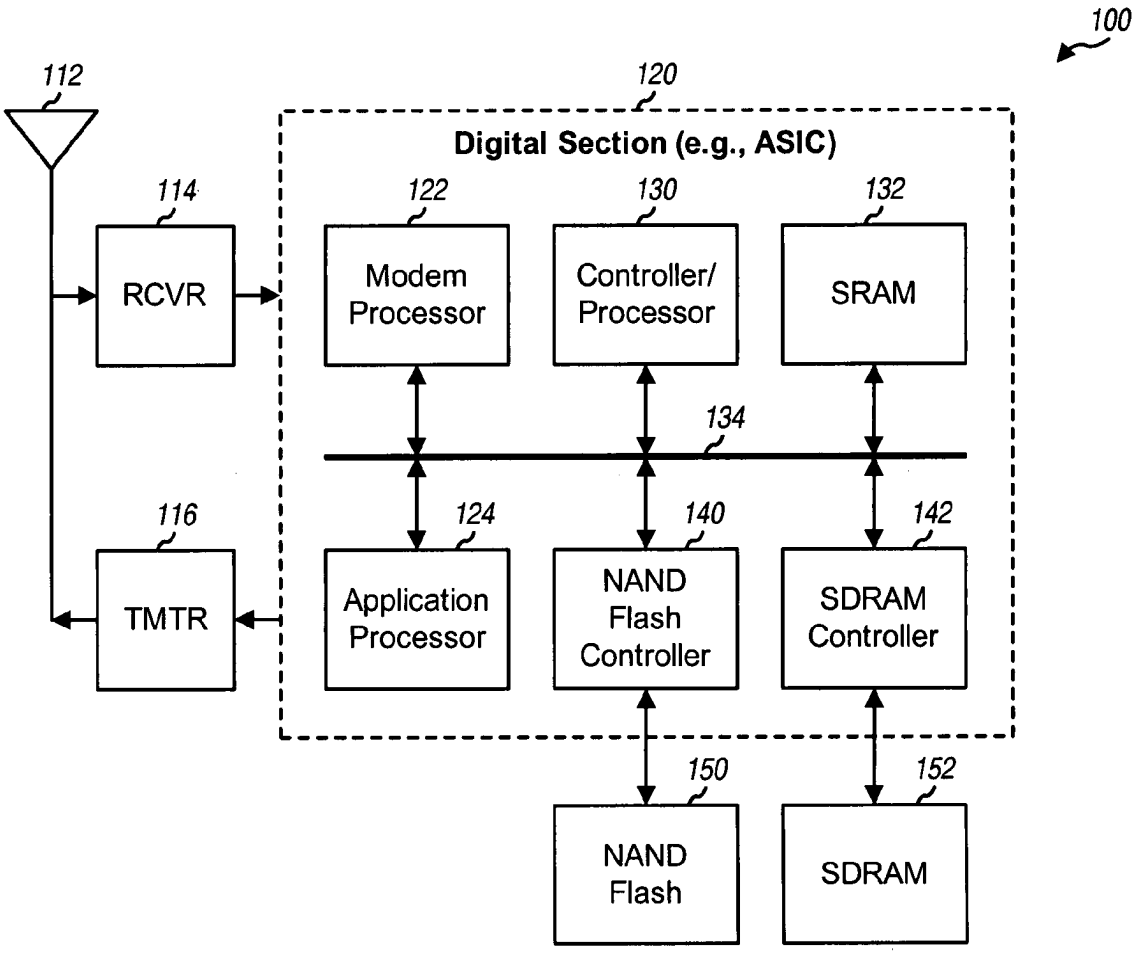
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/176**

(57) **ABSTRACT**

Techniques to securely boot up an electronics device (e.g., a cellular phone) from an external storage device are described. Secure data (e.g., a hash digest, a signature, a cryptographic key, and so on) is initially retrieved from a non-writable area of an external memory device (e.g., an one-time programmable (OTP) area of a NAND Flash device). A first program (e.g., a boot program) is retrieved from a writable or main area of the external memory device and authenticated based on the secure data. The first program is enabled for execution if authenticated. A second program may be retrieved from the main area of the external memory device and authenticated based on the secure data. The second program is enabled for execution if authenticated. Additional programs may be retrieved and authenticated. Each program may be authenticated using a secure hash function, a digital signature, and/or some other cryptographic technique.



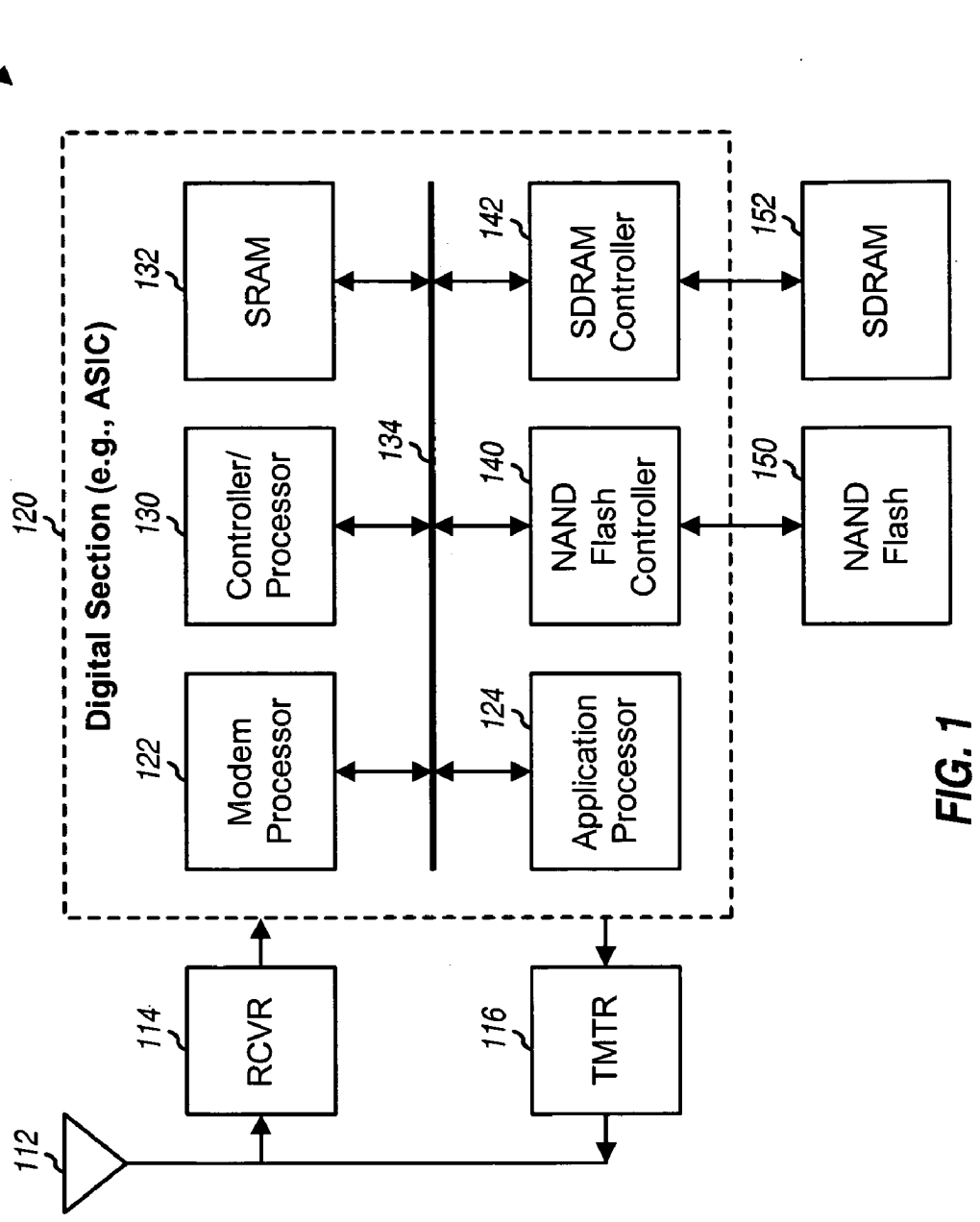

100
Digital Section (e.g., ASIC)
120
SRAM
132
Controller/ Processor
130
Modem Processor
122
134
SDRAM Controller
142
NAND Flash Controller
140
Application Processor
124
SDRAM
152
NAND Flash
150
RCVR
114
TMTR
116
112

FIG. 1

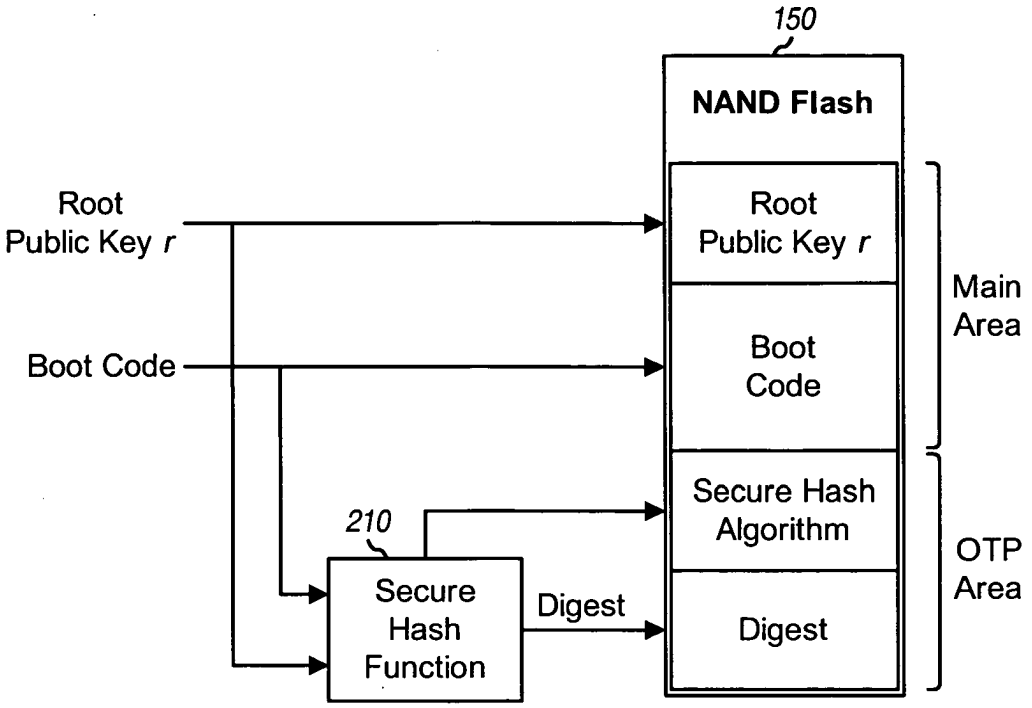

150
NAND Flash
Root
Public Key r
Boot Code
Root
Public Key r
Boot
Code
Secure Hash
Algorithm
Digest
Main
Area
OTP
Area
210
Secure
Hash
Function
Digest

FIG. 2A

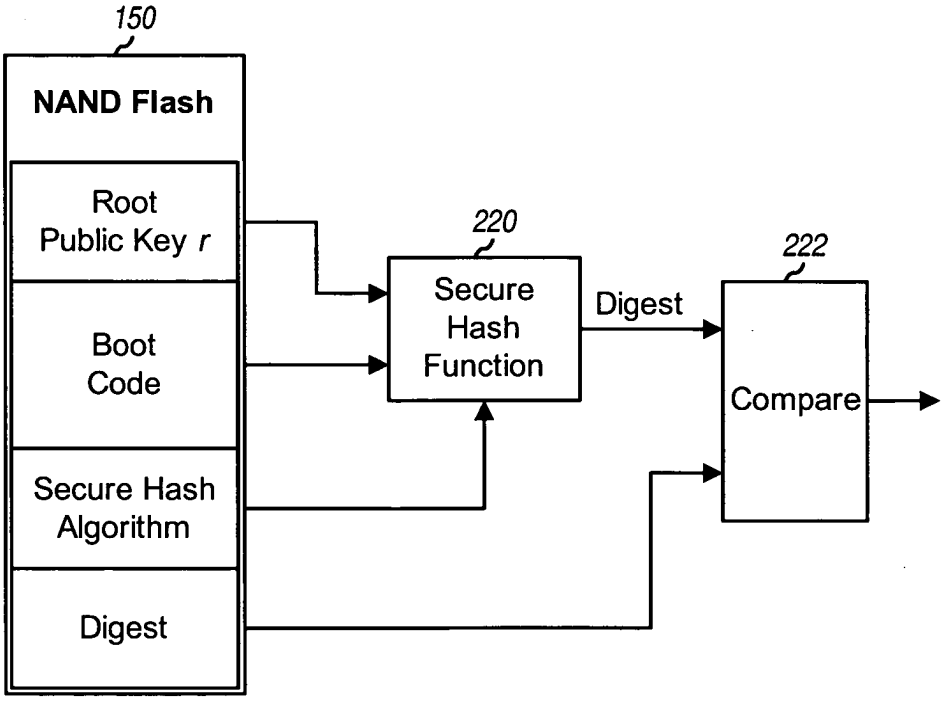

150
NAND Flash
Root
Public Key r
Boot
Code
Secure Hash
Algorithm
Digest
220
Secure
Hash
Function
Digest
222
Compare

FIG. 2B

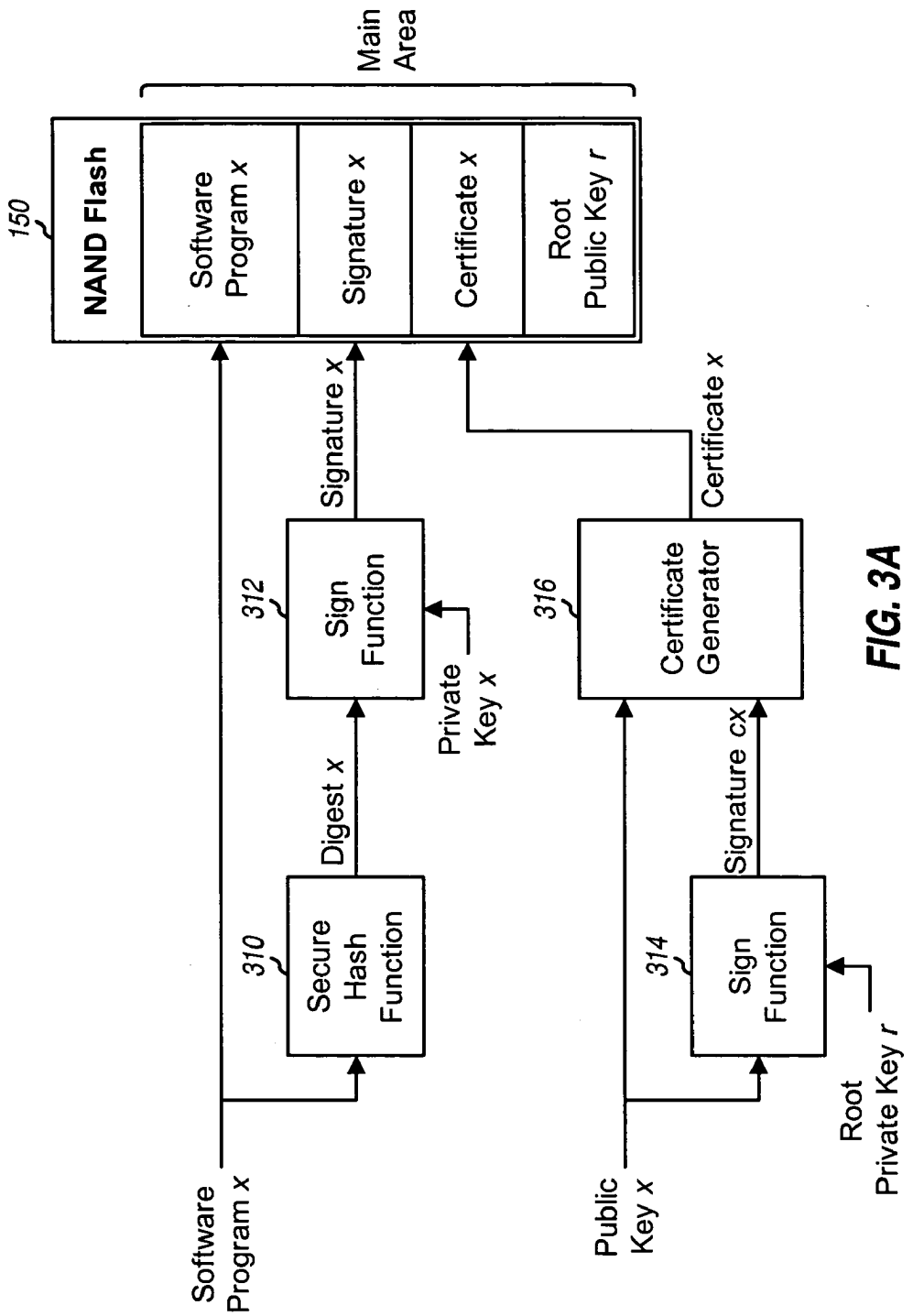

Main Area
150
NAND Flash
Software Program x
Signature x
Certificate x
Root Public Key r
Signature x
Certificate x
312
Sign Function
316
Certificate Generator
Private Key x
Digest x
Signature cx
310
Secure Hash Function
314
Sign Function
Software Program x
Public Key x
Root Private Key r

FIG. 3A

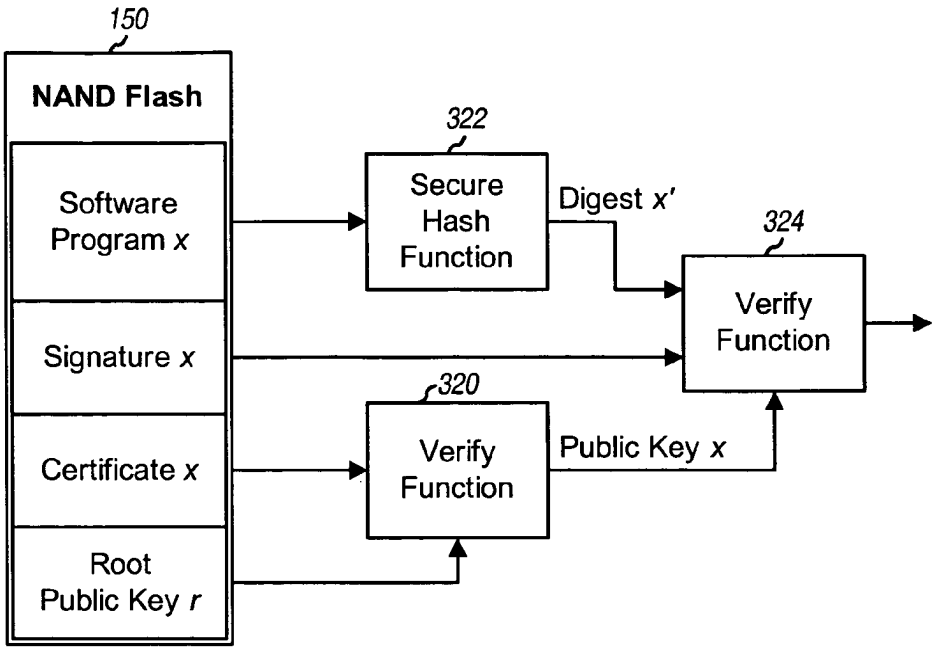

150
NAND Flash
Software Program x
Signature x
Certificate x
Root Public Key r
322
Secure Hash Function
Digest x'
324
Verify Function
320
Verify Function
Public Key x

FIG. 3B

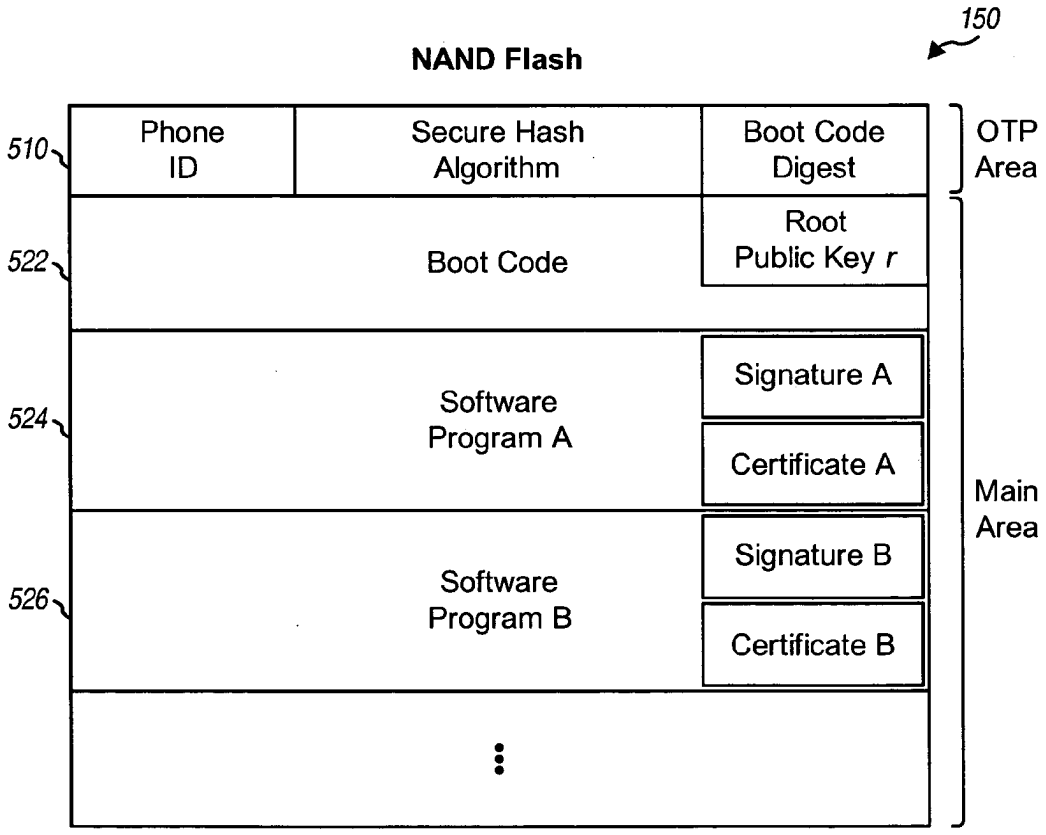

150
NAND Flash
510
Phone ID
Secure Hash Algorithm
Boot Code Digest
OTP Area
522
Boot Code
Root Public Key r
524
Software Program A
Signature A
Certificate A
526
Software Program B
Signature B
Certificate B
Main Area

FIG. 5

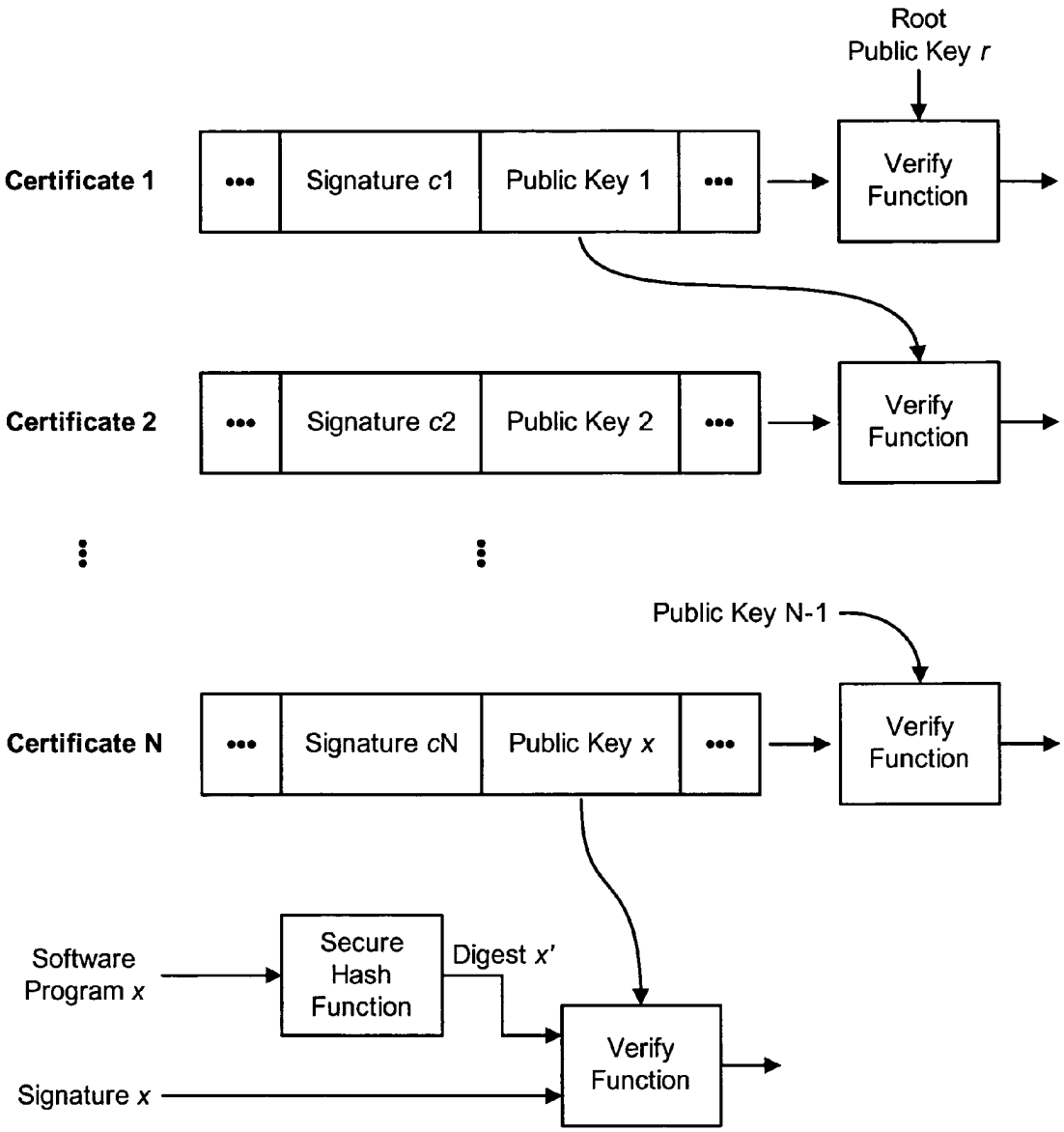

Root
Public Key r
Certificate 1
Signature c1
Public Key 1
Verify Function
Certificate 2
Signature c2
Public Key 2
Verify Function
Public Key N-1
Certificate N
Signature cN
Public Key x
Verify Function
Software Program x
Secure Hash Function
Digest x'
Verify Function
Signature x

FIG. 4

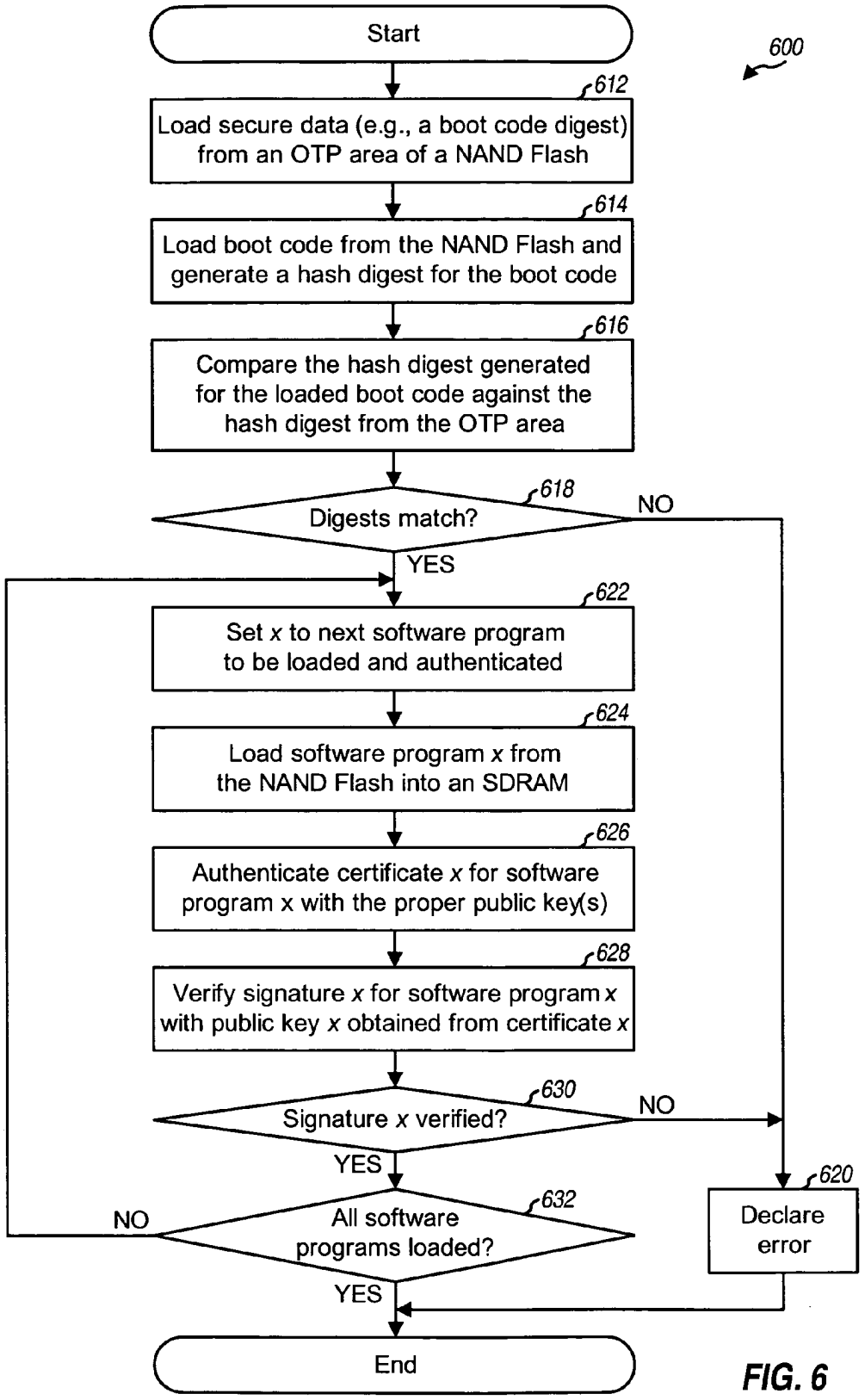

Start
600
612
Load secure data (e.g., a boot code digest) from an OTP area of a NAND Flash
614
Load boot code from the NAND Flash and generate a hash digest for the boot code
616
Compare the hash digest generated for the loaded boot code against the hash digest from the OTP area
618
Digests match?
NO
YES
622
Set x to next software program to be loaded and authenticated
624
Load software program x from the NAND Flash into an SDRAM
626
Authenticate certificate x for software program x with the proper public key(s)
628
Verify signature x for software program x with public key x obtained from certificate x
630
Signature x verified?
NO
YES
632
All software programs loaded?
NO
YES
620
Declare error
End

FIG. 6

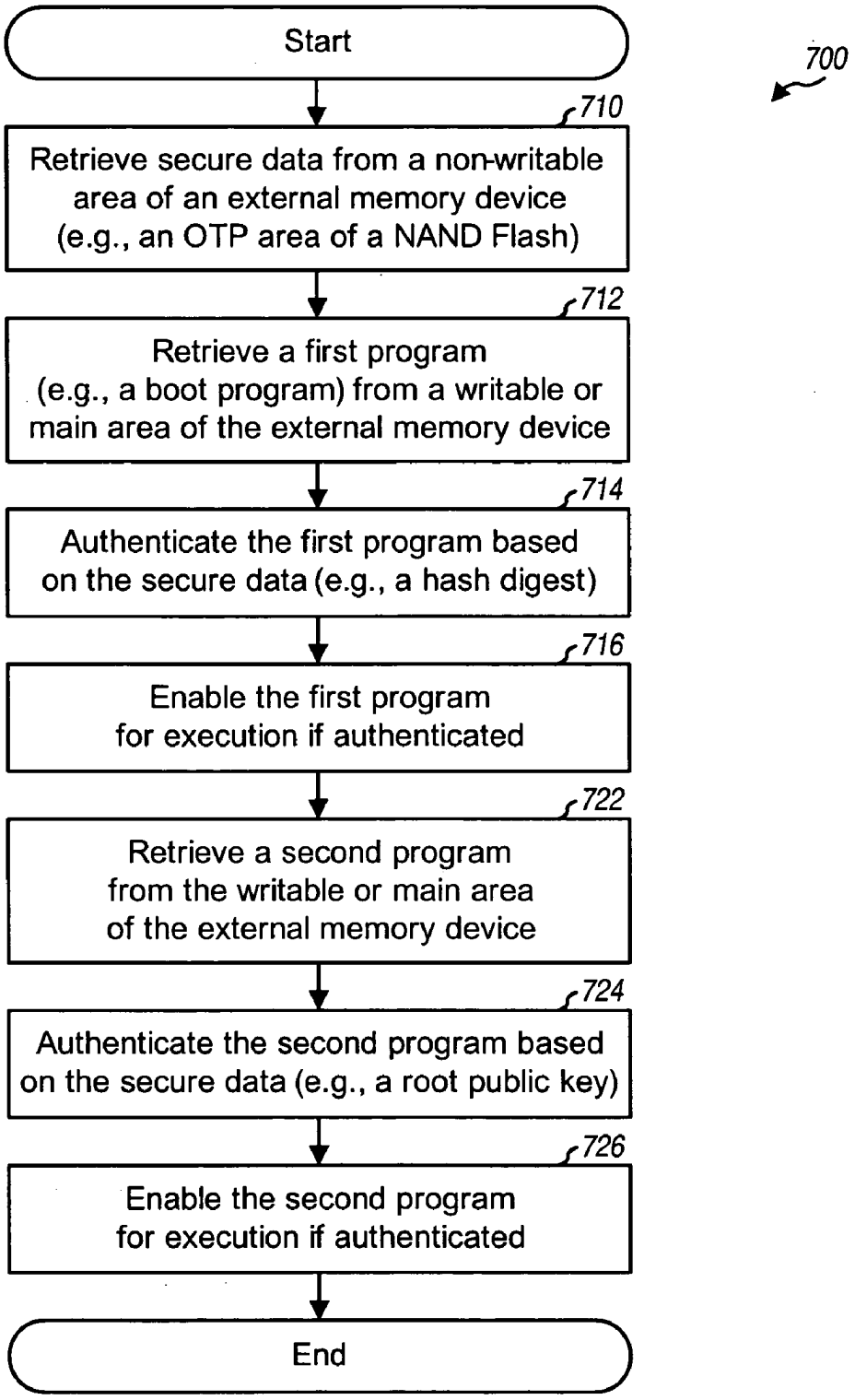

Start
700
710
Retrieve secure data from a non-writable area of an external memory device (e.g., an OTP area of a NAND Flash)
712
Retrieve a first program (e.g., a boot program) from a writable or main area of the external memory device
714
Authenticate the first program based on the secure data (e.g., a hash digest)
716
Enable the first program for execution if authenticated
722
Retrieve a second program from the writable or main area of the external memory device
724
Authenticate the second program based on the secure data (e.g., a root public key)
726
Enable the second program for execution if authenticated
End

FIG. 7

METHOD AND APPARATUS FOR SECURELY BOOTING FROM AN EXTERNAL STORAGE DEVICE

BACKGROUND

[0001] I. Field

[0002] The present disclosure relates generally to electronics, and more specifically to techniques for securely booting an electronics device from an external storage device.

[0003] II. Background

[0004] An electronics device (e.g., a cellular phone) typically operates based on software and/or firmware that control the hardware within the device and support various designed functions. The software and/or firmware may be stored in an external non-volatile memory, loaded into a faster internal memory and/or an external volatile memory during power up, and executed by a processor. The external and internal memories are typically selected to provide the desired storage capacity and access capability and to be as economical as possible.

[0005] In many instances, it is desirable or necessary to ascertain whether the software and/or firmware retrieved from the external memory are valid and authorized for execution. For example, different software versions with different features may be available for different levels of service subscription. It may then be desirable to prevent an electronics device with a basic subscription from loading and executing a software version with enhanced functionality intended for a premium subscription. As another example, it may be desirable to prevent tampering with the software and/or firmware to enable features that are not authorized. In addition, far worse consequences such as network destruction and/or blackout may be caused by hostile parties.

SUMMARY

[0006] There is therefore a need in the art for techniques to store software and/or firmware in economical memories and to check the validity of the software and/or firmware retrieved from these memories.

[0007] Techniques to securely boot up an electronics device (e.g., a cellular phone) from an external storage device (e.g., a NAND Flash memory device) are described herein. Secure boot refers to a process of loading software programs from an external storage device and checking the validity of the loaded software programs. A software program may comprise software code, firmware code, or a combination of both.

[0008] The techniques described herein may utilize a non-writable area on the external storage device to store secure data that is practically non-alterable. The non-writable area may be a one-time programmable (OTP) area, a one-time write (OTW) area, etc. As used herein, secure data includes data that is not easily altered (e.g., data stored in an OTP area or an OTW area) as well as data that is authenticated by the not easily altered data. The secure data may comprise one or more hash digests, signatures, certificates, cryptographic keys, etc. , or a combination thereof. The techniques utilize the secure data to authenticate software programs loaded from the external storage device, to allow authenticated programs to execute, and to prevent unauthorized programs from executing.

[0009] In an embodiment of the secure boot, secure data is initially retrieved from a non-writable area of an external memory device (e.g., an OTP area of a NAND Flash). A first program (e.g., a boot program) is retrieved from a writable or main area of the external memory device and authenticated based on the secure data. For example, the secure data may comprise a first hash digest. The first program may then be authenticated by (1) hashing the first program to generate a second hash digest and (2) comparing the first and second hash digests. The first program is enabled for execution if authenticated.

[0010] A second program may be retrieved from the main area of the external memory device and authenticated based on the secure data. For example, the secure data may comprise a cryptographic key, which may be stored in the non-writable area or authenticated by the data stored in the non-writable area. The second program may then be authenticated by (1) retrieving a certificate containing a first signature and a public key, (2) retrieving a second signature for the second program, (3) verifying the first signature with the cryptographic key to authenticate the certificate, and (4) verifying the second signature with the public key from the certificate to authenticate the second program. The second program is enabled for execution if authenticated. Additional programs may be retrieved and authenticated. Each program may be authenticated using a secure hash function, a digital signature, and/or some other cryptographic technique.

[0011] Various aspects and embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The features and nature of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly throughout.

[0013] FIG. **1** shows a block diagram of a wireless communication device.

[0014] FIGS. **2**A and **2**B show a process to authenticate a boot program using a secure hash function.

[0015] FIGS. **3**A and **3**B show a process to authenticate a software program using digital signature.

[0016] FIG. **4** shows multiple levels of authentication with certificates.

[0017] FIG. **5** shows a NAND Flash with an OTP area and a main area.

[0018] FIG. **6** shows a process for performing a secure boot from the NAND Flash.

[0019] FIG. **7** shows a process for authenticating software programs.

DETAILED DESCRIPTION

[0020] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any

embodiment or design described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments or designs.

[0021] The secure boot techniques described herein may be used for various electronics devices such as those used for wireless communication, personal electronics, computing, networking, etc. The techniques may also be used with various storage devices having non-writable area, such as solid-state memory devices, memory cards, hard disks, compact discs (CDs), etc. A non-writable area is an area of a storage device that cannot be over-written with data. For example, the non-writable area may be an OTP area that can be programmed with data only once. The non-writable area may be used to store secure data that supports the secure boot process. For clarity, the techniques are described below for a wireless communication device having a NAND Flash memory with an OTP area.

[0022] FIG. **1** shows a block diagram of a wireless communication device **100**, which may be a cellular phone, a handset, a handheld device, a wireless module, a personal digital assistant (PDA), a terminal, a modem, or some other apparatus or device. Wireless device **100** is capable of providing bidirectional communication with one or more wireless communication systems via a receive path and a transmit path. On the receive path, signals transmitted by base stations are received by an antenna **112** and provided to a receiver (RCVR) **114**. Receiver **114** conditions and digitizes the received signal and provides input samples to a digital section **120** for further processing. On the transmit path, a transmitter (TMTR) **116** receives and conditions data to be transmitted by wireless device **100** and generates a modulated signal, which is transmitted via antenna **112** to the base stations.

[0023] Digital section **120** includes various processing, interface, and memory units that support digital processing for wireless device **100**. For the embodiment shown in FIG. **1**, digital section **120** includes a modem processor **122**, an application processor **124**, a controller/processor **130**, a static random access memory (SRAM) **132**, a NAND Flash controller **140**, and a synchronous dynamic RAM (SDRAM) controller **142**, all of which may communicate with one another via one or more buses **134**. Modem processor **122** performs processing for data transmission and reception (e.g., encoding, modulation, demodulation, decoding, etc). Application processor **124** may perform processing for audio, video, graphics, and/or other applications such as hash and verification algorithms. Controller/processor **130** may direct the operation of various units within digital section **120**. SRAM **132** stores program codes and data used by the controllers and processors within digital section **120**.

[0024] NAND Flash controller **140** facilitates transfer of data between a NAND Flash **150** and digital section **120**. SDRAM controller **142** facilitates transfer of data between an SDRAM **152** and digital section **120**. Controller/processor **130** may also direct the operation of NAND Flash controller **140** and/or SDRAM controller **142**. Controller/processor **130** may direct data transfer from NAND Flash **150** to SRAM **132** and may further facilitate data transfer between NAND Flash **150** and SDRAM **152** during boot up, e.g., when wireless device **100** is powered on.

[0025] NAND Flash **150** and SDRAM **152** are memory devices that are external to digital section **120** and provide mass storage for the processing units within digital section **120**. NAND Flash **150** provides non-volatile storage for program codes and data used by digital section **120**. NAND Flash **150** may also be replaced with other types of non-volatile memory. SDRAM **152** provides storage with random access capability for program codes and data used by digital section **120**. SDRAM **152** may also be replaced with other types of volatile memory (e.g., SRAM, DRAM, and so on) and/or non-volatile memory (e.g., NOR Flash).

[0026] In general, digital section **120** may include any number of processing, interface, and memory units. The controllers and processors within digital section **120** may be implemented with one or more digital signal processors (DSPs), micro-processors, reduced instruction set computing (RISC) processors, complex instruction set computing (CISC) processors, etc. Digital section **120** may be implemented on one or more application specific integrated circuits (ASICs) and/or some other types of integrated circuit (IC).

[0027] As shown in FIG. **1**, wireless device **100** may utilize a memory architecture with different types of memory. SRAM and SDRAM are volatile memories that lose their data once power is removed. SRAM and SDRAM may be accessed in a random manner and are commonly used as the main run-time memory. Flash is a non-volatile memory that can retain its data even after power is removed. NAND Flash, which is one type of Flash, has large storage capacity, good speed for continued memory access, and low cost. However, NAND Flash has poor performance for random memory access and is typically accessed in units of pages, one page at a time, with each page being of a particular size (e.g., 512 bytes).

[0028] The memory architecture shown in FIG. **1** incorporates both NAND Flash and SRAM/SDRAM and is capable of providing large storage capacity with random access at reduced cost. For this memory architecture, program codes may be permanently stored in the NAND Flash. Upon being powered on, the wireless device performs a boot that entails (among other things) transferring the program codes from the NAND Flash to the SRAM/SDRAM.

[0029] The NAND Flash may store various software programs that control the hardware within the wireless device and further support various designed functions and features. A software program (or simply, a program) may comprise software codes, firmware codes, or a combination thereof. Firmware typically refers to program codes that are embedded in a hardware device such as a Flash or a read-only memory (ROM). Software typically refers to program codes that can be modified more easily than firmware.

[0030] The software programs stored in the NAND Flash may comprise a boot program that controls the boot up process and higher-layer programs that control the operation of the hardware and support the desired features and functions. The boot program may also be referred to as a boot code, a boot loader, etc. The higher-layer programs may include, e.g., a hardware initialization program that initializes various pieces of hardware within the wireless device, an operating system that is responsible for direct control and management of the hardware and basic system operations, application programs that support various applications (e.g., audio, video, graphics, and gaming, etc.), and/or other software programs. These various software programs may

be dependent on one another and may be loaded in a sequential order during the boot up process.

[0031] The software programs may be programmed into the NAND Flash during manufacturing, downloaded into the NAND Flash during activation of the wireless device, etc. Regardless of how the software programs are loaded into the NAND Flash, it may be desirable or necessary to ascertain whether or not the software programs stored in the NAND Flash are authorized, to allow execution of programs that are authorized, and to prevent execution of programs that are unauthorized.

[0032] The techniques described herein support secure boot from an external storage device such as the NAND Flash. The secure boot checks each program retrieved from the NAND Flash and verifies whether the program is authorized for execution. The secure boot may be achieved using an OTP area of the NAND Flash and cryptographic techniques.

[0033] The NAND Flash includes a main area and an OTP area. The main area is a large area of the NAND Flash that can be written with data any number of times. The OTP area is typically a small area of the NAND Flash that can be programmed only once. The OTP area is for practical purposes non-alterable. The data stored in the OTP area is permanent and cannot be easily modified or tampered. The data from both the OTP area and the main area can be readily accessed or retrieved.

[0034] FIGS. **2**A and **2**B show an embodiment of a process to authenticate the boot code and a root public key r (described below) using a secure hash function. FIG. **2**A shows the processing performed at a source entity, e.g., a manufacturer of the wireless device. For the embodiment shown in FIG. **2**A, the boot code and the root public key r are used to form an input message that is hashed by a secure hash function **210** to generate a digest. The input message to secure hash function **210** may be any length, and the output digest is a pseudo-random bit string having a fixed length determined by the hash algorithm selected for use. Secure hash function **210** may implement SHA-**1** (Secure Hash Algorithm), SHA-**2** (which includes SHA-**224**, SHA-**256**, SHA-**384** and SHA-**512**), MD-**4** (Message Digest), MD-**5**, or some other secure hash algorithm known in the art. A secure hash algorithm has cryptographic properties so that the function between a message and its digest is irreversible, and the likelihood of two messages mapping to the same digest is very small. For the embodiment shown in FIG. **2**A, the boot code and the root public key r are stored in the main area of the NAND Flash, and the digest and the secure hash algorithm are stored in the OTP area of the NAND Flash. In other embodiments, the root public key r and/or the boot code may be stored in the OTP area of the NAND Flash.

[0035] FIG. **2**B shows the processing performed at the wireless device to authenticate the boot code and the root public key r. The boot code and the root public key r are retrieved from the NAND Flash and hashed by a secure hash function **220** to generate a digest. Secure hash function **220** implements the same secure hash algorithm used by secure hash function **210** at the source entity. This secure hash algorithm may be resident at the wireless device (not shown in FIG. **2**B) or may be retrieved from the OTP area of the NAND Flash (as shown in FIG. **2**B). The secure hash algorithm may also be stored in the form of code to be executed by a processor within ASIC **120**. A compare unit **222** receives the digest stored in the OTP area of the NAND Flash and the digest generated by secure hash function **220**, compares the stored digest against the generated digest, and declares that the boot code and the root public key r are authenticated if the two digests match. The digest stored in the OTP area cannot be easily tampered or replaced. The cryptographic properties of the secure hash algorithm ensure that the likelihood of another combination of boot code and root public key r mapping to the same digest stored in the OTP area is very small. Hence, any tampering with either the boot code or the root public key r by a third party can easily be detected by a mismatch between the generated digest and the stored digest.

[0036] FIGS. **3**A and **3**B show an embodiment of a process to authenticate software program x using a digital signature. Software program x may be the boot code or a higher-level program. This embodiment uses two sets of cryptographic keys: (1) a set of private and public keys to sign and authenticate software program x, which are referred to as private key x and public key x, and (2) a set of private and public keys to identify and authenticate the source entity, which are referred to as the root private and public keys r. The root private key r and private key x are secret and only known to the source entity. The root public key r is made available to the wireless device and is used to verify signatures generated with the root private key. Public key x is used to verify signatures generated with private key x.

[0037] FIG. **3**A shows the processing performed at the source entity. Software program x is hashed by a secure hash function **310** to generate a digest, which is called digest x. Secure hash function **310** may implement SHA-**1**, SHA-**2**, MD-**5**, or some other secure hash algorithm. A sign function **312** generates a signature over digest x using private key x. This signature is referred to as signature x. Sign function **312** may implement the RSA (Rivest, Shamir, and Adleman) algorithm, the Digital Signature Standard (DSS) algorithm, or some other cryptographic (digital signature or encryption) algorithm known in the art. Software program x and signature x may be stored in the main area of the NAND Flash.

[0038] A sign function **314** generates a signature over public key x and possibly other information using the root private key r. This signature is referred to as signature cx and is used to authenticate the source entity. Sign function **314** may implement the RSA, DSS, or some other cryptographic algorithm. Sign functions **312** and **314** may implement the same or different cryptographic algorithms. A certificate generator **316** forms a certificate containing signature cx, public key x, and possibly other information such as an identifier for the source entity, the cryptographic algorithm selected for use, the expiration date of the certificate, and so on. This certificate is referred to as certificate x and may be stored as an X.509 certificate or in some other format known in the art. Certificate x may be stored in the main area of the NAND Flash. The root public key r may be stored anywhere in the NAND Flash or may be made available to the wireless device in other manners, e.g., stored within the wireless device.

[0039] FIG. **3**B shows the processing performed at the wireless device to authenticate software program x. The root public key r and certificate x are retrieved from the NAND Flash. A verify function **320** extracts signature cx and public

key x from certificate x, verifies signature cx with the root public key r, and provides public key x if signature cx is verified. For the embodiment shown in FIGS. **2**A and **2**B, the root public key r is stored in the NAND Flash and is verified by the secure hash algorithm against the digest stored in the OTP area of the NAND Flash. Hence, any tampering with certificate x by a third party can be easily detected by signature cx not verifying.

[**0040**] Software program x is retrieved from the NAND Flash and hashed by a secure hash function **322** to generate a digest, which is referred to as digest x'. Secure hash function **322** implements the same secure hash algorithm used by secure hash function **310** at the source entity. A verify function **324** receives digest x' from secure hash function **322**, signature x from the NAND Flash, and public key x from verify function **320**. Verify function **324** verifies signature x with public key x and digest x' and indicates whether or not signature x is verified. Public key x is authenticated with the root public key r, which in turn is authenticated by the boot code digest stored in the OTP area of the NAND Flash. Hence, any tampering with software program x and/or signature x by a third party can be easily detected by signature x not verifying.

[**0041**] The embodiment shown in FIGS. **3**A and **3**B allows one root public key r to authenticate any number of software programs. A signature may be generated for each software program with a private key for that program, and a certificate may be generated for the program with the root private key r. The root public key r may be used to authenticate the certificate for each software program, and the public key within the authenticated certificate may be used to authenticate the program's signature.

[**0042**] FIG. **4** shows an embodiment of N levels of authentication with certificates, where N may be any positive value. For this embodiment, certificate **1** contains (1) signature cl that is generated with the root private key r, (2) public key **1** and (3) possibly other information that is not shown in FIG. **4**. In general, certificate n, for n=1, . . . , N, contains (1) signature cn that is generated with private key n−1, (2) public key n and (3) possibly other information. Private key **0** is the root private key r. Public key N may be public key x for software program x to be authenticated. For the first level of authentication, certificate **1** is authenticated by verifying signature cl with the root public key r. If signature cl is verified, then for each subsequent level n of authentication, certificate n for that level is authenticated by verifying signature cn with public key n−1 from the prior level. If all N levels are authenticated, then public key x may be used to authenticate software program x, as described above for FIG. **3**B.

[**0043**] Multiple levels of authentication may be used for a multi-tier cryptographic key hierarchy. Certificate **1** may be used to authenticate a root certificate authority (CA) that acts as the foundation of trust. Since the root certificate authority's private keys r are the foundation of trust, steps are taken to protect these private keys, and therefore their use is restricted. Additional levels of intermediate certificate authorities may be created which are more "expendable." Organizationally, the multi-tier key hierarchy is convenient because the verification chain of certificates may be generated by the organizations that produce the software programs. Hence, portions of the software programs loaded onto the wireless device may be individually customized by different wireless device manufacturers.

[**0044**] In another embodiment, a software program (which may be the boot code or a higher-level program) is signed with a private key, and the corresponding public key is stored in the OTP area of the NAND Flash.

[**0045**] In general, the software programs may be authenticated using secure hash, digital signature, encryption, and/or other cryptographic techniques. Authentication is achieved based on secure data that is stored in the OTP area of the NAND Flash. The data considered secure is integrity protected, i.e., not easily modified or tampered with. The secure data may include one or more digests, signatures, certificates, cryptographic keys, and so on, or any combination thereof.

[**0046**] FIG. **5** shows an embodiment of NAND Flash **150**, which includes an OTP area and a main area. For the embodiment shown in FIG. **5**, OTP area **510** stores an identifier for the wireless device (phone ID), the secure hash algorithm used for the boot code, and a hash digest generated by the source entity for the boot code and the root public key. The phone ID may be an Electronic Serial Number (ESN), a Mobile Equipment Identifier (MEID), or some other type of identifier that is unique to the wireless device. The phone ID may be used to ensure that the NAND Flash is used for the proper wireless device. The secure hash algorithm may be stored in the OTP area of the NAND Flash and retrieved for use by digital section **120** during the boot up process. Alternatively, the secure hash algorithm may be resident within digital section **120** and not stored in the OTP area. The boot code digest may be generated based on the boot code and the root public key, as shown in FIG. **2**A. The root public key is used to authenticate certificates generated by the source entity and is verified by the secure hash algorithm during boot to check for its validity. Alternatively, the root public key may be stored within the wireless device, e.g., inside digital section **120**.

[**0047**] The boot code is stored in a section **522** of the main area of the NAND Flash. The boot code is typically the first program to be loaded and executed after the secure data and hash algorithm verify the validity of the boot code during the boot up process. The boot code initializes and configures the wireless device and then retrieves, verifies, and executes higher level software programs. Software program A is stored in a section **524** of the main area of the NAND Flash. A signature and a certificate may be generated for software program A (e.g., as shown in FIG. **3**A) and stored in section **524** as signature A and certificate A, respectively. Software program A may be the second program to be loaded and executed during the boot up process, e.g., if the boot code is authenticated. Software program B is stored in a section **526** of the main area of the NAND Flash. A signature and a certificate may be generated for software program B (e.g., as shown in FIG. **3**A) and stored in section **526** as signature B and certificate B, respectively. Software program B may be the third program to be loaded and executed during the boot up process, e.g., if software program A is authenticated. Other software programs may also be stored in the NAND Flash. Each software program may include a signature and a certificate used to authenticate that software program.

[**0048**] In general, the NAND Flash may store any number of software programs and any type of software program. The

software programs may be loaded and executed in any order. In an embodiment, the software programs are loaded in a hierarchical or sequential order, e.g., the boot code first, then software program A, then software program B, etc. This sequential loading allows one program to authenticate another program. For example, software program A may contain basic functions that initialize the hardware within the wireless device. Software program B may contain custom functions and features that rely on the basic functions provided by software program A. Software program A may be generated by a designer of the wireless device, and software program B may be generated by a vendor or an original equipment manufacturer (OEM) to customize the wireless device.

[0049] FIG. **6** shows an embodiment of a process **600** for performing a secure boot from the NAND Flash. Process **600** may be performed, e.g., when the wireless device is powered on. Initially, secure data is loaded from the OTP area of the NAND Flash into the SRAM within the digital section (block **612**). The secure data may include any data used to authenticate the content of the NAND Flash. For the embodiment shown in FIG. **5**, the secure data includes the boot code digest and the secure hash algorithm. The secure data may include other types of data for other embodiments.

[0050] The boot code is then loaded from the NAND Flash into the SRAM and/or SDRAM (block **614**). A hash digest is generated based on the loaded boot code using the same secure hash algorithm used at the source entity for the boot code (also block **614**). Since the NAND Flash is more prone to bit errors, an error correction code (ECC) and/or error detection code may be used to reduce the probability of data error and to ensure data integrity when loading data from the NAND Flash.

[0051] The hash digest generated from the loaded boot code is then compared against the hash digest stored in the OTP area (block **616**). If the generated hash digest does not match the stored hash digest, as determined in block **618**, then an error is declared (block **620**), and the boot up process terminates. The user may be notified via an error message and/or other appropriate actions may be taken in block **620**.

[0052] If the generated and stored hash digests match and the answer is 'Yes' for block **618**, then the boot code is authenticated. The boot code may be executed and may control and/or direct the remaining boot up process. For example, the boot code may initiate NAND Flash controller **140** and SDRAM controller **142** to load the remaining software programs directly from the NAND Flash to the SDRAM.

[0053] Index x is set to the next software program to be loaded and authenticated (e.g., x=A for NAND Flash **150** in FIG. **5**) (block **622**). Software program x is then loaded from the NAND Flash into the SDRAM (block **624**). Certificate x and signature x for software program x are also loaded from the NAND Flash. Certificate x is authenticated with the proper public key(s), e.g., the root public key, as described above for FIGS. **3**B and **4** (block **626**). If certificate x is authenticated, then signature x is verified with the loaded software program x and public key x obtained from certificate x, as also described above for FIGS. **3**B and **4** (block **628**).

[0054] A determination is then made whether signature x is verified (block **630**). If the answer is 'No', then an error is declared and/or other actions may be taken (block **620**), and the boot up process terminates. Otherwise, if signature x is verified, then software program x is allowed to execute. Software program x and/or the boot code may load the next software program. A determination is then made whether all software programs have been loaded (block **632**). If the answer is 'No', then the process returns to block **622** to load the next software program. Otherwise, if all software programs have been loaded, then the process terminates.

[0055] For the embodiment shown in FIG. **6**, the software programs may be loaded in a hierarchical order. Each software program may be authenticated by a prior program based on the cryptographic data (e.g., signature, certificate, and/or cryptographic key) stored for that software program. The authentication process may utilize secure data stored in the OTP area. The authentication process may originate from the secure data (e.g., the root public key, which may be a part of, or authenticated by, the secure data stored in the OTP area) and may chain up any number of levels. Each authenticated program is allowed to execute and may initialize the appropriate hardware within the wireless device. Each authenticated program may also be trusted to authenticate other higher-level program(s). All programs that are authenticated back to the root can be trusted.

[0056] The load-and-authenticate process may continue until all pertinent programs have been loaded from the NAND Flash to the SDRAM. The operating system may start processes as soon as a sufficient number of programs have been loaded, without having to wait until all programs are loaded into the SDRAM. After the last program has been loaded, the wireless device is fully functional.

[0057] The hash digest for the boot code is generated based on the entire boot code, as shown in FIG. **2**A. The signature for software program x is generated based on digest x, which is generated based on the entire software program, as shown in FIG. **3**A. The authentication of a given software program (which may be the boot code or a higher-level program) may be expedited by performing the hash computation on the fly as the software program is loaded from the NAND Flash.

[0058] Data is read from the NAND Flash in units of pages, one page at a time, with each page being of a particular size (e.g., 512 bytes). To read a page of data from the NAND Flash, the NAND Flash is first activated, a read command is sent to the NAND Flash, and a page address is also sent to the NAND Flash. The selected page of data is then transferred from a NAND array to a NAND buffer within the NAND Flash. This page transfer takes some amount of time. When the page transfer is completed, the NAND Flash indicates that it is ready by bringing a Ready/Busy signal to logic high. At this point, the page of data may be read from the NAND Flash by providing a read clock.

[0059] In an embodiment, a hash digest is generated by hashing one page of data at a time. After a page of data has been loaded from the NAND Flash, a command to read the next page is sent to the NAND Flash. While the NAND Flash is busy transferring the next page from the NAND Flash's cell array to the NAND Flash's internal buffer, the hash digest is computed (e.g., by processor **124** in FIG. **1**) for the page just loaded. Once the last page has been loaded from the NAND Flash, the hash computation is performed for the last page, and the hash digest is generated shortly

thereafter. Since a software program may be stored in many pages, computing the hash digest as each page is loaded may substantially shorten the amount of time to perform the hash, which may shorten the boot up process.

[0060] For clarity, the secure boot techniques have been described with secure data stored in an OTP area. In general, secure data may be stored in any secure area of a storage device. A secure area is an area that is non-writable and not easily altered or modified. For example, secure data may be stored in an OTP area, a one-time write (OTW) area, a read-only memory (ROM) area, a lock-able area with a lock control to prevent writing to the area, or some other non-writable area.

[0061] For clarity, the secure boot techniques have been described for a NAND Flash having an OTP area. NAND Flash have various desirable features such as high storage capacity, low cost, good erase and program characteristics, good data transfer speed for continued access, and so on. The techniques may also be used for other types of memory devices (e.g., a NOR Flash) and other types of storage devices (e.g., memory cards, hard disks, compact discs (CDs), and so on). For all of these storage devices, the secure data stored in the non-writable (e.g., OTP) area may be trusted to a sufficient degree and may be used as the secure root for authenticating software programs stored in the main area of the storage devices.

[0062] The secure boot techniques may be used for a wireless device that may communicate with one or more wireless wide area network (WEANS), wireless local area networks (PLANS), wireless personal area networks (SPANS), and/or other wireless networks. A WAN may be a Code Division Multiple Access (COMA) network, a Global System for Mobile Communications (GEM) network, a Universal Mobile Telecommunications System (UMPS) network, etc. A COMA network implements coma2000, which covers IS-95, IS-2000, IS-856, etc. A UMPS network implements Wideband-COMA (W-COMA). W-COMA and GEM are described in documents from a consortium named "3rd Generation Partnership Project" (3GPP). coma2000 is described in documents from a consortium named "3rd Generation Partnership Project 2" (3GPP2). 3GPP and 3GPP2 documents are publicly available. The secure boot techniques may also be used for other electronics devices.

[0063] FIG. 7 shows an embodiment of a process **700** for authenticating software programs in an electronics device. Secure data is retrieved from a non-writable area of an external memory device (e.g., an OTP area of a NAND Flash) (block **710**). A first program (e.g., a boot program) is retrieved from a writable or main area of the external memory device (block **712**) and authenticated based on the secure data (block **714**). For example, the secure data may comprise a first hash digest along with the hash algorithm to be executed. The first program may then be authenticated by (1) hashing the first program to generate a second hash digest and (2) comparing the first and second hash digests. The first program is enabled for execution if authenticated (block **716**).

[0064] A second program may be retrieved from the writable or main area of the external memory device (block **722**) and authenticated based on the secure data (block **724**). For example, the secure data may comprise a cryptographic key. The second program may then be authenticated by (1) retrieving a certificate containing a first signature and a public key from either the writable or non-writable area of the external memory device, (2) retrieving a second signature for the second program from either the writable or non-writable area, (3) verifying the first signature with the cryptographic key to authenticate the certificate, and (4) verifying the second signature with the public key from the certificate to authenticate the second program. The second program is enabled for execution if authenticated (block **726**). Additional programs may be retrieved and authenticated.

[0065] The secure boot techniques described herein may be implemented by various means. For example, these techniques may be implemented in hardware, firmware, software, or a combination thereof. For a hardware implementation, the processing units used to perform secure boot may be implemented within one or more ASICs, DSPs, digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, electronic devices, other electronic units designed to perform the functions described herein, or a combination thereof.

[0066] The techniques may also be implemented with firmware and/or software modules (e.g., procedures, functions, etc.) that perform the functions described herein. The modules may be stored in a memory (e.g., SRAM **132**, NAND Flash **150**, and/or SDRAM **152** in FIG. **1**) and executed by a processor (e.g., processor **130**).

[0067] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

What is claimed is:

1. An apparatus comprising:

at least one processor configured to retrieve secure data from a non-writable area of an external memory device, to retrieve a first program from a writable area of the external memory device, to authenticate the first program based on the secure data, and to enable execution of the first program if authenticated; and

an internal memory coupled to the at least one processor.

2. The apparatus of claim 1, wherein the secure data comprises a first hash digest, and wherein the at least one processor is configured to hash the first program to generate a second hash digest, and to compare the first and second hash digests to authenticate the first program.

3. The apparatus of claim 1, wherein the at least one processor is configured to verify a signature for the first program with a cryptographic key to authenticate the first program, wherein the cryptographic key is obtained from or authenticated by the secured data.

4. The apparatus of claim 1, wherein the at least one processor is configured to retrieve a first signature for the first program and a certificate comprising a second signature

and a public key from the external storage device, to verify the second signature with a cryptographic key to authenticate the certificate, wherein the cryptographic key is obtained from or authenticated by the secured data, and to verify the first signature with the public key to authenticate the first program.

5. The apparatus of claim 1, wherein the first program is a boot code that boots up the apparatus.

6. The apparatus of claim 1, wherein the at least one processor is configured to retrieve a second program from the writable area of the external memory device, to authenticate the second program based on the secure data, and to enable execution of the second program if authenticated.

7. The apparatus of claim 6, wherein the second program is authenticated by the first program.

8. The apparatus of claim 6, wherein the at least one processor is configured to retrieve a third program from the writable area of the external memory device, to authenticate the third program based on the secure data, and to enable execution of the third program if authenticated.

9. The apparatus of claim 8, wherein the third program is authenticated by the second program.

10. The apparatus of claim 1, wherein the external storage device is a NAND Flash device.

11. The apparatus of claim 1, wherein the external storage device is a NOR Flash device.

12. The apparatus of claim 1, wherein the non-writable area is a one-time programmable (OTP) area.

13. A method comprising:

retrieving secure data from a non-writable area of an external memory device;

retrieving a first program from a writable area of the external memory device;

authenticating the first program based on the secure data; and

enabling execution of the first program if authenticated.

14. The method of claim 13, wherein the secure data comprises a first hash digest, and wherein the authenticating the first program comprises

hashing the first program to generate a second hash digest, and

comparing the first and second hash digests to authenticate the first program.

15. The method of claim 13, wherein the authenticating the first program comprises

retrieving a first signature for the first program and a certificate comprising a second signature and a public key from the external storage device,

verifying the second signature with a cryptographic key to authenticate the certificate, wherein the cryptographic key is obtained from or authenticated by the secured data, and

verifying the first signature with the public key to authenticate the first program.

16. The method of claim 13, further comprising:

retrieving a second program from the writable area of the external memory device;

authenticating the second program based on the secure data; and

enabling execution of the second program if authenticated.

17. An apparatus comprising:

means for retrieving secure data from a non-writable area of an external memory device;

means for retrieving a first program from a writable area of the external memory device;

means for authenticating the first program based on the secure data; and

means for enabling execution of the first program if authenticated.

18. The apparatus of claim 17, wherein the secure data comprises a first hash digest, and wherein the means for authenticating the first program comprises

means for hashing the first program to generate a second hash digest, and

means for comparing the first and second hash digests to authenticate the first program.

19. The apparatus of claim 17, wherein the means for authenticating the first program comprises

means for retrieving a first signature for the first program and a certificate comprising a second signature and a public key from the external storage device,

means for verifying the second signature with a cryptographic key to authenticate the certificate, wherein the cryptographic key is obtained from or authenticated by the secured data, and

means for verifying the first signature with the public key to authenticate the first program.

20. The apparatus of claim 17, further comprising:

means for retrieving a second program from the writable area of the external memory device;

means for authenticating the second program based on the secure data; and

means for enabling execution of the second program if authenticated.

21. A wireless communication device comprising:

at least one processor configured to retrieve secure data from a one-time programmable (OTP) area of a NAND Flash device, to retrieve a boot program from a main area of the NAND Flash device, to authenticate the boot program based on the secure data, and to enable execution of the boot program if authenticated; and

a memory coupled to the at least one processor.

22. The apparatus of claim 21, wherein the secure data comprises a first hash digest, and wherein the at least one processor is configured to hash the boot program to generate a second hash digest, and to compare the first and second hash digests to authenticate the boot program.

23. The apparatus of claim 22, wherein the at least one processor is configured to retrieve the boot program from the main area of the NAND Flash device one page at a time, and to hash the boot program, one page at a time as the page is retrieved from the NAND Flash device, to generate the second digest.

24. The apparatus of claim 21, wherein the at least one processor is configured to execute the boot program if authenticated, to retrieve a second program from the main area of the NAND Flash device, to authenticate the second program based on the secure data, and to enable execution of the second program if authenticated.

25. The apparatus of claim 24, wherein the at least one processor is configured to retrieve a certificate comprising a first signature and a public key, to retrieve a second signature for the second program, to verify the first signature with a cryptographic key to authenticate the certificate, wherein the cryptographic key is obtained from or authenticated by the secured data, and to verify the second signature with the public key to authenticate the second program.

26. The apparatus of claim 25, wherein the at least one processor is configured to retrieve the second program from the main area of the NAND Flash device one page at a time, to hash the second program, one page at a time as the page is retrieved from the NAND Flash device, to generate a hash digest, and to verify the second signature with the public key and the hash digest.

* * * * *

US 20060112266A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0112266 A1

Little et al. (43) Pub. Date: May 25, 2006

(54) METHOD AND DEVICE FOR AUTHENTICATING SOFTWARE

(75) Inventors: **Herbert A. Little**, Waterloo (CA); **Ryan J. Hickey**, Waterloo (CA)

Correspondence Address:
DIMOCK STRATTON LLP
20 QUEEN STREET WEST SUITE 3202, BOX 102
TORONTO, ON M5H 3R3 (CA)

(73) Assignee: **RESEARCH IN MOTION LIMITED**, Waterloo (CA)

(21) Appl. No.: **11/046,943**

(22) Filed: **Feb. 1, 2005**

(30) **Foreign Application Priority Data**

Nov. 22, 2004 (EP) 04105984.1

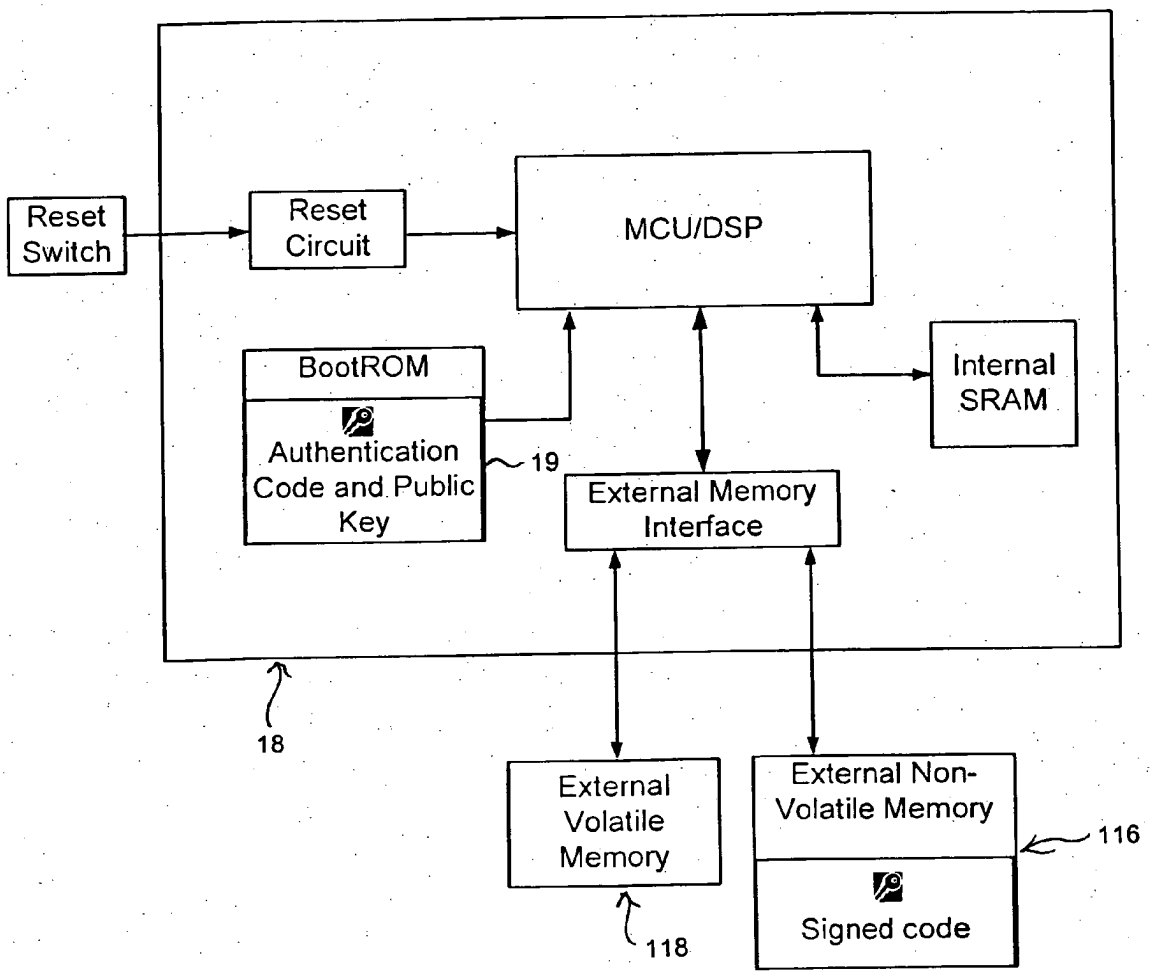
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/161**

(57) **ABSTRACT**

A method and device for authenticating software stored in non-volatile memory in a data processing device. The processor comprises an internal immutable memory, preferably a read only memory (ROM), and during the boot up procedure the software in external memory is authenticated using code that is stored in the internal ROM. The on-chip ROM is physically integrated with the processor itself, so the code stored in ROM can neither be tampered with nor replaced, and can therefore be assumed at all times to be authentic. Thus, in the method and device of the invention known good code is used to authenticate the untrusted code in external memory, so the integrity of the system is significantly improved.



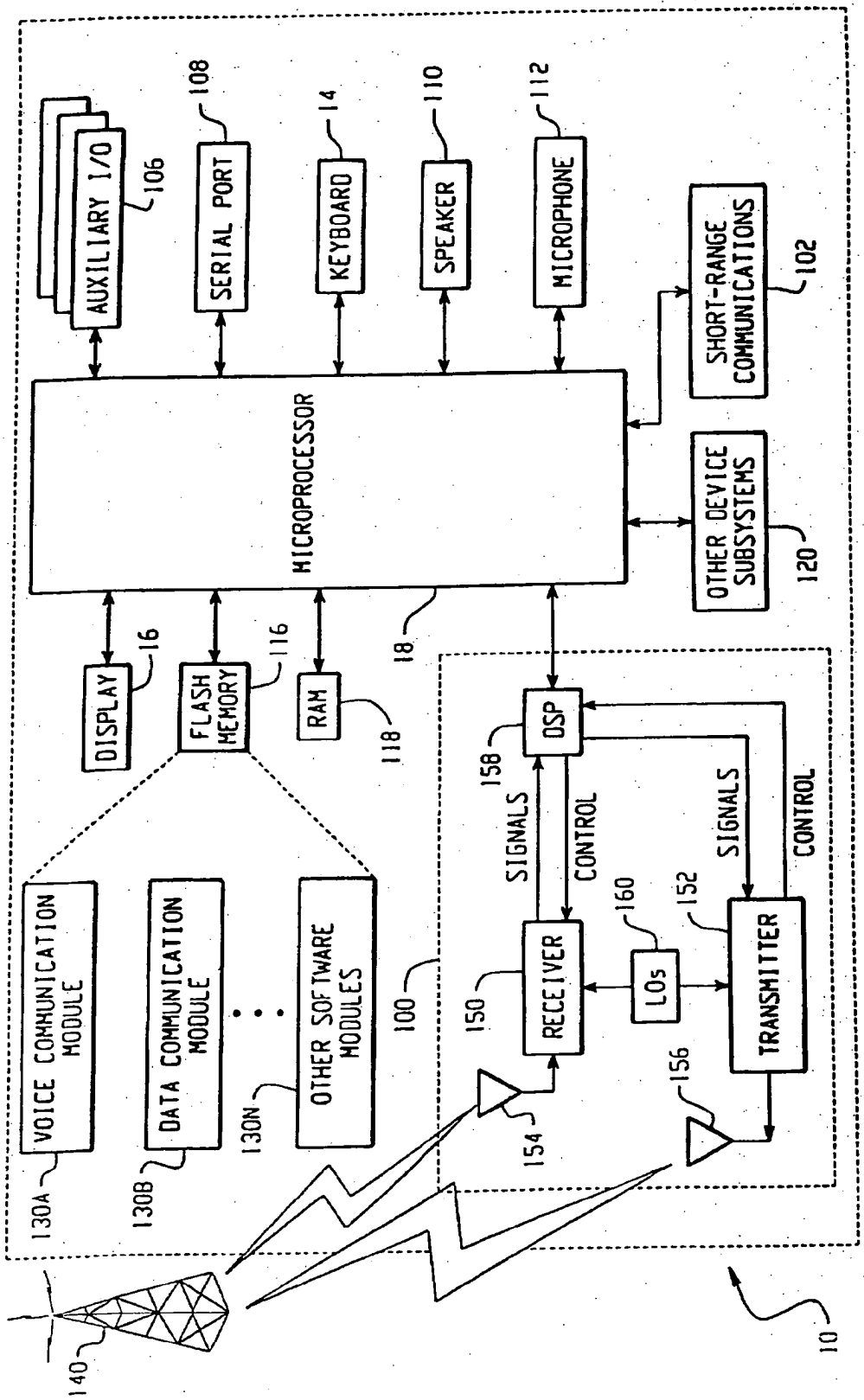

AUXILIARY I/O
106
SERIAL PORT
108
KEYBOARD
14
SPEAKER
110
MICROPHONE
112
SHORT-RANGE COMMUNICATIONS
102
MICROPROCESSOR
OTHER DEVICE SUBSYSTEMS
120
DISPLAY
16
FLASH MEMORY
116
RAM
118
18
DSP
158
SIGNALS
CONTROL
SIGNALS
CONTROL
160
152
VOICE COMMUNICATION MODULE
DATA COMMUNICATION MODULE
OTHER SOFTWARE MODULES
130N
100
150
RECEIVER
LOs
TRANSMITTER
156
154
130A
130B
140
10

FIG. 1

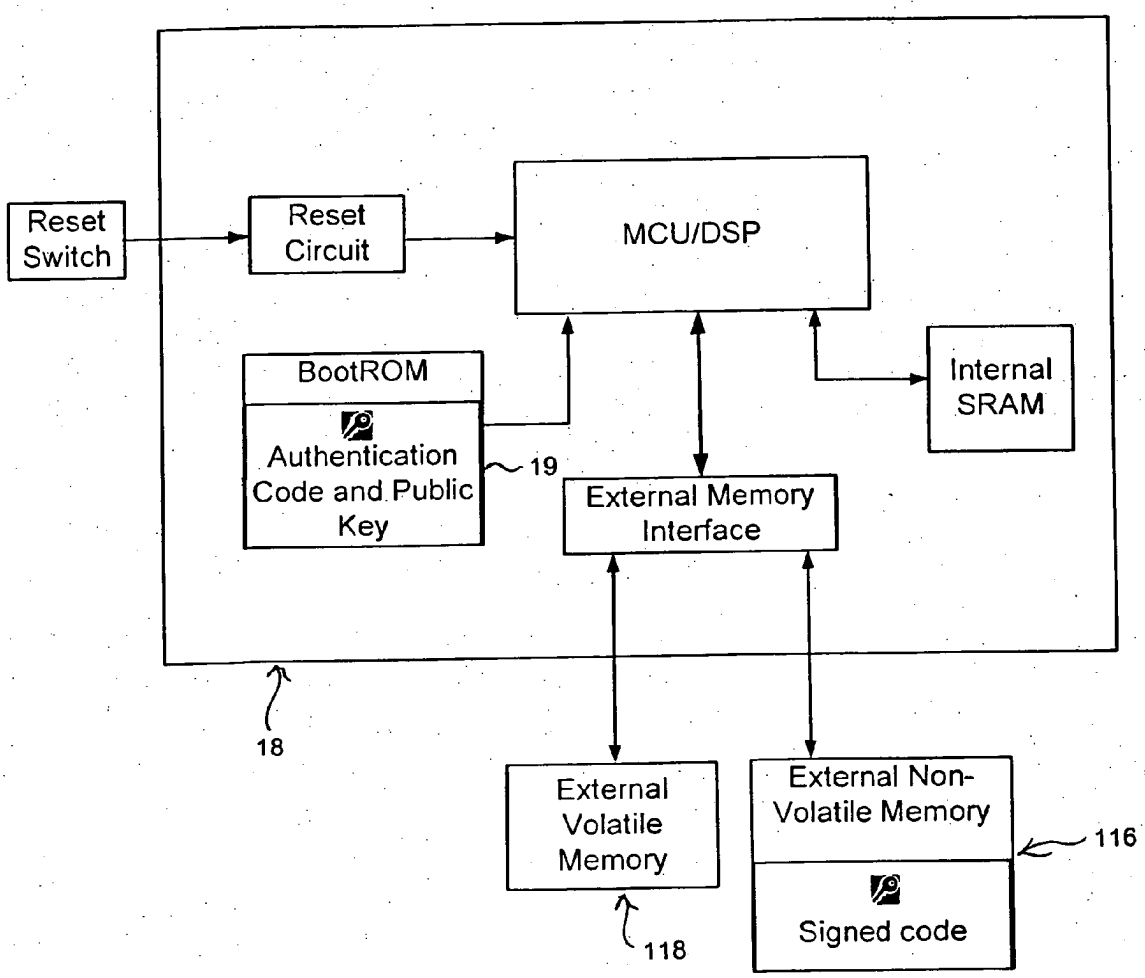

Reset Switch
Reset Circuit
MCU/DSP
BootROM
Authentication Code and Public Key
19
Internal SRAM
External Memory Interface
18
External Volatile Memory
118
External Non-Volatile Memory
116
Signed code

FIG. 2

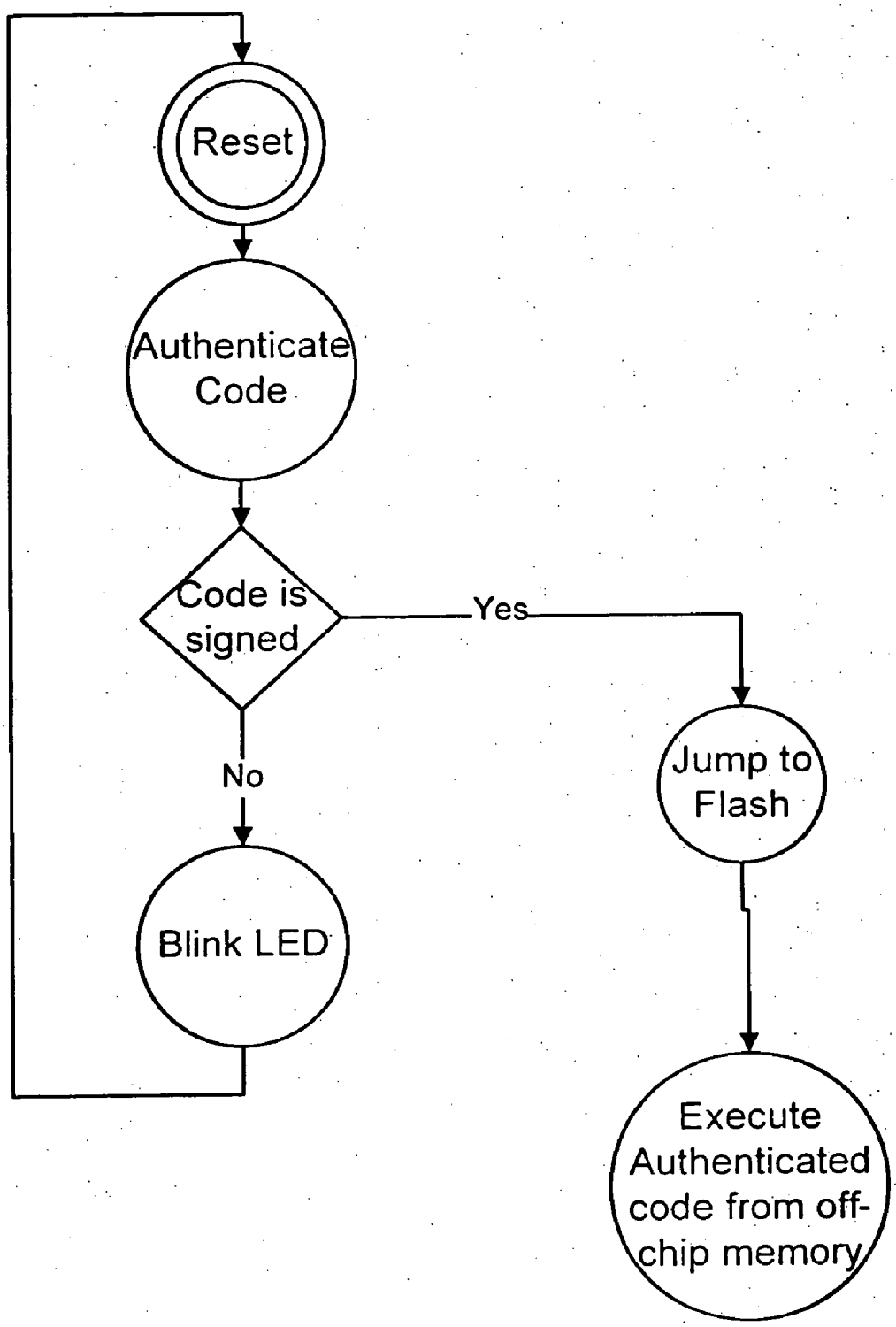

Reset
Authenticate Code
Code is signed
Yes
No
Jump to Flash
Blink LED
Execute Authenticated code from off-chip memory

FIG. 3

METHOD AND DEVICE FOR AUTHENTICATING SOFTWARE

FIELD OF THE INVENTION

[0001] This invention relates to security in data processing systems. In particular, this invention relates to a method and device for the authentication of software stored in non-volatile memory.

BACKGROUND OF THE INVENTION

[0002] The use of portable data processing systems has increased significantly in recent years. In addition to so called "laptop" and "tablet" computers, there is a growing popularity in handheld data processing devices, often called a "personal digital assistant" or "PDA." All of these devices are capable of storing a significant amount of user data, including calendar, address book, tasks and numerous other types of data for business and personal use. Most handheld data processing devices have the ability to connect to a personal computer for data exchange, and many are equipped for wireless communications using, for example, conventional email messaging systems.

[0003] Depending upon the user's needs much of this data can be highly sensitive in nature, especially for example in a government, military or commercial context. Accordingly, protection of the data in such a device is an important consideration. The integrity of a secure system relies entirely on the authenticity of its program code. It is possible to attack these types of systems by replacing the device's program code with malicious code. Thus, in any system that values security, when the embedded system boots up and the processor begins executing boot code, the boot code will immediately authenticate the software before executing any program code.

[0004] The fundamental deficiency in this method of software authentication is that the initial boot code is usually stored in off chip non-volatile memory and therefore cannot itself be trusted, because it is possible for an attacker to replace the non-volatile memory chip with another compatible chip containing malicious code.

[0005] It would accordingly be advantageous to provide a method of authenticating software in which the boot code that performs the authentication process can be guaranteed to be authentic. The authentication process itself can then be trusted, and the program code can be determined with certainty not to have been tampered with.

SUMMARY OF THE INVENTION

[0006] The present invention accordingly provides a method and apparatus for authenticating software stored in external non-volatile memory using a hardware mechanism before the software is allowed to run on the processor.

[0007] According to the method and apparatus of the invention, in the preferred embodiment of the invention, during the boot up procedure the code in external memory is authenticated using code that is stored in on-chip (internal) immutable memory, preferably a read only memory (ROM). The internal memory is physically integrated into the processor itself, so the code stored in the internal memory can neither be tampered with nor replaced, and can therefore be assumed at all times to be authentic. The public key needed for the authentication process is also stored in the internal memory.

[0008] In the preferred embodiment of the invention the boot procedure is as follows:

[0009] 1) Following a reset signal (e.g. when the device is activated), rather than fetching instructions from an untrustworthy source such as an external NOR or NAND flash memory chip, the processor executes code read directly from the internal memory.

2) The code in the internal memory first runs a program that authenticates all or a portion of the external memory.

3) If the code is authenticated successfully using the public key stored in the internal memory, the authentication program jumps to code stored in external memory.

4) If the code authentication is unsuccessful, the program resets the processor. Where the external memory has been tampered with, this results in an endless resetting loop, thereby preventing malicious code from being executed.

[0010] The present invention thus provides a method of authenticating software in a data processing device comprising a data processor comprising at least one internal memory, the internal memory being immutable once programmed, and at least one external memory containing program software, comprising the steps of: a. issuing a reset signal to the processor; b. reading authentication code from the internal memory; c. executing the authentication code to authenticate at least a portion of the software in the external memory using a public key stored in the internal memory; and d. (i) if the software is authenticated successfully, reading and executing code stored in external memory; or (ii) if the software is not authenticated successfully, sending a reset signal to the processor.

[0011] The present invention further provides data processing device, comprising at least one external memory containing program software, and a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code and a public key for authenticating the program software in the at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

[0012] The present invention further provides a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code and a public key for authenticating program software in at least one external memory, whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] In drawings which illustrate by way of example only a preferred embodiment of the invention,

[0014] **FIG. 1** is a block diagram of a system overview of a conventional hand-held data processing device.

[0015] **FIG. 2** is a block diagram of a processor chip in the data processing device of **FIG. 1**.

[0016] **FIG. 3** is a flow chart showing the boot procedure in the data processing device of **FIG. 1**.

DETAILED DESCRIPTION OF THE INVENTION

[0017] The invention will be described in detail below, by way of example only, in the context of a hand-held data processing device having wireless communications capabilities and a battery, as illustrated in **FIG. 1**, in which a memory controller interface caches sectors out of non-volatile memory into volatile memory for processing, and writes modified data from volatile memory into non-volatile memory for more permanent storage. However, although the invention is particularly advantageous in the hand-held data processing device **10** of **FIG. 1**, it will be appreciated that the principles of the system apply to other data processing devices and the system is not intended to be limited thereby.

[0018] The hand-held data processing devices **10** include a housing, a keyboard **14** and an output device **16**. The output device shown is a display **16**, which is preferably a full graphic LCD. Other types of output devices may alternatively be utilized. A processor **18**, which is shown schematically in **FIG. 1**, is contained within the housing and is coupled between the keyboard **14** and the display **16**. The processor **18** controls the operation of the display **16**, as well as the overall operation of the data processing device **10**, in response to actuation of keys on the keyboard **14** by the user.

[0019] The housing may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keyboard may include a mode selection key, or other hardware or software for switching between text entry and telephony entry. The housing contains the primary power supply, in the embodiment shown a battery **170**, a secondary power supply **180** (illustrated in **FIG. 2**), which may be a small rechargeable battery or capacitor capable of sustaining power to the processor **18**, NAND flash **116** and SDRAM **118** for the duration of an AutoSave interval and a Power Manager **190**.

[0020] In addition to the processor **18**, other parts of the data processing device **10** are shown schematically in **FIG. 1**. These include a communications subsystem **100**; a short-range communications subsystem **102**; the keyboard **14** and the display **16**, along with other input/output devices **106**, **108**, **110** and **112**; as well as memory devices **116**, **118** and various other device subsystems **120**. The data processing device **10** is preferably a two-way RF communication device having voice and data communication capabilities. In addition, the data processing device **10** preferably has the capability to communicate with other computer systems via the Internet.

[0021] Operating system software executed by the processor **18** is preferably stored in a persistent store, such as a flash memory **116**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as a random access memory (RAM including also DRAM and SDRAM) **118**. Communication signals received by the data processing device **10** may also be stored to the RAM **118**.

[0022] The processor **18**, in addition to its operating system functions, enables execution of software applications **130**A-**130**N on the device **10**. A predetermined set of applications that control basic device operations, such as data and voice communications **130**A and **130**B, may be installed on the device **10** during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM is preferably capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also preferably capable of sending and receiving data items via a wireless network **140**. Preferably, the PIM data items are seamlessly integrated, synchronized and updated via the wireless network **140** with the device user's corresponding data items stored or associated with a host computer system.

[0023] Communication functions, including data and voice communications, are performed through the communication subsystem **100**, and possibly through the short-range communications subsystem. The communication subsystem **100** includes a receiver **150**, a transmitter **152**, and one or more antennas **154** and **156**. In addition, the communication subsystem **100** also includes a processing module, such as a digital signal processor (DSP) **158**, and local oscillators (LOs) **160**. The specific design and implementation of the communication subsystem **100** is dependent upon the communication network in which the data processing device **10** is intended to operate. For example, a data processing device **10** may include a communication subsystem **100** designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, GSM, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the data processing device **10**.

[0024] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore requires a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0025] When required network registration or activation procedures have been completed, the data processing device **10** may send and receive communication signals over the communication network **140**. Signals received from the communication network **140** by the antenna **154** are routed to the receiver **150**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows

the DSP **158** to perform more complex communication functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network **140** are processed (e.g. modulated and encoded) by the DSP **158** and are then provided to the transmitter **152** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **140** (or networks) via the antenna **156**.

[**0026**] In addition to processing communication signals, the DSP **158** provides for control of the receiver **150** and the transmitter **152**. For example, gains applied to communication signals in the receiver **150** and transmitter **152** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **158**.

[**0027**] In a data communication mode, a received signal, such as a text message or web page download, is processed by the communication subsystem **100** and is input to the processor **18**. The received signal is then further processed by the processor **18** for an output to the display **16**, or alternatively to some other auxiliary I/O device **106**. A device user may also compose data items, such as e-mail messages, using the keyboard **14** and/or some other auxiliary I/O device **106**, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communication network **140** via the communication subsystem **100**.

[**0028**] In a voice communication mode, overall operation of the device is substantially similar to the data communication mode, except that received signals are output to a speaker **110**, and signals for transmission are generated by a microphone **112**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device **10**. In addition, the display **16** may also be utilized in voice communication mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[**0029**] The short-range communications subsystem enables communication between the data processing device **10** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth™ communication module to provide for communication with similarly-enabled systems and devices.

[**0030**] The device **10** embodying the invention, illustrated in **FIG. 2**, authenticates software stored in an external memory such as non-volatile memory **116** (for example a NOR or NAND flash memory chip) using a internal authentication program, before any software from the memory **116** is executed by the processor **18**. The processor comprises an internal immutable memory, preferably a read only memory (ROM) **19**, which is physically integrated into the processor **18** when the processor's silicon die is fabricated.

[**0031**] The internal ROM **19** contains the authentication code, including one or more public keys, required for authenticating the program software residing in external memory **116** in known fashion. The authentication process is initiated when a reset signal is sent to the processor **18** (for example when the device **10** is activated or restarted). This initiates the boot up procedure, illustrated in **FIG. 3**, which in the preferred embodiment of the invention is as follows:

1) After the processor **18** receives the reset signal, rather than fetching instructions from an untrusted source (e.g. off-chip memory such as NOR flash **116**), the processor **18** executes code read directly from its internal ROM **19**.

[**0032**] 2) The code in the processor's internal ROM **19** comprises a conventional software authentication program that authenticates all or a portion of the external memory **116** containing the program software for the device **10**, which is executed by the processor **18** before any code from the external memory **116** is executed. The program software residing in external memory **116** may be authenticated in any conventional fashion, for example using a digital signature verification system such as "RSA," or any other suitable system, and preferably using a public key stored in the internal ROM **19**.

[**0033**] 3) If the processor **18** determines that the program software in the external memory **116** has been authenticated successfully, the processor **18** begins to fetch and execute program code stored in the external memory **116** to initiate the basic functions of the device **10**.

[**0034**] 4) If the processor **18** determines that the program software in the external memory **116** has not been authenticated successfully, the boot program causes another reset signal to be sent the processor **18**. The boot routine thus repeats and again tries to authenticate the program software in the external memory **116**. If the unsuccessful authentication attempt was merely due to an execution error, the program software will likely be authenticated on a subsequent execution of the authentication code. However, if the unsuccessful authentication attempt occurred because the external memory **116** had been tampered with, an endless resetting loop will result, thereby preventing malicious code from being executed by the processor **18**.

[**0035**] The method and device of the invention thus ensures that the boot code performing the authentication process is guaranteed to be authentic. As an alternative, it is possible to stack the non-volatile memory **116** in the same package as the processor **18**, on the assumption that there is no way for an attacker to modify the boot code stored in on-chip flash. However, authenticating the device's code using internal ROM **19** is more secure, since it is impossible to change the code stored in ROM without re-fabricating the silicon die itself. Accordingly, in the method and device of the invention trusted code is always used to authenticate the untrustworthy code in external memory, so the integrity of the system is significantly improved.

[**0036**] When authenticating the code in external memory such as flash memory **116**, it is important to ensure the code is signed correctly. Several algorithms can be used to accomplish this. By way of example only, RSA is a good candidate since it runs quickly and has a small memory footprint. However, other authentication algorithms are available for this and the invention is not intended to be limited to any particular authentication means.

[**0037**] Although internal ROM **19** is preferred, other internal memory technologies that are immutable when in operation (i.e. once programmed), such as one time programmable flash could be used to hold the bootROM and public key(s). However, whatever type of memory is used,

the internal bootROM code and public key(s) should be immutable once the device has been deployed so that they cannot be changed. Regular flash can be used if protected by hardware that secures a regular programmable flash memory to render it immutable once it has been written to, and a programmable flash memory so equipped would be immutable for purposes of the invention and thus suitable for use in the invention.

[0038] Various embodiments of the present invention having been thus described in detail by way of example, it will be apparent to those skilled in the art that variations and modifications may be made without departing from the invention. The invention includes all such variations and modifications as fall within the scope of the appended claims.

We claim:

1. A method of authenticating software in a data processing device comprising a data processor comprising at least one internal memory, the internal memory being immutable once programmed, and at least one external memory containing program software, comprising the steps of:

a. issuing a reset signal to the processor;

b. reading authentication code from the internal memory;

c. executing the authentication code to authenticate at least a portion of the software in the external memory using a public key stored in the internal memory; and

d. (i) if the software is authenticated successfully, reading and executing code stored in external memory; or

(ii) if the software is not authenticated successfully, sending a reset signal to the processor.

2. The method of claim 1 wherein the internal memory comprises a read only memory.

3. A data processing device, comprising

at least one external memory containing program software, and

a data processor comprising at least one internal memory, the internal memory being immutable once programmed and comprising authentication code and a public key for authenticating the program software in the at least one external memory,

whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

4. The device of claim 3 wherein the internal memory comprises a read only memory.

5. A data processor comprising at least one internal read only memory, the internal read only memory being immutable once programmed and comprising authentication code and a public key for authenticating program software in at least one external memory,

whereby when the processor receives a reset signal the processor executes the authentication code to authenticate at least a portion of the software in the external memory, and if the software is authenticated successfully the processor reads and executes code stored in external memory, or if the software is not authenticated successfully a further reset signal is sent to the processor.

6. The data processor of claim 1 wherein the internal memory comprises a read only memory.

* * * * *

US 20050076226A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2005/0076226 A1

Boivie et al. (43) Pub. Date: Apr. 7, 2005

(54) COMPUTING DEVICE THAT SECURELY RUNS AUTHORIZED SOFTWARE

(75) Inventors: **Richard H. Boivie**, Monroe, CT (US); **William Eric Hall**, Clinton, CT (US)

Correspondence Address:
F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797 (US)

(73) Assignee: **International Business Machines Corporation**

(21) Appl. No.: **10/677,933**

(22) Filed: **Oct. 1, 2003**

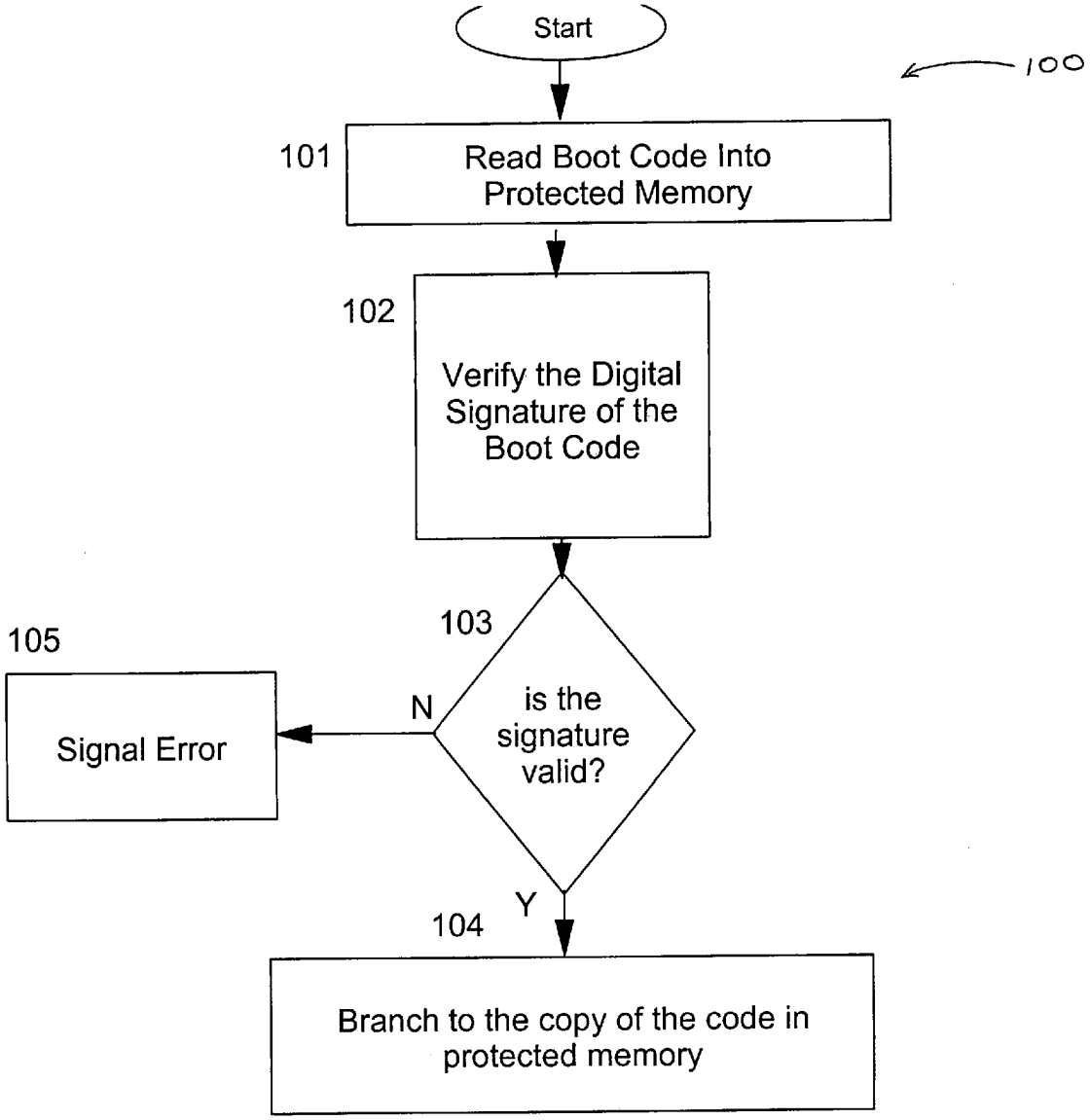
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/32**; G06F 12/14

(52) **U.S. Cl.** **713/187**; 713/190

(57) **ABSTRACT**

A computing device for securely executing authorized code includes a protected memory for storing authorized code, which contains an original digital signature, and a processor in signal communication with the protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in the code is original in accordance with a public key, and if the original digital signature is verified, then branching to a copy of the authorized code in the protected memory to begin execution.



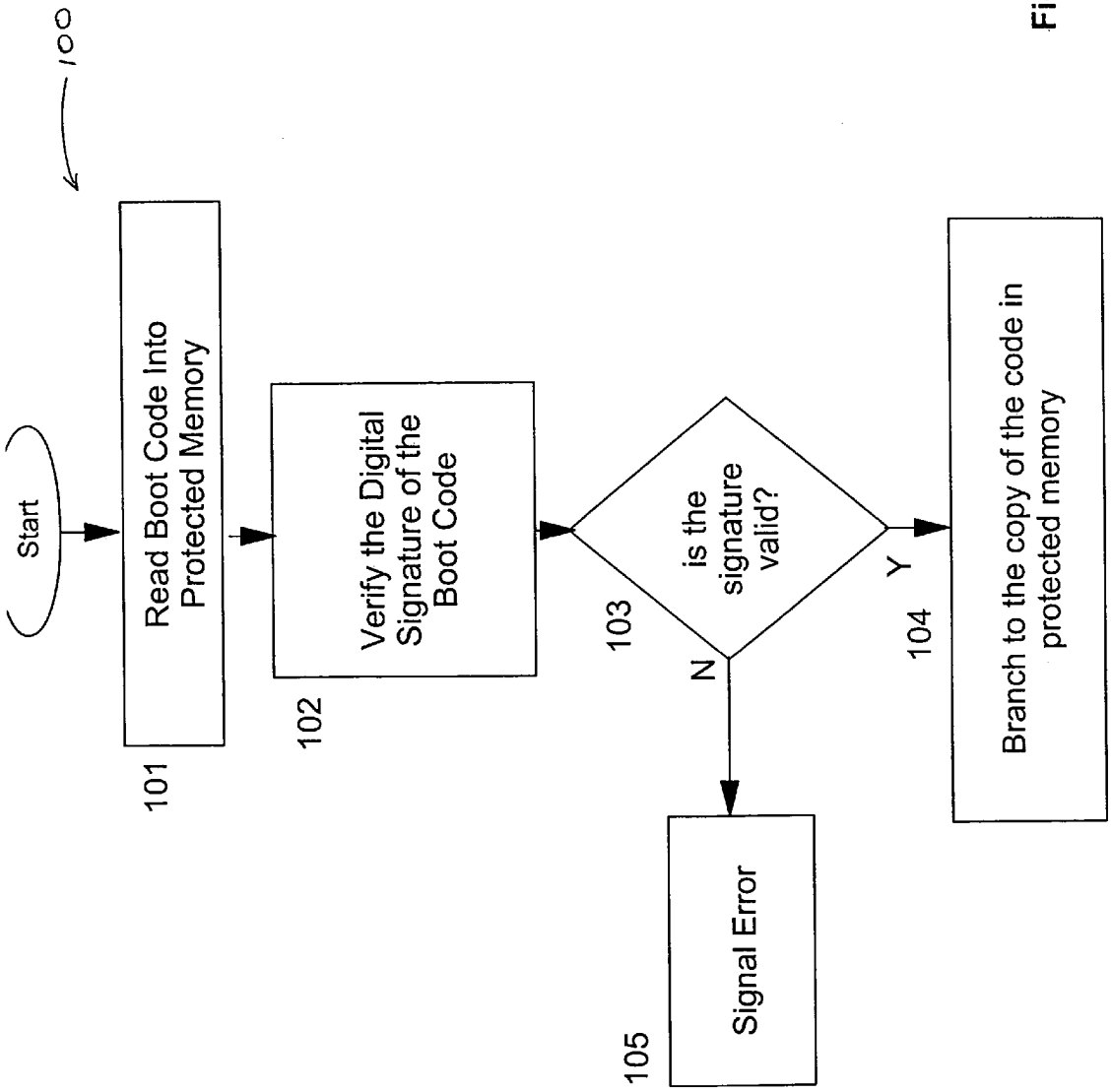

100
Start
Read Boot Code Into Protected Memory
101
Verify the Digital Signature of the Boot Code
102
is the signature valid?
103
N
Y
Signal Error
105
Branch to the copy of the code in protected memory
104

Figure 1

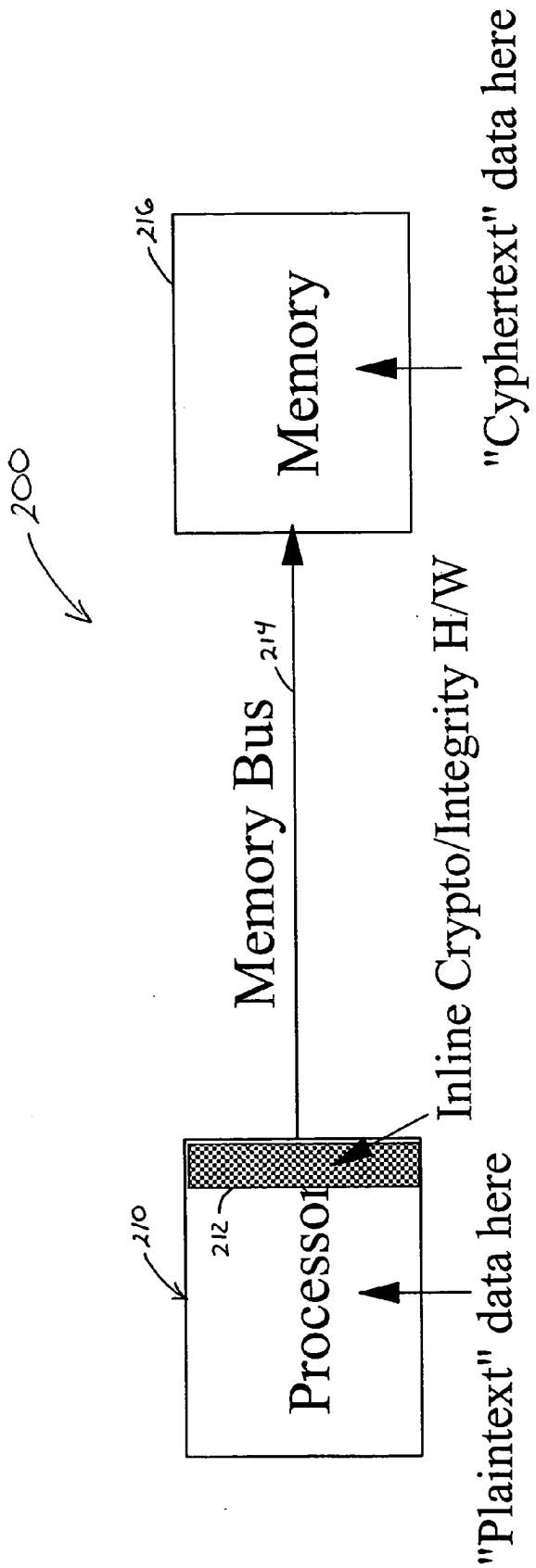

200
216
Memory
"Cyphertext" data here
Memory Bus
214
Inline Crypto/Integrity H/W
210
212
Processor
"Plaintext" data here

Figure 2

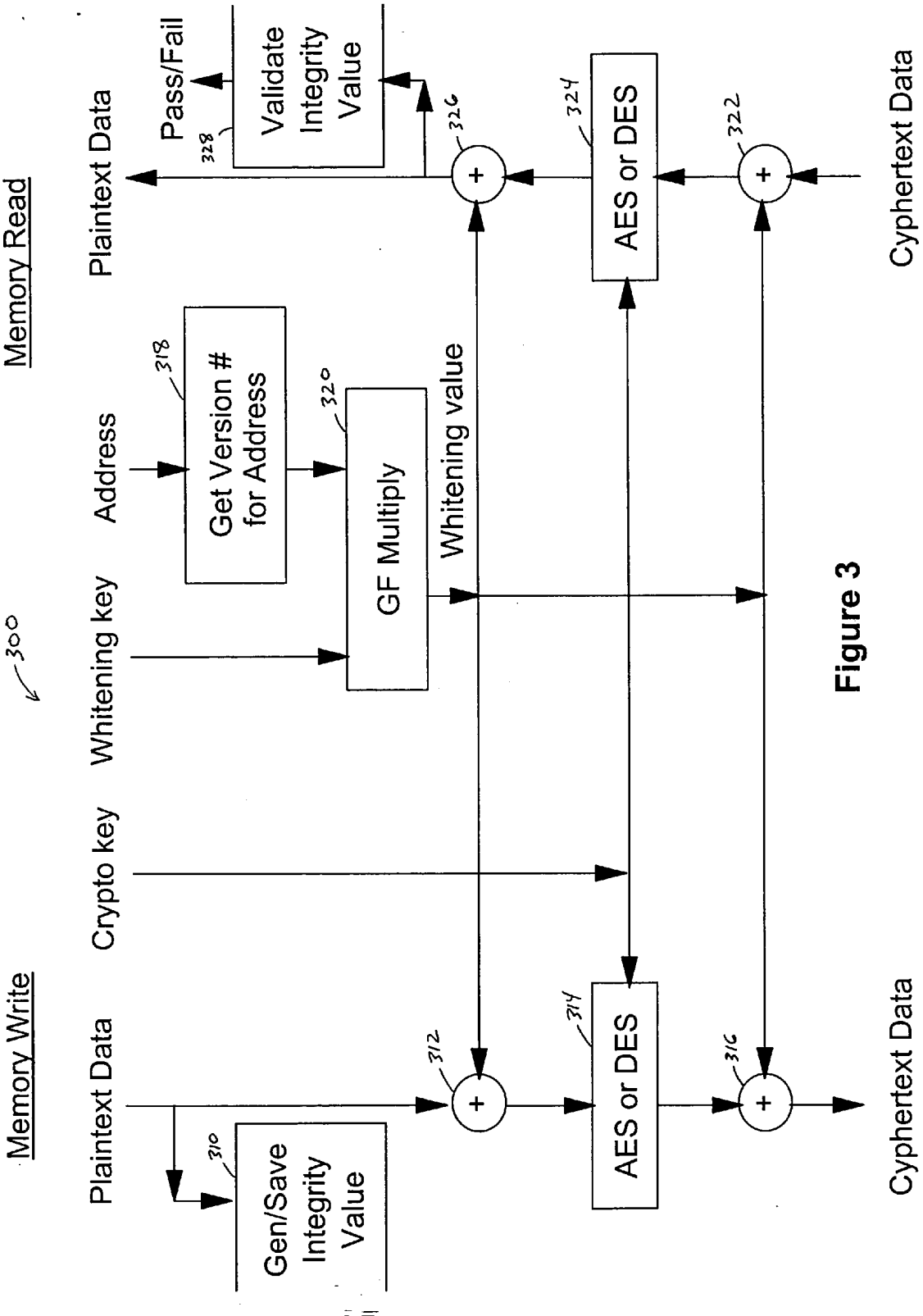

Memory Read
Memory Write
300
Plaintext Data
Crypto key
Whitening key
Address
Plaintext Data
Pass/Fail
Get Version # for Address
GF Multiply
Whitening value
Gen/Save Integrity Value
Validate Integrity Value
AES or DES
AES or DES
Cyphertext Data
Cyphertext Data
310
312
314
316
318
320
322
324
326
328

Figure 3

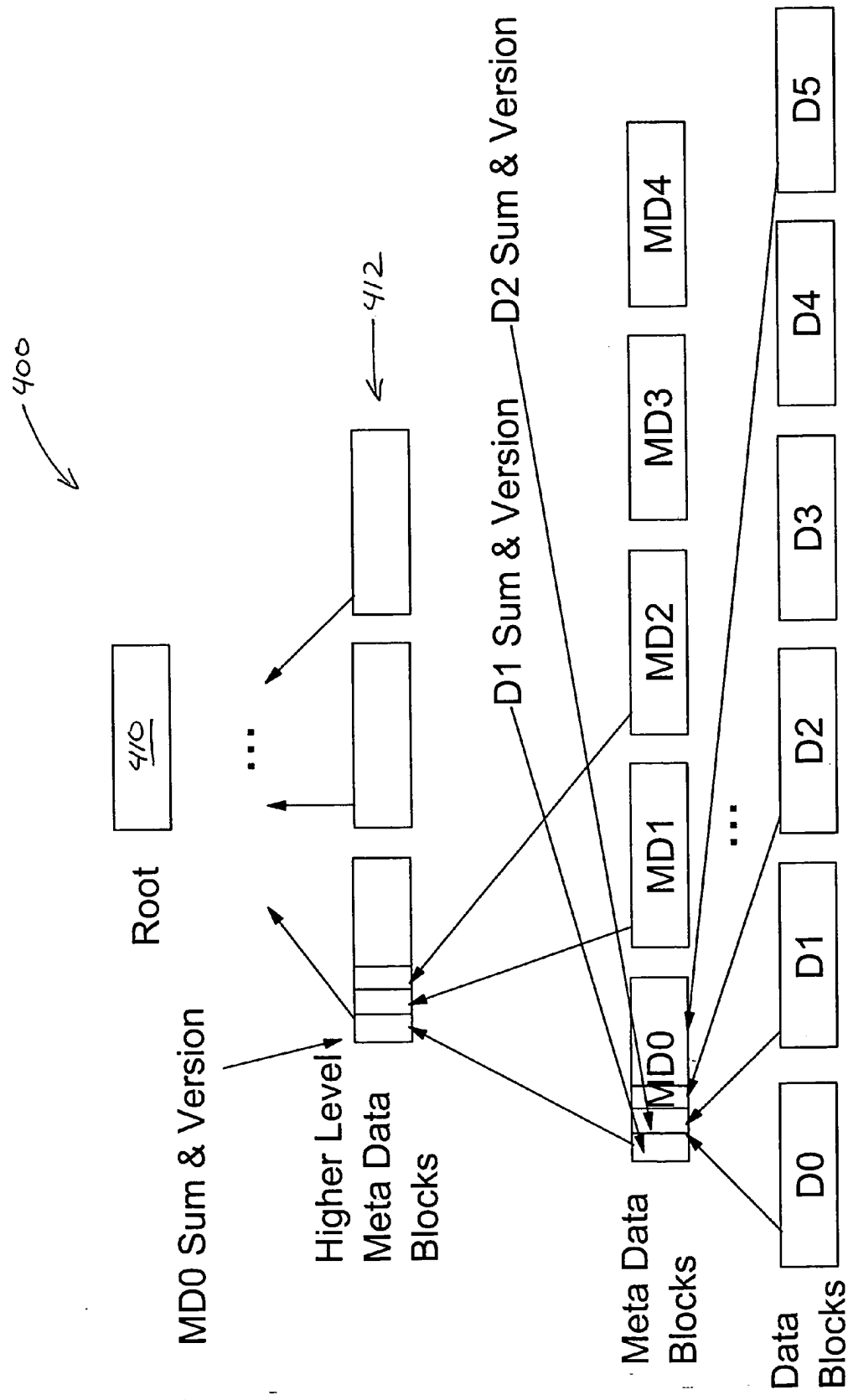

400
410
Root
412
MD0 Sum & Version
Higher Level Meta Data Blocks
D1 Sum & Version
D2 Sum & Version
MD0
MD1
MD2
MD3
MD4
Meta Data Blocks
D0
D1
D2
D3
D4
D5
Data Blocks

Figure 4

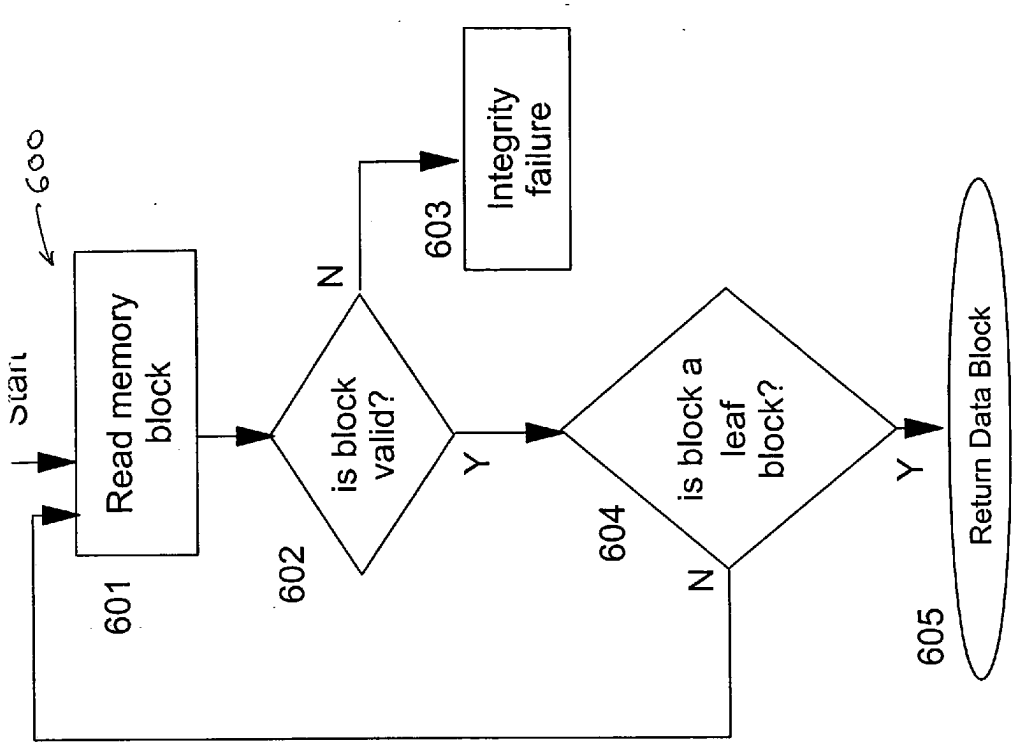


Figure 6

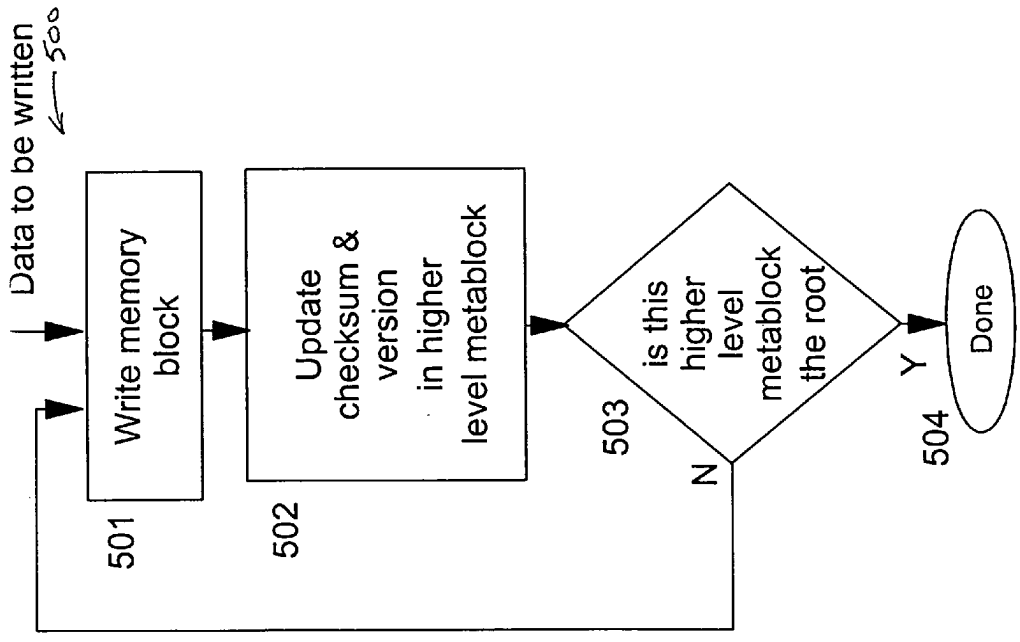


Figure 5

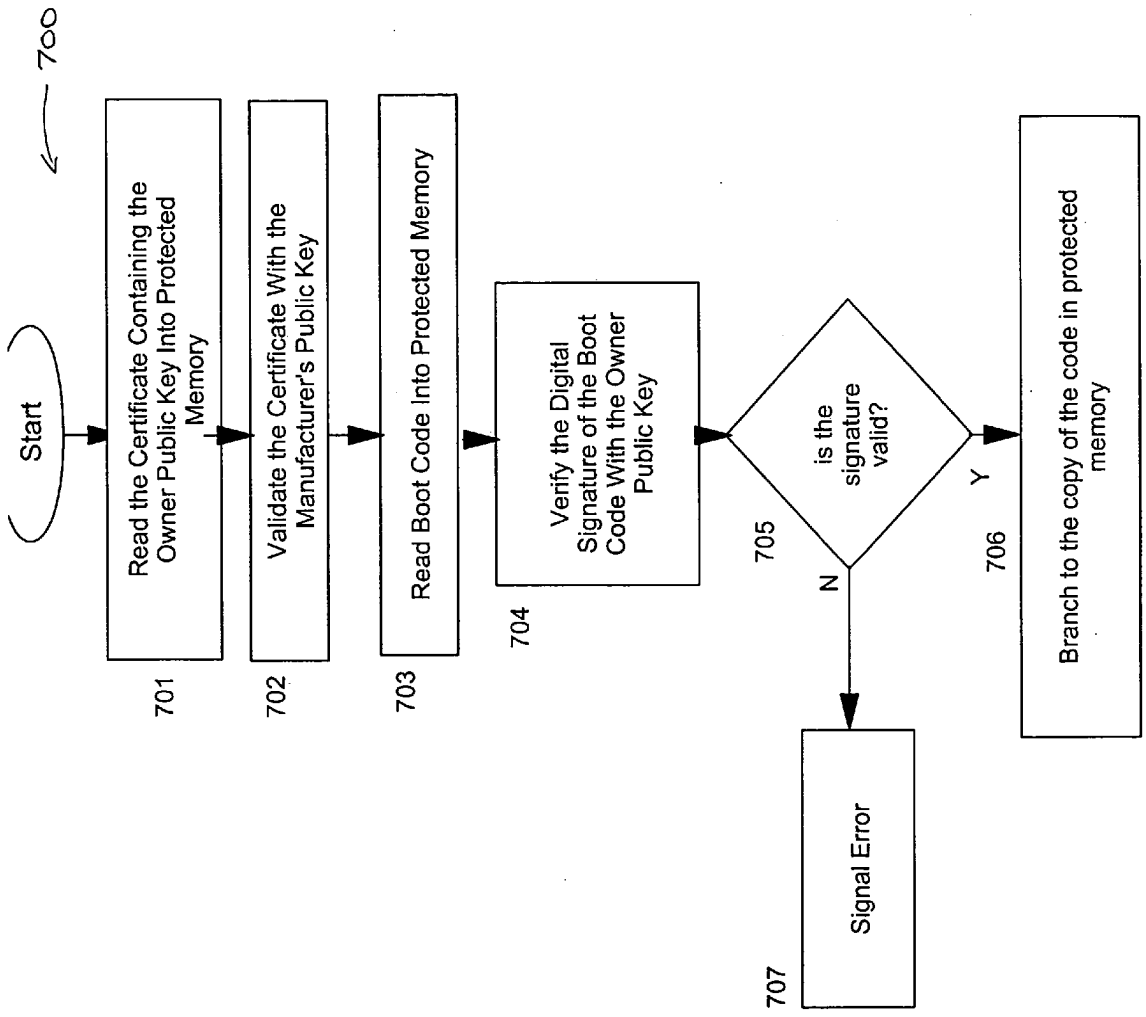

700
Start
Read the Certificate Containing the Owner Public Key Into Protected Memory
701
Validate the Certificate With the Manufacturer's Public Key
702
Read Boot Code Into Protected Memory
703
Verify the Digital Signature of the Boot Code With the Owner Public Key
704
is the signature valid?
705
N
Signal Error
707
Y
706
Branch to the copy of the code in protected memory

Figure 7

COMPUTING DEVICE THAT SECURELY RUNS AUTHORIZED SOFTWARE

BACKGROUND OF THE INVENTION

[0001] The present invention relates generally to a secure computing device that protects its secrets and its integrity using hardware mechanisms and advanced cryptographic techniques.

[0002] There are a number of situations in which it is important to protect the integrity of a computing device from physical tampering. For example, a biometric security device would not provide much security if an attacker could tamper with the device and compromise its function. Similarly, a cable TV company's set-top boxes would not provide much security and might allow an attacker to watch the pay-per-view movies for free, for example, if the attacker could compromise the function of the set-top box.

[0003] The federal government has issued standards relating to "secure computing". The National Institute of Standards and Technology has issued Federal Information Processing Standards Publication, FIPS PUB 140-1, defining "Security Requirements for Cryptographic Modules". Security level 4 provides the highest level of security and includes an "envelope" of protection around the cryptographic module that provides protection against attempts to penetrate the envelope. If an attacker attempts to penetrate the security envelope, the attempt should be detected and all critical security parameters zero-ized. As FIPS PUB 140-1 states: "Level 4 devices are particularly useful for operation in a physically unprotected environment when an intruder could possibly tamper with the device".

[0004] Accordingly, what is needed is a secure computing device capable of protecting its secrets and its integrity using hardware mechanisms and advanced cryptographic techniques.

SUMMARY OF THE INVENTION

[0005] The above and other drawbacks and deficiencies of the prior art are overcome or alleviated by a secure computing device that protects secrets, protects its own integrity, and that can run any software that is digitally signed by the owner of the device.

[0006] A computing device for securely executing authorized code includes a protected memory for storing authorized code, which contains an original digital signature, and a processor in signal communication with the protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in the code is original in accordance with a public key, and if the original digital signature is verified, then branching to a copy of the authorized code in the protected memory to begin execution.

[0007] These and other aspects, features and advantages of the present disclosure will become apparent from the following description of exemplary embodiments, which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention may be better understood with reference to the following exemplary figures, in which:

[0009] **FIG. 1** shows a flow diagram of a boot process for a secure computing device in accordance with the principles of the present disclosure;

[0010] **FIG. 2** shows a schematic diagram of a secure computing device in accordance with the principles of the present disclosure;

[0011] **FIG. 3** shows a process diagram for encryption, decryption and maintaining integrity of data for a secure computing device in accordance with the principles of the present disclosure;

[0012] **FIG. 4** shows a data diagram of an integrity tree for a secure computing device in accordance with the principles of the present disclosure;

[0013] **FIG. 5** shows a flow diagram of a memory write process for a secure computing device in accordance with the principles of the present disclosure;

[0014] **FIG. 6** shows a flow diagram of a memory read process for a secure computing device in accordance with the principles of the present disclosure; and

[0015] **FIG. 7**. shows a flow diagram of an alternate embodiment modified boot process for a secure computing device in accordance with the principles of the present disclosure.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0016] A secure computing device is provided that protects secrets and its own integrity. The secure computing device is further capable of running any compatible software that is digitally signed by the owner of the device. Digitally signed code, as defined herein, comprises code having a hash (e.g., a secure hash algorithm or "SHA-1", as known in the art) with a digital signature. The secure computing device, which can run software that is digitally signed by an authorized party and protect the integrity of that software during execution, will not run any software that is not signed by an authorized party.

[0017] The secure computing device described herein protects its secrets and its integrity using hardware mechanisms and advanced cryptographic techniques. This secure computing device can run any software that the owner of the device chooses, and the owner can update the software on the device at any time. The secure computing device protects the integrity of this software over the "lifetime" of the software. The software is protected from the time it "ships", throughout its execution until the software is no longer needed. Thus an attacker cannot compromise the function of the device.

[0018] The "owner" of a device is not necessarily the "user" of the device. For example, the owner of a set-top box might be a cable television ("TV") company, while the user of the set-top box might be a potential attacker. In this case, the secure computing device could prevent an attacker from modifying the function of the set-top box in a way that would allow the attacker to watch all the pay-per-view movies for free, for example.

[0019] In the case of a personal data assistant ("PDA"), the secure computing device could prevent an attacker that gains physical control of the PDA from accessing confidential information stored on the PDA. The secure computing device could also prevent the attacker from modifying the function of the device to include a "Trojan horse" that would record and mail passwords or other confidential information to the attacker.

[0020] The secure computing device described here protects secrets and its own integrity using hardware mechanisms and advanced cryptographic techniques. Implementation of the device includes a public key that is inside the device that is used to check the signature of digitally signed code.

[0021] As shown in **FIG. 1**, a flow diagram of a boot process for a secure computing device in accordance with the principles of the present disclosure is indicated generally by the reference numeral **100**. At boot time, a read-only memory ("ROM") inside the device reads the boot code from a standard boot address and copies the boot code into "protected memory" at step **101**, verifies the digital signature on the boot code at step **102**, checks whether the digital signature is valid at step **103**, and, if valid, branches to the copy of the code in protected memory at step **104**. If, on the other hand, the digital signature is found to be invalid at step **103**, an error is signaled at step **105**.

[0022] Here, the protected memory can be a memory that is inside the computing device and inaccessible to an attacker that might want to compromise the integrity of the device. Alternatively, the protected memory can be a memory that is outside of the device and protected by an inline encryption scheme as illustrated in **FIG. 2**.

[0023] Turning to **FIG. 2**, a secure computing device in accordance with the principles of the present disclosure is indicated generally by the reference numeral **200**. The secure computing device **200** includes a processor **210** in signal communication with a memory bus **214**, which is in signal communication with a memory **216**. The processor **210** includes inline cryptography and integrity hardware **212**. The processor **210** uses "plain text" data, while the memory **216** uses "ciphertext" data. In this exemplary embodiment, the memory **216** is a protected memory that is outside of the device, and protected by the hardware **212** using inline encryption.

[0024] In one embodiment of this invention, a symmetric key inside the device is used to encrypt information that is written outside the chip and decrypt information as it is read back in. This inline encryption process protects both the confidentiality of information stored outside of the chip as well as the integrity of that information.

[0025] The public key can be in an on-chip ROM and thus fixed for all copies of a design, or in fuses that are programmed at the wafer stage (e.g., laser trimmed) or at system assembly time (e.g., in-system programmable). The last option allows the chip manufacturer to make and package parts without a customer-specific public key but this option is not available in certain chip technologies.

[0026] One solution to this problem is to include a small number of on-chip laser trimmed fuses to identify the "owner number" for a particular chip. If the chip also includes the public key of the chip manufacturer, the chip manufacturer's public key can be used to validate a certificate that provides the public key for a given owner number. **FIG. 7**, discussed later, illustrates how the boot process might work in this case.

[0027] The integrity protection scheme defends against modification of data as well as replay and relocation of data. A "replay" of a data block is the replacement of that data block with a value that was valid at that data block's address at some earlier point in time. A "relocation" of a data block is the replacement of the data block with a block that is valid at a different address. The encryption/integrity scheme may use an encryption algorithm, such as the data encryption standard ("DES") or advanced encryption standard ("AES") with time and location sensitivity, to defend against replay and relocation of data.

[0028] The encryption of a plaintext block is a function of the plaintext data, an encryption key and a "whitening" value. The whitening value is a function of a whitening key, the block's "address" and a counter or "version number" that is incremented each time a block is written. The use of the block's address in the whitening value defends against relocation and the use of the version number defends against replay.

[0029] Turning now to **FIG. 3**, data flow for encryption, decryption and integrity of data for a secure computing device is indicated generally by the reference numeral **300**. In a Memory Write portion of the data flow **300**, Plaintext data is received, for which an integrity value is generated and saved at a function block **310**. The received Plaintext data is also received at a first summing block **312**, which also receives a Whitening Value to sum with the Plaintext data. The output of the summing block **312** is received and encrypted by a function block **314**, which also receives a Cryptographic Key and encrypts the data using AES or DES, for example. The output of the encryption block **314** is received by a second summing block **316**, which also receives a Whitening Value to sum with the encrypted data. The output of the summing block **316** comprises Ciphertext data to be stored in protected memory.

[0030] The address of the data is received by a function block **318**, which gets a version number for the received address. The output of the block **318** is received by a Galois Field ("GF") multiply block **320**. The GF multiply block **320** also receives a Whitening Key, and thereby produces the Whitening Value.

[0031] In a Memory Read portion of the data flow **300**, Ciphertext data is retrieved from protected memory to a third summing block **322**. The summing block **322** sums the retrieved Ciphertext data with the Whitening Value. A decryption block **324** receives the output of the summing block **322**, receives the Cryptographic Key, and produces a decrypted output using AES or DES, for example. The output of the decryption block **324** is received by a fourth summing block **326**, which sums it with the Whitening Value to produce Plaintext data. The Plaintext data output from the fourth summing block **326** is received at a function block **328**, which validates the Integrity Value of the Plaintext data, and produces a Pass/Fail flag.

[0032] In this variant of the scheme, as shown in **FIG. 3**, the whitening value is a multiplication in a Galois field of the version number and the whitening key. In the variant of the scheme shown in **FIG. 3**, whitening includes an exclusive-or of the data with the whitening value, and whitening is applied to the data both before and after the DES or AES encryption on memory writes, as well as before and after the DES or AES decryption on memory reads.

[0033] An integrity value is also computed whenever a block is written out to memory. The integrity value can be a sum (e.g., "exclusive or") of all of the plaintext in the data

block. Since the integrity value for a data block also needs to be protected if the data block is to be protected, and since the version number needs to be maintained and protected, the <integrity value, version number> pair for a given block is combined with similar pairs of other data blocks (e.g., nearby), and the group of pairs is written to another data block, a "meta-data" block that in turn must be protected.

[0034] As shown in **FIG. 4**, an integrity tree for a secure computing device is indicated generally by the reference numeral **400**. The exemplary integrity tree **400** includes data blocks D**0**, D**1**, D**2**, D**3**, D**4** and D**5**. The tree further includes meta-data blocks MD**0**, MD**1**, MD**2**, MD**3** and MD**4**. The meta-data block MD**0**, for example, comprises the sum and version for all of the data blocks D**0**, D**1**, D**2**, D**3**, D**4** and D**5**. In addition, this exemplary integrity tree includes higher-level meta-data blocks **412**, one of which comprises the sum and version for all of the meta-data blocks MD**0**, MD**1** and MD**2**, for example. The has a root **410**, which might directly comprise the sum and version for all of the higher-level meta-data blocks **412**, or might comprise meta-data blocks of even higher level in alternate embodiments.

[0035] Thus, in this variation of the scheme, the <integrity value, version number> pair for the meta-data block is combined with those of other nearby meta-data blocks and written to a higher-level meta-data block, which is, in turn, protected. The meta-data blocks including the higher-level meta-data blocks form a tree and the root of the tree protects the integrity of the entire protected memory. Although one exemplary design embodiment for an integrity tree has been described, alternative designs are also possible. For example, an integrity tree such as that described in the co-pending patent application entitled "Parallelizable Authentication Tree for Random Access Storage" (Attorney Disclosure No. YOR820020483) might be employed in place of the exemplary integrity tree described here. Of course, other integrity tree designs are also possible as will be recognized by those skilled in the pertinent art.

[0036] The root of the integrity tree, as well as the encryption and whitening keys, are stored inside the secure computing device. In addition, the contents of the meta-data integrity tree are updated and verified inside the secure computing device. This means that an attacker has no visibility into the contents of the protected memory. This also means that the secure computing device can detect any modifications that an attacker may make to the contents of protected memory including any "replay" or "relocation" attacks.

[0037] The integrity tree embodiment **400** allows for off-chip storage of data. The integrity values and version numbers form a tree and only the highest-level root of the tree is stored and physically protected inside of the chip. However, alternate embodiments may be applied where there is enough on-chip storage available to store a lower level of the integrity tree below the root. If all of the integrity and version information does not fit inside the chip, but if there is sufficient on-chip memory to completely store such a lower level of the integrity tree, then it is not necessary to build an entire integrity tree up to a single highest root. For example, if the lowest level of the integrity tree fits on-chip, then it would not be necessary to maintain any higher-level integrity values. Alternatively, if the lowest level did not fit on the chip, but the next higher second level did fit on the chip, then it would not be necessary to maintain any higher levels above that second integrity level since the second integrity level would be physically protected inside of the chip.

[0038] Turning to **FIG. 5**, a Memory Write process for a secure computing device is indicated generally by the reference numeral **500**. The process **500** receives data to be written at a function block **501**, which writes the memory block and passes control to a function block **502**. The function block **502** updates the checksum and version in a higher-level metablock, and passes control to a decision block **503**. The decision block **503**, in turn, determines whether this higher-level metablock is the root of the integrity tree. If the root is not detected, control is passed back to the function block **501**. If, on the other hand, the root is detected, control is passed to a return block **504**.

[0039] Thus, **FIG. 5** illustrates the steps involved in writing a data block to the protected memory. The block is written out to the protected memory in step **501**. In step **502**, updated versions of the data block's checksum and version number are saved in the data block's "meta-data" block. If this meta-data block corresponds to the root of the integrity tree, as determined in step **503**, then the process completes at step **504**. If, on the other hand, the meta-data block is not the root of the integrity tree, then the meta-data block needs to be written out to the protected memory in step **501** and the checksum and version number for the meta-data block needs to be saved in a higher-level meta-data block in step **502**. As before, if this higher-level meta-data block corresponds to the root, as determined in step **503**, the process completes at step **504**. Otherwise, the meta-data block needs to be written out to the protected memory and the process continues until a higher-level meta-data block corresponds to the root, at which point the process terminates at step **504**. In this case, all of the blocks that are written out to the protected memory are protected using the encryption and integrity scheme shown in **FIG. 3**.

[0040] Turning now to **FIG. 6**, a Memory Read process for a secure computing device is indicated generally by the reference numeral **600**. The process **600** includes a function block **601**, which reads a memory block and passes control to a decision block **602**. The decision block **602** determines whether the block is valid, and, if not, passes control to a function block **603** to recognize an integrity failure. If, on the other hand, the block is valid, then the block **602** passes control to a second decision block **604**. The second decision block **604** determines whether the block is a leaf block, and, if not, passes control back to the function block **601**. If, on the other hand, the block is a leaf block, then the decision block **604** passes control to a return block **605**, which returns the data block.

[0041] Thus, **FIG. 6** illustrates the steps involved in reading a data block from the protected memory. In step **601**, the first data block on the path from the root of the integrity tree to the desired data block is read from the protected memory. In step **602**, the block's validity is checked with checksum and version information from the root of the integrity tree. If the integrity check fails, an integrity failure condition is signaled in step **603**. On the other hand, if the block is determined to be valid, then a check is performed in step **604** to determine whether the block is the desired data block. If it is, the data is returned to the user in step **605**. If

it is not, the next data block on the path from the root to the desired data block is read in step **601**. As before, the integrity of this block is checked in step **602**. In addition, as before, an integrity failure condition is signaled in step **603** if the integrity check fails. As before, if the block is determined to be valid, a check is performed, in step **604**, to determine whether the block is the desired data block. If it is, the data is returned to the user in step **605**. If not, the next data block on the path is read and so on until either an integrity check fails in which case an integrity failure condition is signaled in step **603**, or the desired data block is reached and the data is returned to the user in step **605**. In this case, all of the blocks that are read from the protected memory are decrypted and have their integrity checked as shown in **FIG. 3**.

[**0042**] In addition, the blocks on the path from the root to the desired data blocks can be cached to improve performance. Using an alternate embodiment modified integrity tree, such as the one described in the co-pending patent application entitled "Parallelizable Authentication Tree for Random Access Storage" (Atty. Discl. No. YOR820020483), the integrity of data blocks on the path from the root to the desired data can be checked in parallel, further improving performance.

[**0043**] As shown in **FIG. 7**, an alternate embodiment modified boot process is indicated generally by the reference numeral **700**. The process **700** includes a function block **701**, which reads a Certificate containing an Owner Public Key into protected memory, and passes control to a function block **702**. The block **702** validates the Certificate with the Manufacturer's Public Key, which is present on the processor, and passes control to a function block **703**. The block **703**, in turn, reads the Boot Code into protected memory, and passes control to a function block **704**. The block **704** verifies the Digital Signature of the Boot Code with the Owner Public Key, and passes control to a decision block **705**. The decision block **705** determines whether the Digital Signature is valid, and, if so, passes control to a branch block **706**. The branch block **706** branches to the copy of the code in protected memory. If, on the other hand, the decision block **705** determines that the Digital Signature is not valid, it passes control to a function block **707** to signal an error.

[**0044**] Thus, as mentioned following the description of **FIG. 3**, the alternate embodiment boot process **700** of **FIG. 7** may use, for example, a small number of on-chip laser trimmed fuses to identify the "owner number" for a particular chip. If the chip also includes the public key of the chip manufacturer, the chip manufacturer's public key can be used to validate a certificate that provides the public key for a given owner number.

[**0045**] Although illustrative embodiments have been described herein with reference to the accompanying drawings, it is to be understood that the present invention is not limited to those precise embodiments, and that various changes and modifications may be effected therein by one of ordinary skill in the pertinent art without departing from the scope or spirit of the present invention. All such changes and modifications are intended to be included within the scope of the present invention as set forth in the appended claims.

What is claimed is:

1. A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing authorized code, which contains an original digital signature; and

a processor in signal communication with said protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in said code is original in accordance with a public key, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

2. A computing device as recited in claim 1 wherein said protected memory is cryptographically protected.

3. A computing device as recited in claim 1 wherein the integrity of the contents of said protected memory is protected by encryption.

4. A computing device as recited in claim 1 wherein said protected memory is physically protected.

5. A computing device as recited in claim 1 wherein said public key is stored in said protected memory.

6. A computing device as recited in claim 1 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

7. A computing device as recited in claim 6 wherein the integrity of said authorized code is protected at run time with symmetric key encryption.

8. A computing device as recited in claim 6, wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

9. A computing device as defined in claim 1 wherein:

the protected memory stores code with an original digital signature corresponding to an Owner Public Key; and

the processor verifies the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifies the original digital signature in accordance with the Owner Public Key.

10. A computing device as defined in claim 9, further comprising:

reading means for reading a Certificate containing an Owner Public Key;

validation means for validating the Certificate with the Manufacturer Public Key;

matching means for finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

verification means for using the matched Owner Public Key to verify the authorized code.

11. A method for ensuring that a processor will execute only authorized code, said method comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory; preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

12. A method as recited in claim 11 wherein said protected memory is cryptographically protected.

13. A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption.

14. A method as recited in claim 11 wherein said protected memory is physically protected.

15. A method as recited in claim 11 wherein said public key is stored in said protected memory.

16. A method as recited in claim 11 wherein the integrity of said authorized code is protected at run time.

17. A method as recited in claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. A method as recited in claim 11 wherein the privacy of said authorized code is protected at run time.

19. A method as recited in claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20. A method as defined in claim 11, further comprising:

storing code in the protected memory with an original digital signature corresponding to an Owner Public Key; and

verifying the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifying the original digital signature in accordance with the Owner Public Key.

21. A method as defined in claim 20, further comprising:

reading a Certificate containing an Owner Public Key;

validating the Certificate with the Manufacturer Public Key;

finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

using the matched Owner Public Key to verify the authorized code.

22. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

branching to a copy of said authorized code in said protected memory to begin execution if said original digital signature is verified.

* * * * *

US 20010007131A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2001/0007131 A1**

GALASSO et al. (43) **Pub. Date: Jul. 5, 2001**

(54) **METHOD FOR VALIDATING EXPANSION ROMS USING CRYPTOGRAPHY**

(76) Inventors: **LEONARD J. GALASSO**, RANCHO SANTA MARGARITA, CA (US); **SON VU**, HUNTINGTON BEACH, CA (US); **QUANG PHAN**, TUSTIN, CA (US)

Correspondence Address:
KIMBERLEY G. NOBELS
IRELL & MANELLA, LLP
840 NEWPORT CENTER DRIVE
SUITE 400
NEWPORT BEACH, CA 92660 (US)

(*) Notice: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

(21) Appl. No.: **08/927,934**

(22) Filed: **Sep. 11, 1997**

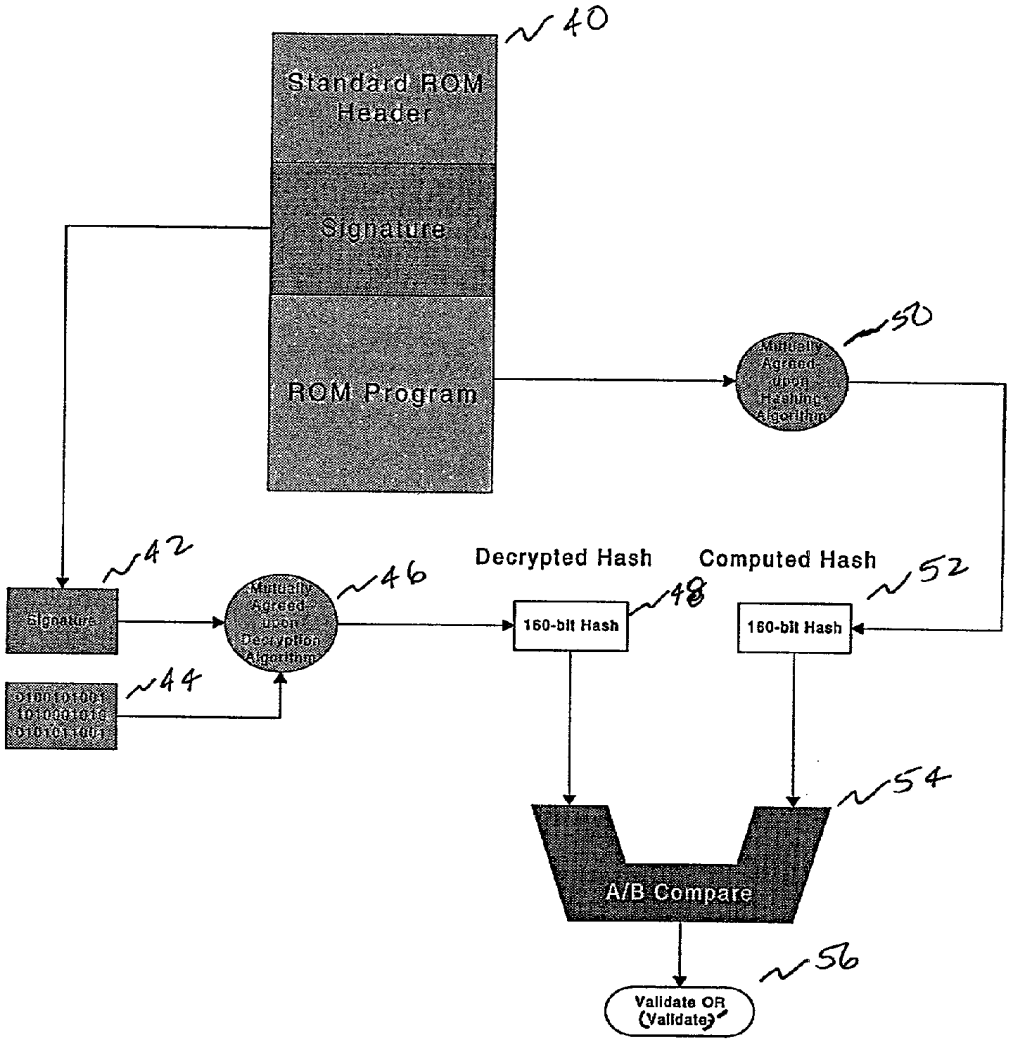
Publication Classification

(51) **Int. Cl.**[7] **G06F 12/14**

(52) **U.S. Cl.** **713/187**; 713/189

(57) **ABSTRACT**

A method for validating expansion ROM cards which are loaded into a Personal Computer. A ROM image is signed (encrypted) using a private key and an encryption algorithm to create a digital signature. The digital signature is stored along with the ROM image on an expansion ROM. The system BIOS scans the system for the presence of an expansion ROM and when one is detected, the digital signature is verified (decrypted) using a public key corresponding to the private key. If the decrypted digital signature matches the ROM image (or a hash digest thereof), then the BIOS loads the ROM image.



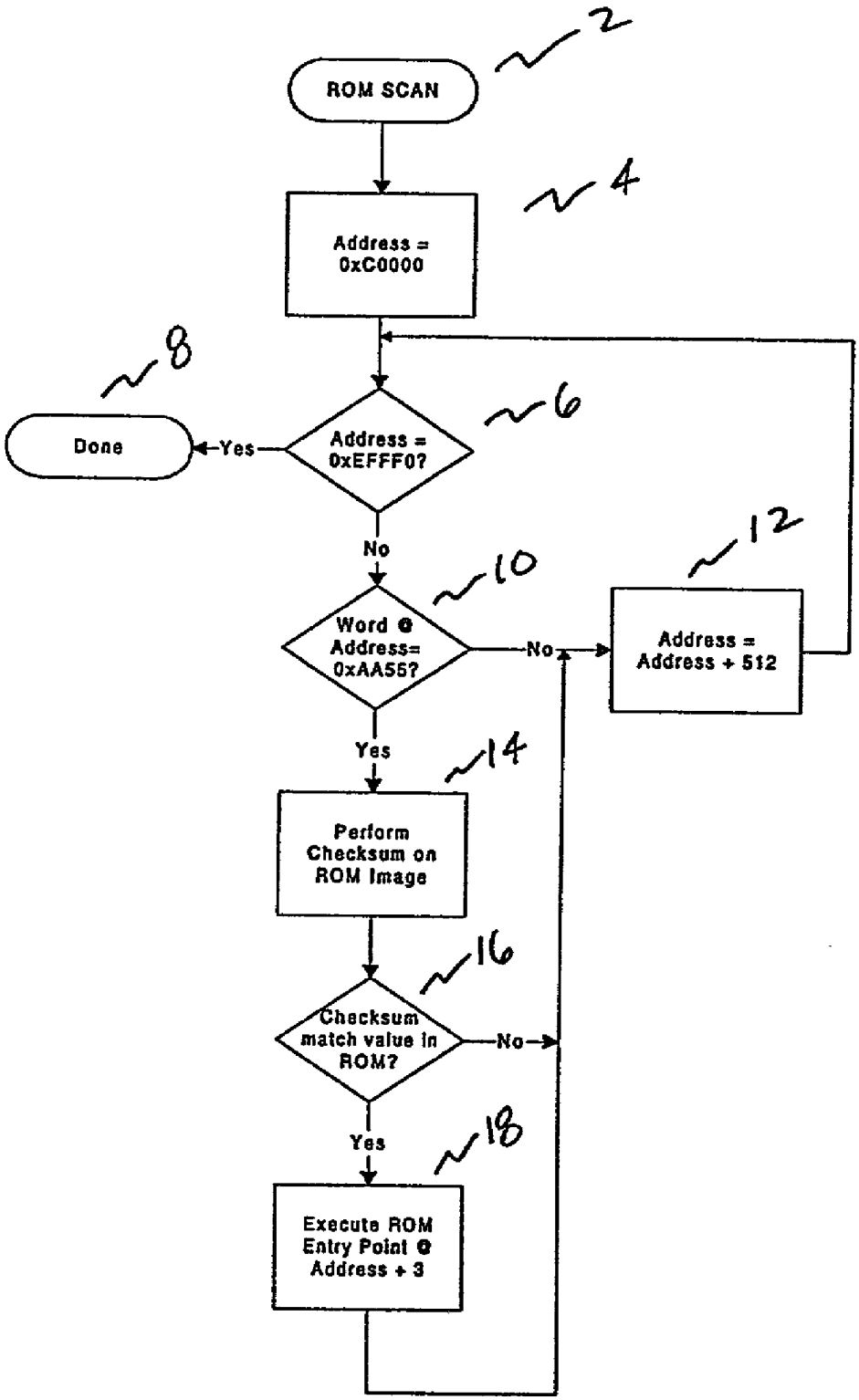

ROM SCAN
2
Address = 0xC0000
4
Address = 0xEFFF0?
6
Done
8
Yes
No
Word @ Address= 0xAA55?
10
No
Address = Address + 512
12
Yes
Perform Checksum on ROM Image
14
Checksum match value in ROM?
16
No
Yes
Execute ROM Entry Point @ Address + 3
18

Figure 1

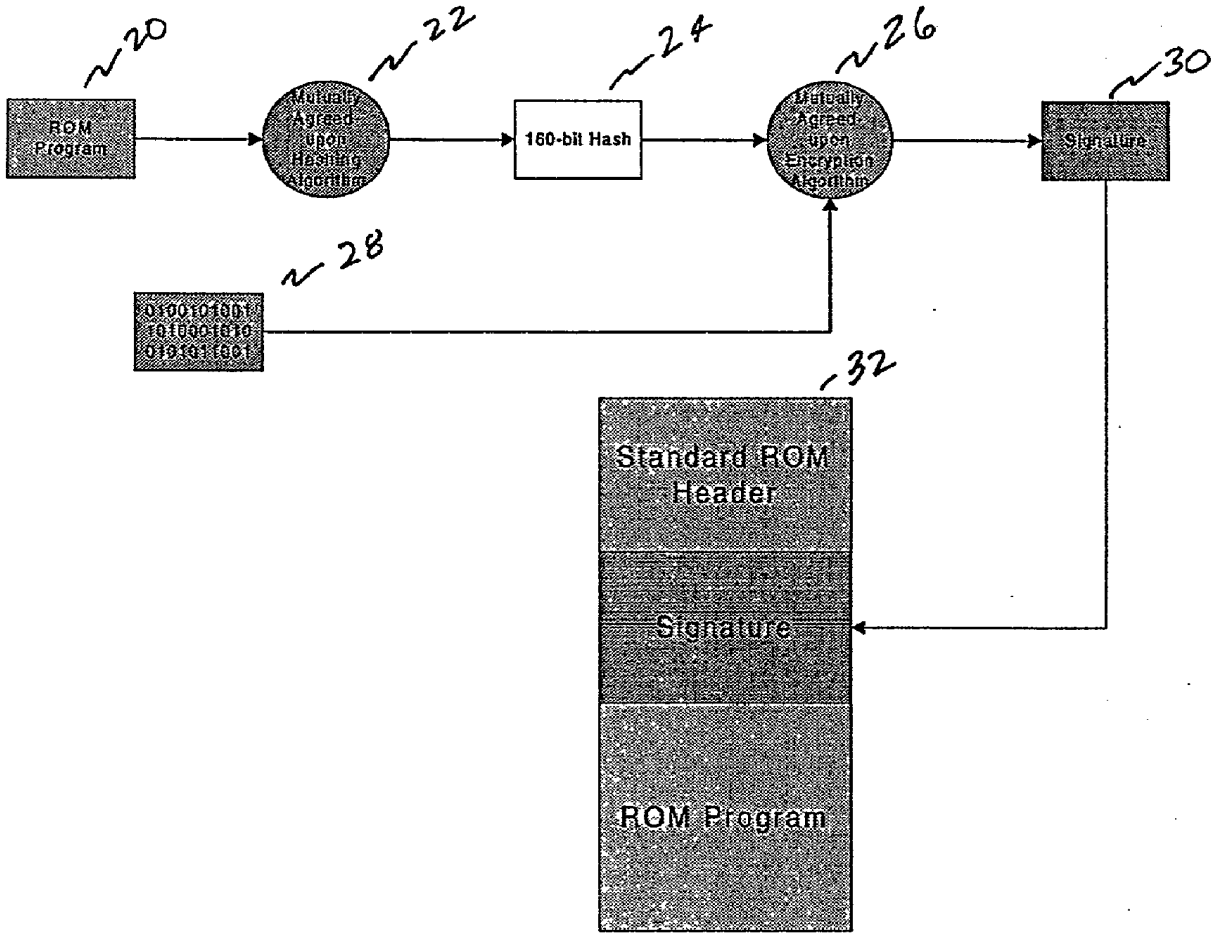

20
22
24
26
30
ROM Program
Mutually Agreed upon Hashing Algorithm
160-bit Hash
Mutually Agreed upon Encryption Algorithm
Signature
28
32
Standard ROM Header
Signature
ROM Program

Figure 2

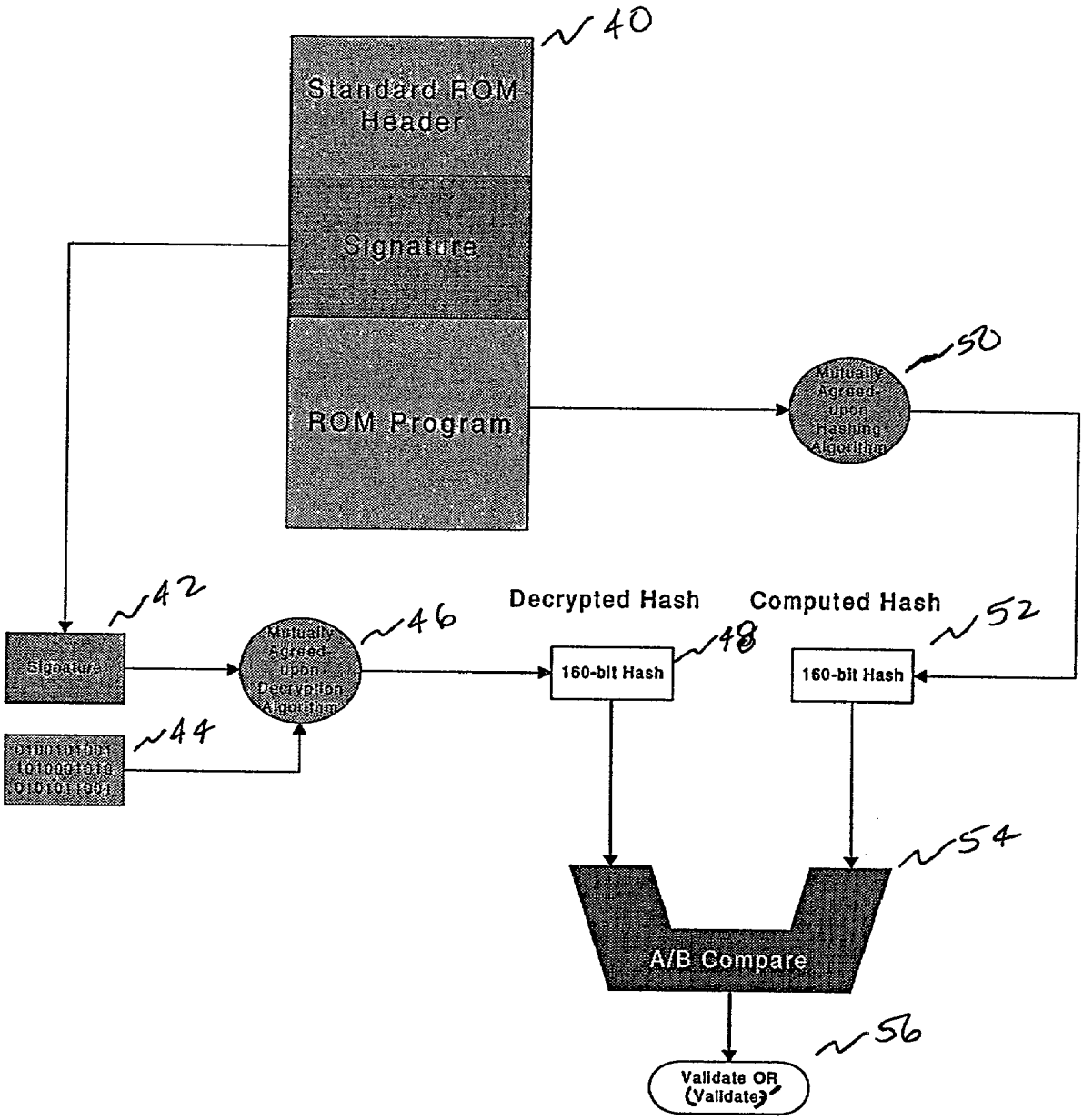

40
Standard ROM Header
Signature
ROM Program
50
Mutually Agreed-upon Hashing Algorithm
42
Signature
46
Mutually Agreed-upon Decryption Algorithm
Decrypted Hash
Computed Hash
52
48
160-bit Hash
160-bit Hash
44
54
A/B Compare
56
Validate OR (Validate)

Figure 3

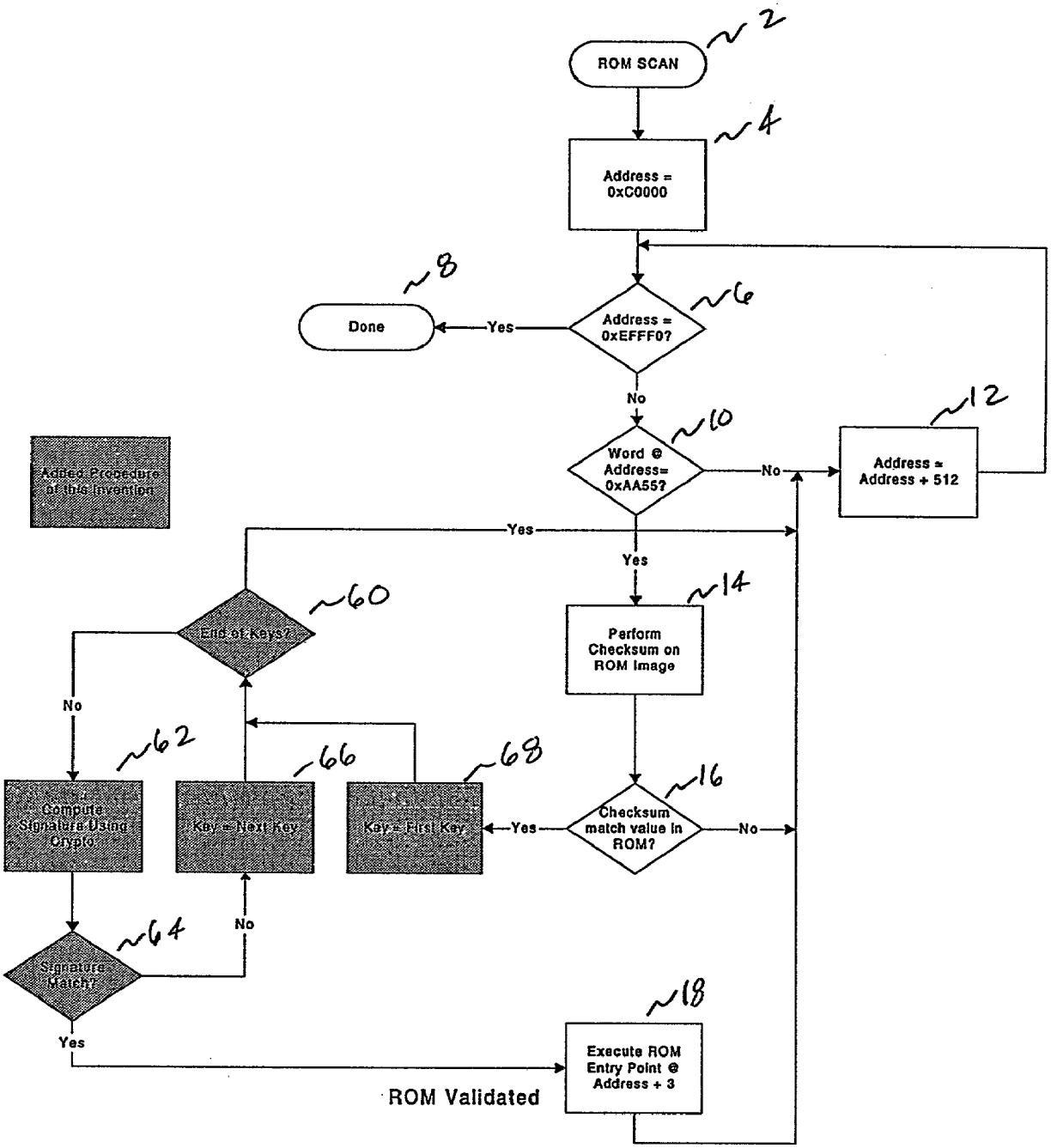

ROM SCAN
2
Address = 0xC0000
4
Address = 0xEFFF0?
6
Done
8
Yes
No
Word @ Address= 0xAA55?
10
No
Address = Address + 512
12
Added Procedure of this Invention
Yes
Yes
Perform Checksum on ROM Image
14
Checksum match value in ROM?
16
Yes
No
End of Keys?
60
No
Compute Signature Using Crypto
62
Key = Next Key
66
Key = First Key
68
Signature Match?
64
No
Yes
Execute ROM Entry Point @ Address + 3
18
ROM Validated

Figure 4

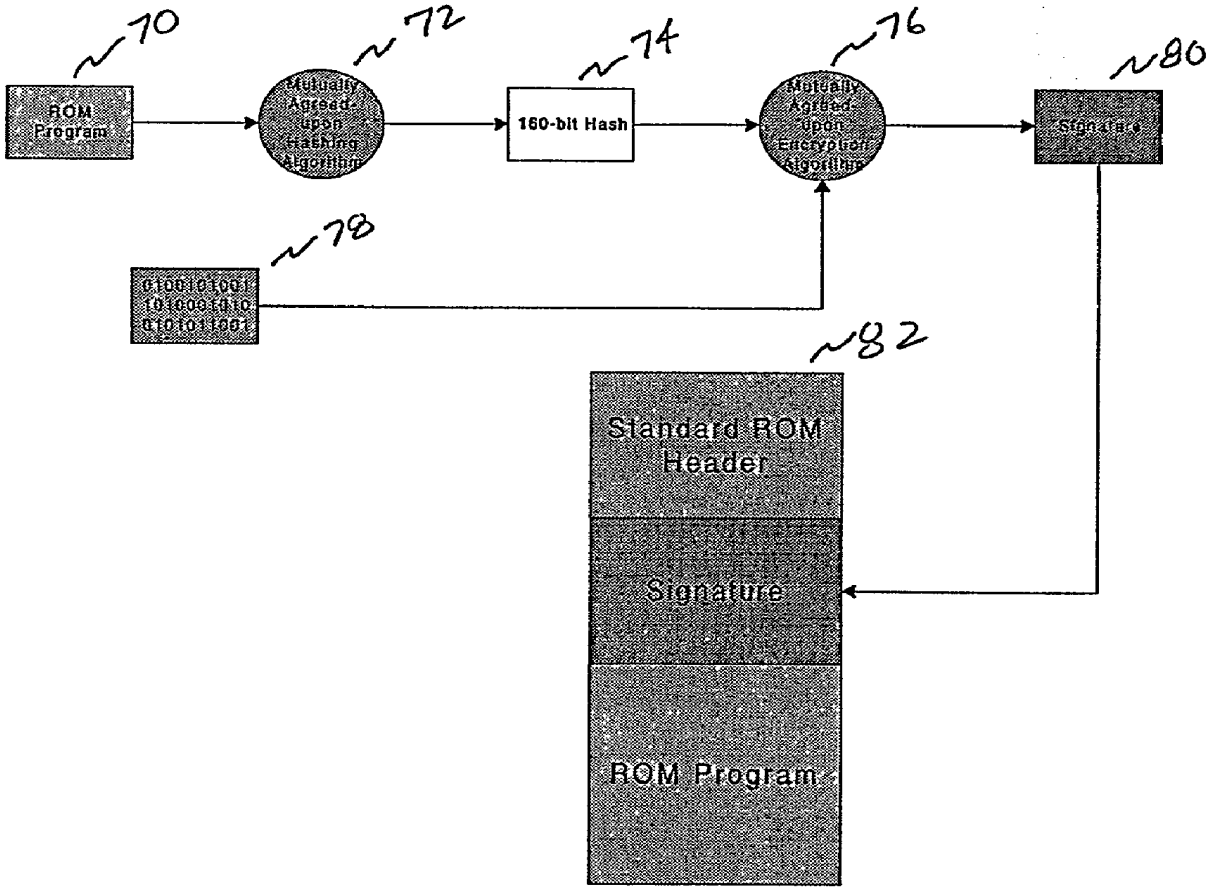

70
72
74
76
80
ROM Program
Mutually Agreed upon Hashing Algorithm
160-bit Hash
Mutually Agreed upon Encryption Algorithm
Signature
78
82
Standard ROM Header
Signature
ROM Program

Figure 5

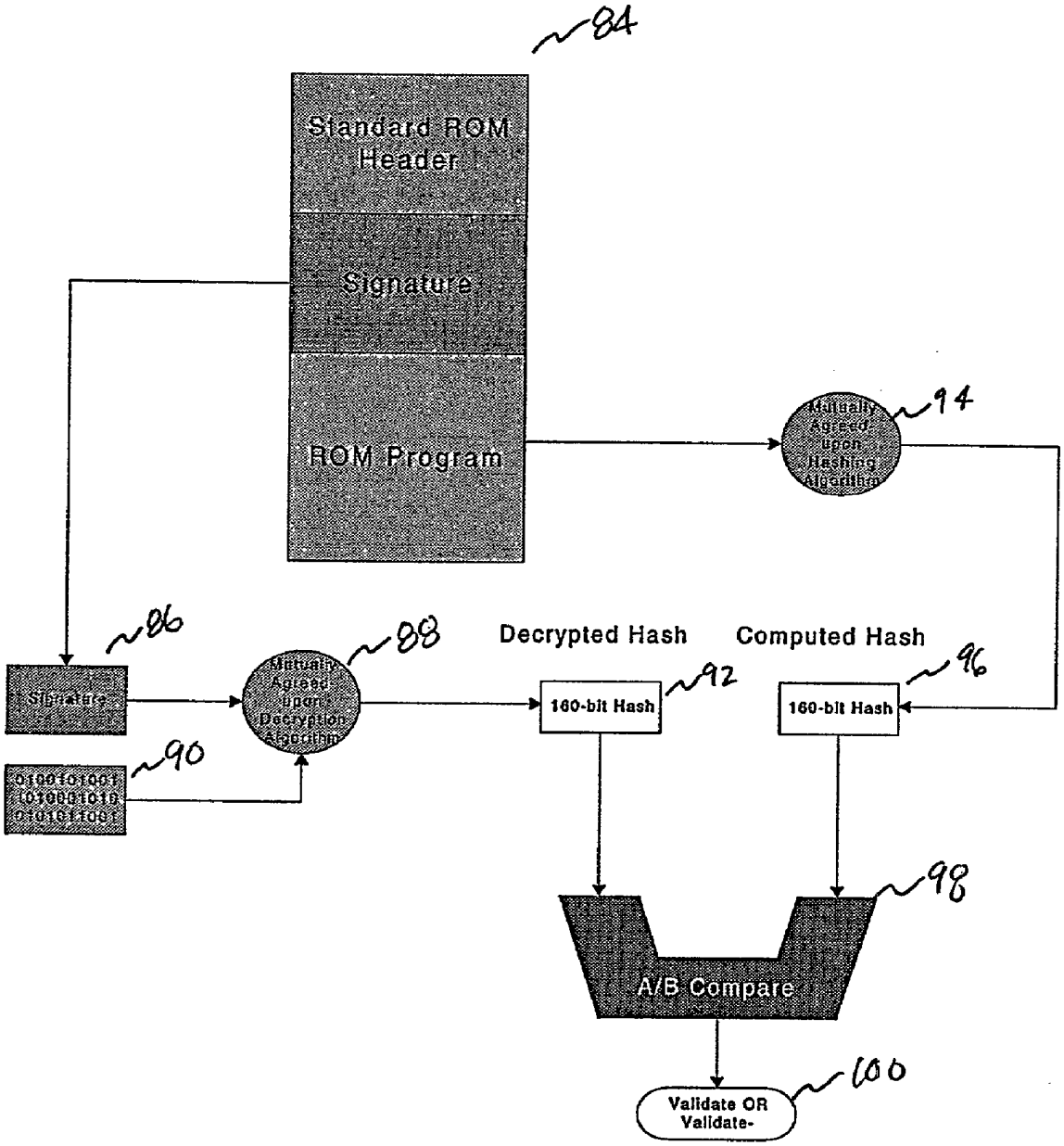

84
Standard ROM Header
Signature
ROM Program
94
Mutually Agreed-upon Hashing Algorithm
86
Signature
88
Mutually Agreed-upon Decryption Algorithm
90
Decrypted Hash
Computed Hash
160-bit Hash
92
160-bit Hash
96
98
A/B Compare
100
Validate OR Validate-

Figure 6

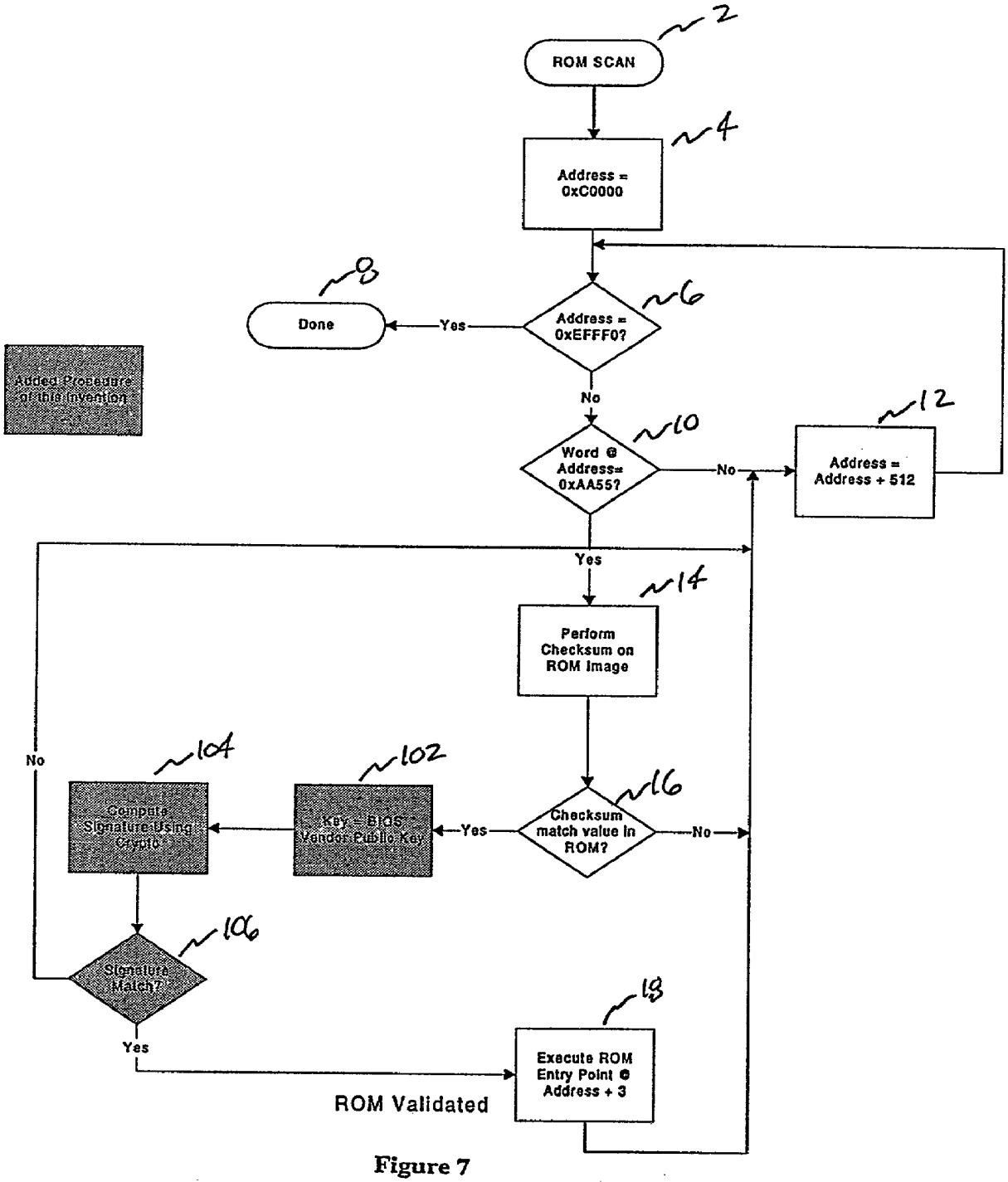

2
ROM SCAN
4
Address = 0xC0000
8
Done
Yes
6
Address = 0xEFFF0?
Added Procedure of this Invention
No
10
Word @ Address= 0xAA55?
No
12
Address = Address + 512
Yes
14
Perform Checksum on ROM Image
No
104
Compute Signature Using Crypto
102
Key = BIOS Vendors Public Key
Yes
16
Checksum match value in ROM?
No
106
Signature Match?
Yes
18
Execute ROM Entry Point @ Address + 3
ROM Validated

Figure 7

METHOD FOR VALIDATING EXPANSION ROMS USING CRYPTOGRAPHY

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates generally to the field of computer security, and more particularly, to a method for validating third-party expansion ROMs in a personal computer using cryptography.

[0003] 2. Description of Related Art

[0004] The original IBM Personal Computer (PC) Basic Input Output System (BIOS) architecture allowed for the inclusion into the system of third-party expansion ROMs—ROMs that share the address space with BIOS, but which are not actually part of the PC BIOS. These third-party expansion ROMs may be present on system plug-in cards, for example. During system initialization, the system BIOS "scans" the proscribed address spaces, looking for a simple byte pattern that designates the start of an expansion ROM. If such a pattern is encountered, the BIOS performs a simple checksum on the ROM image and if the result is correct, the BIOS executes the program contained in the ROM by jumping to an entry point located on a known boundary.

[0005] This procedure for loading expansion ROMs generally works fine in an unsecured environment. However, since the expansion ROM's program is executed without regard for its origin or content, a destructive agent, virus, or program may be introduced into the system during initialization. The security problem has recently become more acute with the advent and proliferation of so-called "temporal devices", i.e., devices which are introduced into the system after normal operating-system initialization.

[0006] The emerging HOT-PLUG PCI standard, which allows for the so-called "Hot Insertion" of a device (inserting a device into a live, powered-up bus, while an operating system is still running), will require that a system agent, in order to detect and configure the device, scan the device for valid expansion ROMs. Without proper security countermeasures, serious system-security compromises may occur. This is especially true in network or file server configurations in which system security is of paramount importance. Hot Insertion will soon be a viable feature which will allow system operators to make dynamic system hardware changes to a server without bringing down the whole network. Therefore, there is a need for a security method for validating expansion ROMs to ensure system integrity.

OBJECTS AND SUMMARY OF THE INVENTION

[0007] The present invention is a method for validating expansion ROMs using cryptography. A ROM image is signed (encrypted) using a private key to create a digital signature. The digital signature is stored along with the ROM image on the ROM. A system BIOS scans the system for the presence of an expansion ROM and when one is detected, the digital signature stored on the ROM is verified (decrypted) using a public key corresponding to the private key. If the verified digital signature matches the ROM image contained on the ROM (or a hashed digest thereof), the BIOS proceeds to load the ROM image.

[0008] A first embodiment of the present invention allows each ROM vendor to use its own private encryption key. The system BIOS then stores a public key corresponding to each ROM vendor's private key in a BIOS database. When an expansion ROM is detected by the system BIOS, each public key is used to verify the ROM until a match occurs, or until all the public keys have been tried.

[0009] In a second embodiment of the present invention, the BIOS vendor digitally signs all the ROM images using its own private key. According to this embodiment, only the public key corresponding to the BIOS vendor's private key needs to be stored in the BIOS and used to verify the expansion ROMs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The exact nature of this invention, as well as its objects and advantages, will become readily apparent from consideration of the following specification as illustrated in the accompanying drawing, and wherein:

[0011] **FIG. 1** is a flowchart depicting a simplified prior-art insecure ROM scan procedure;

[0012] **FIG. 2** is a block diagram illustrating the process of signing a ROM image according to a first embodiment of the present invention;

[0013] **FIG. 3** is a block diagram illustrating BIOS authentication processing of a signed ROM image according to the first embodiment of the present invention;

[0014] **FIG. 4** is a flowchart depicting the simplified ROM scan procedure with the additional processing according to the first embodiment of the present invention;

[0015] **FIG. 5** is a block diagram illustrating the process of signing a ROM image according to a second embodiment of the present invention;

[0016] **FIG. 6** is a block diagram illustrating BIOS authentication processing of a signed ROM image according to the second embodiment of the present invention;

[0017] **FIG. 7** is a flowchart depicting the simplified ROM scan procedure with the additional processing according to the second embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] The following description is provided to enable any person skilled in the art to make and use the invention and sets forth the best modes contemplated by the inventors for carrying out the invention. Various modifications, however, will remain readily apparent to those skilled in the art, since the basic principles of the present invention have been defined herein specifically to provide a method for validating expansion ROMs using cryptography.

[0019] **FIG. 1** depicts a process flow of a simplified prior-art ROM scan procedure. During a system boot-up procedure, the system BIOS scans a personal computer (PC) for the presence of any expansion ROMs at step **2**. The scan begins (step **4**) at address 0xC0000, which is the first possible address for an expansion ROM. This address is an IBM-compatible PC convention and is used universally throughout the PC industry. A boundary check is performed at step **6**. If the current address to be scanned is equal to

0xEFFF0, then there are no more expansion ROMs to be scanned. By industry convention, this boundary address is the end of the possible expansion space. Once the entire expansion space has been scanned, the process flow ends at step **8**. However, if the current address is still within valid expansion ROM address space, then at step **10** the value of the word stored at the current address is compared to the value 0xAA55. The word value is a signature which indicates that the following address space contains expansion ROM code. Again, this signature value is a conventional industry standard.

[**0020**] If the signature value is not present at the current address, then the address is incremented by 512 at step **12**. By industry convention, the expansion ROMs may begin on 512 byte boundaries. The boundary check at step **6** is again performed and the value of the word located at this new address is compared to the signature value. If the signature value matches the value of the word at the current address, then a checksum is performed on the ROM image at step **14**. If the calculated checksum matches a checksum value stored on the ROM (step **16**), then the ROM image is executed beginning at three bytes after the current address (step **18**). If the checksum values do not match, the process continues at step **12**. Likewise, once a ROM image is loaded, the process continues to scan for more ROMs at step **12** until the boundary check condition is met at step **6**.

[**0021**] Note that ordinarily the ROM scan procedure is executed only during the system boot procedure. However, with the advent of hot insertion devices, the ROM scan procedure may be performed upon the detection of the presence of an expansion ROM card, even after the system has already been initialized.

[**0022**] As described, the ROM scan procedure will load any ROM image which contains the standard signature in the correct location, and which passes the simple checksum test. However, the ROM image may contain security breaching code or viruses which will have a harmful effect on the computer system. Therefore, it is desirable to provide a more secure ROM scan process to insure that only valid and approved expansion ROMs are loaded by the system BIOS.

[**0023**] The first embodiment of the present invention is illustrated in FIGS. **2-4**. The following method utilizes a cryptographic process which has both a public key and a private key component. Crypto processes which have a public key and private key are also known as "assymetric" cryptography. One example of such a cryptographic process is the PGP algorithm, which is well known in the cryptographic art. The cryptographic engine may be enabled within a secure processor mode and an associated secure memory area as described in a related patent application entitled "METHOD AND APPARATUS FOR SECURE PROCESSING OF CRYPTOGRAPHIC KEYS" Serial No. , and commonly assigned to the assignee of the present invention. The disclosure of this application is herein incorporated by reference.

[**0024**] The cryptographic engine is used to create and detect the presence of a so-called "digital signature" embedded within a ROM image. A valid digital signature can only be created by a holder of a valid secret key and verified by a holder of the corresponding public key.

[**0025**] **FIG. 2** illustrates the process of signing the ROM image using a private key. Using a mutually-agreed-upon encryption method, such as the PGP algorithm, the public and private keys (key pairs) are generated by an expansion ROM vendor, who maintains the secrecy of the private key. Both the BIOS vendor and the expansion ROM vendors need to mutually agree upon which encryption method to use, in order for the procedure to work correctly. The public key is included in a BIOS database (typically a non-volatile memory) contained on the system. The expansion ROM vendor, using an agreed-upon hashing algorithm **22**, hashes the salient portions of the expansion ROM image **20**, producing a small hash product **24**. A hash algorithm is used to reduce the size of the resulting digital signature, while still providing a high level of security. In this embodiment, a 160-bit hashing algorithm is used, but any agreed upon algorithm may be used. Both the BIOS vendor and the ROM vendors need to mutually agree upon a hashing algorithm before implementing the present invention. This hash product **24** is then signed by the expansion ROM vendor, using its private key **28** and a mutually agreed upon encryption algorithm **26**. The resulting output is known as a "digital signature"**30**. This encryption processing may be performed in a protected environment as described in the above-identified application entitled "METHOD AND APPARATUS FOR SECURE PROCESSING OF CRYPTOGRAPHIC KEYS." The digital signature **30** is then stored along with the original ROM program on the expansion ROM **32**.

[**0026**] **FIG. 3** illustrates the authentication process of an expansion ROM constructed according to the first embodiment of present invention. First, using the signed ROM image **40**, the system BIOS generates a hash product **52** of the ROM program using the mutually agreed upon 160-bit hashing algorithm **50**. Next, the digital signature **42** is decrypted using one of the public keys **44** embedded within a non-volatile storage on the system. The non-volatile storage stores a public key corresponding to each ROM vendor's private key. If the decryption algorithm **46**, using any one of the public keys **44** stored on the system, produces a decrypted hash product **48** which matches bit-for-bit the computed hash product **52** of the ROM program, then the associated ROM program is considered authenticated and secure. The ROM program beginning at the ROM's entry point may then be executed.

[**0027**] Note that only a private key which corresponds to one of the public keys stored in the non-volatile storage will produce a valid signature. Thus, by keeping the private keys secret, only authorized expansion cards manufactured by authorized vendors will be recognized and loaded.

[**0028**] **FIG. 4** depicts the simplified ROM scan process of **FIG. 1** with the additional steps required to validate the ROM program according to the first embodiment of the present invention. The additional steps are shown in darker shades. The operation of steps **2-14** are identical to the operation of the corresponding steps in **FIG. 1** and a description of these steps will not be repeated here. Beginning at step **16**, if there is a checksum match, the variable "key" is set to the value "first key" at step **68**, otherwise the normal process continues at step **12**.

[**0029**] After step **68**, the processing enters the key processing loop. If all the available keys have been processed at step **60**, then the normal processing continues at step **12**. If there are remaining keys to process, then at step **62** the

digital signature of the current ROM image is decrypted using the present public key. If the decrypted signature matches the hashed ROM image, then the ROM image is executed at step **18**. If the decrypted signature does not match the hashed ROM image, however, then the next public key stored in the non-volatile storage is used at step **66**. If all the keys have been used, and there is still no match, the key processing loop exits at step **60** and the normal processing continues at step **12**. Thus, if an expansion ROM is inserted into the system, without the proper digital signature, the associated ROM image will not be executed during the ROM scan process. This protects the system from loading unauthorized expansion ROMs which may cause system malfunctions by introducing viruses or security breaching code into the system.

[**0030**] **FIG. 5** illustrates a second embodiment of the present invention. This second embodiment differs from the first embodiment in that the third-party ROM vendor must first send the ROM program **70** to the BIOS vendor. The BIOS vendor then generates the same type of hash digest **74** of the ROM image **70** as is used in the first embodiment, using the same type of agreed upon 160-bit hashing algorithm **72**. The BIOS vendor then signs the digest **74** by encrypting the digest **74** with its own private key **78**. The signed, encrypted digest **80** is then sent back to the third-party expansion ROM vendor, who then integrates the signature into a new ROM image **82** before manufacturing.

[**0031**] The authentication process for the second embodiment of the present invention is shown in **FIG. 6**. At runtime, the system BIOS authenticates the ROM image **84** by decrypting the signature portion, using the agreed-upon decryption algorithm **88** and the BIOS vendor's public key **90**. The ROM program is also hashed using the mutually agreed upon hashing algorithm **94**. If the decrypted digest **92** matches (A/B compare **98**) bit-for-bit with the hashed digest **96**, then the program is considered validated and safe to execute; otherwise it is considered invalidated and it is not executed (step **100**).

[**0032**] The second embodiment simplifies the runtime processing requirements since only a single key is required to be contained within the BIOS database, i.e. the BIOS vendor's public key. **FIG. 7** illustrates the additional ROM scan steps needed for this second embodiment. Steps **2-14** are identical to the operation of the corresponding steps in **FIG. 1** and a description of these steps will not be repeated here. Beginning at step **16**, if there is a checksum match, the BIOS vendor's public key is read at step **102** and is used at step **104** to decrypt the signature. If the signature matches the computed hash digest at step **106**, then the ROM image is loaded at step **18**. Otherwise, the processing returns to step **12** in order to check the next possible address for an expansion ROM.

[**0033**] One drawback to this second method is that each release of an expansion ROM vendor's ROM program must be sent to the BIOS vendor, hashed, signed and returned back to the ROM vendor. As a practical matter, this procedure may be too cumbersome for certain applications. The advantage of the second embodiment, however, is that only one public key needs to stored in the system BIOS, reducing the amount of required non-volatile storage.

[**0034**] By incorporating the present invention into personal computer systems, BIOS vendors can provide a high-level of security to the systems, guaranteeing that no questionable expansion ROMs will ever be executed. In systems which support the "hot insertion" of expansion cards, the present invention can be invoked each time a new card is detected in order to ensure that only authorized ROM programs are loaded into the system. This provides a much greater level of system protection than is currently available.

[**0035**] Those skilled in the art will appreciate that various adaptations and modifications of the just-described preferred embodiments can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

What is claimed is:

1. A method for validating an expansion ROM card containing a ROM program, the method comprising the steps of:

creating a digital signature by signing (encrypting) the ROM program using a private key and a mutually agreed upon encryption algorithm;

storing the digital signature on the expansion ROM card;

decrypting the digital signature on the ROM card using a public key corresponding to the private key; and

comparing the decrypted digital signature with the ROM program;

wherein if the decrypted digital signature matches the ROM program, then the expansion ROM card is validated and loaded, and wherein if the decrypted digital signature does not match the ROM program, then the expansion ROM card is not validated and is not loaded.

2. The method of claim 1, wherein the step of creating a digital signature comprises the steps of:

creating a hash digest of the ROM program using a mutually agreed upon hashing algorithm; and

signing the hash digest using the private key and the mutually agreed upon encryption algorithm.

3. The method of claim 2, wherein the step of comparing comprises comparing the decrypted digital signature to a hash digest of the ROM image, wherein the hash digest is created using the mutually agreed upon hashing algorithm.

4. The method of claim 3, wherein each vendor of expansion ROM cards creates a unique digital signature using a unique private key.

5. The method of claim 4, wherein a system BIOS stores a public key corresponding to each ROM vendor's unique private key.

6. The method of claim 5, wherein each public key is used to decrypt (verify) the digital signature until a match is detected, or until all the public keys stored in the system BIOS have been used.

7. The method of claim 3, wherein a BIOS vendor creates the digital signature using a single private key.

8. The method of claim 7, wherein a system BIOS stores a single public key corresponding to the BIOS vendor's private key.

9. The method of claim 6, wherein the steps of decrypting the digital signature and of creating a hash digest of the stored ROM image are performed during a secure processor mode and in an associated secure memory area.

10. The method of claim 8, wherein the steps of decrypting the digital signature and of creating a hash digest of the stored ROM image are performed during a secure processor mode and in an associated secure memory area.

11. A method for validating an expansion ROM card containing a ROM program, the method comprising the steps of:

signing (encrypting) the ROM program to create a digital signature, the step of signing further comprising the steps of:

creating a first hash digest of the ROM program using a hashing algorithm known by both a ROM vendor and a BIOS vendor;

encrypting the first hash digest of the ROM program using a ROM vendor's private key, and an encryption algorithm known by both the ROM vendor and the BIOS vendor;

storing the digital signature on the expansion ROM card;

storing a public key corresponding to each ROM vendor's private key in a system BIOS;

decrypting the digital signature on the ROM card using a public key corresponding to the ROM vendor's private key, the public key stored in the system BIOS;

calculating a second hash digest of the ROM image using the hashing algorithm; and

comparing the decrypted digital signature with the second hash digest;

wherein if the decrypted digital signature matches the second hash digest, then the expansion ROM card is validated and loaded, and wherein if the decrypted digital signature does not match the hash digest, then the expansion ROM card is not validated and is not loaded.

12. The method of claim 11, wherein the steps of decrypting the digital signature and of creating a second hash digest of the stored ROM image are performed during a secure processor mode and in an associated secure memory area.

13. A method for validating an expansion ROM card containing a ROM program, the method comprising the steps of:

signing (encrypting) the ROM program to create a digital signature, the step of signing further comprising the steps of:

creating a first hash digest of the ROM program using a hashing algorithm;

encrypting the first hash digest of the ROM program using a BIOS vendor's private key, and an encryption algorithm;

storing the digital signature on the expansion ROM card;

storing a public key corresponding to the BIOS vendor's private key in a system BIOS;

decrypting the digital signature on the ROM card using the public key corresponding to the BIOS vendor's private key, the public key stored in the system BIOS;

calculating a second hash digest of the ROM image using the hashing algorithm; and

comparing the decrypted digital signature with the second hash digest;

wherein if the decrypted digital signature matches the hash digest, then the expansion ROM card is validated and loaded, and wherein if the decrypted digital signature does not match the hash digest, then the expansion ROM card is not validated and is not loaded.

14. The method of claim 13, wherein the steps of decrypting the digital signature and of creating a second hash digest of the stored ROM image are performed during a secure processor mode and in an associated secure memory area.

* * * * *

Electronic Patent Application Fee Transmittal

Application Number:	12355900
Filing Date:	19-Jan-2009
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Filer:	Nathan Eldon Black/Nancy Nolan
Attorney Docket Number:	2162.162700/DE0892

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	13082879
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	Nathan Eldon Black/Nancy Nolan
Filer Authorized By:	Nathan Eldon Black
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	22-JUN-2012
Filing Date:	19-JAN-2009
Time Stamp:	14:06:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	350
Deposit Account	500786
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	Information_Disclosure_Statement_Letter.pdf	87710 d6c1d6c035ffed88bb3fbd5c53c949bb117ed5d6	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	EFS_IDS_Form.pdf	612287 1c3d50034595d6a825353e83106e9b7fb43ab2a1	no	4
Warnings:					
Information:					
3	Foreign Reference	PCT_Search_Report.pdf	1105254 8986f47774e33cfcca1d2d58a4dbc478218ab628	no	20
Warnings:					
Information:					
4	Foreign Reference	EP1659472.pdf	224295 d4ef94872bac53e6cf467daade9ab9a04c792ab7	no	12
Warnings:					
Information:					
5	Foreign Reference	20070192610.pdf	947584 7e771f82c3b5a29c9210cf38dc5b56b6fdfd0391	no	16
Warnings:					
Information:					
6	Foreign Reference	20060112266.pdf	480663 baf9f98b9c8c34d7ab41fed3dc2f7336e98349ea	no	8
Warnings:					
Information:					
7	Foreign Reference	20050076226.pdf	591053 4f48f0a5c5328fe1ba727016d05ffa8e50df7949	no	12
Warnings:					
Information:					
8	Foreign Reference	20010007131.pdf	828005 965754d18976c3ffca2e047102187 0f527464e9b	no	12
Warnings:					
Information:					

9	Fee Worksheet (SB06)	fee-info.pdf	30567 889f46183a5b651714080475e477b7c9f6f9008f	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	4907418

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Confirmation No.: 7735 Group Art Unit: 2115
Serial No.: 12/355,900	Examiner: Jaweed A. Abbaszadeh
Filed: January 19, 2009	Att'y Docket: 2000.162700/DE0892
For: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRIPTION	Customer No.: 10742

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In compliance with the duty of disclosure under 37 C.F.R. § 1.56, it is respectfully requested that this Information Disclosure Statement be entered and the documents listed on attached Form PTO/SB/08a be considered by the Examiner and made of record. Copies of the listed foreign patent document and foreign official communication have been submitted herewith, where applicable.

In accordance with 37 C.F.R §§ 1.97(g),(h), this Information Disclosure Statement is not to be construed as a representation that a search has been made, and is not to be construed to be an admission that the information cited is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

A fee as set forth in 37 C.F.R. § 1.17(p) in the amount of $180.00 is due. The Commissioner is hereby authorized to deduct said fee from Williams, Morgan & Amerson, P.C., Deposit Account No. 50-07860/2162.162700/DE0892.

Applicants respectfully request that the listed documents be made of record in the present case.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 10742

Date: June 22, 2012

By: /Nathan E. Black/
Nathan E. Black Reg. No. 66,191
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4093
(713) 934-7011 (facsimile)

ATTORNEY FOR APPLICANT(S)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

10742 7590 10/10/2012

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

EXAMINER	
ABBASZADEH, JAWEED A	
ART UNIT	PAPER NUMBER
2115	

MAIL DATE	DELIVERY MODE
10/10/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	12/355,900	GRELL ET AL.	
	Examiner	Art Unit	
	JAWEED A. ABBASZADEH	2115	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *7-18* is/are allowed.

7)☒ Claim(s) *1-5 and 19-21* is/are rejected.

8)☒ Claim(s) *6* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/22/2012*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-21 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 19, and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320 in view of Kumar et al. (hereinafter 'Kumar') US 2008/0159541.

Bhatt was cited as the prior art reference in the previous office action. As such, his relevant teachings are hereby incorporated by reference.

As to claim 1, Bhatt teaches a method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit [Fig. 2, execute verification code on reset 205, 0024—"verification code from boot storage 130" Boot storage 130 is located on the processor package as shown in Fig. 1], said computer system containing an encryption key [0025—"Any now known or later developed hashing…or similar algorithm...may be stored in boot storage 130" A signature is determined using the key];

determining a current signature of at least a signed portion of boot data [0027—"the verification code executed by processor 120 may compute a signature of the boot code 180"], said signed portion of boot data containing a stored signature of said portion of boot data [0027—"signature value from ID storage"], said stored signature created by applying said encryption key [0025—"Any now known or later developed hashing…or similar algorithm...may be stored in boot storage 130 and used in act 225" Act 225 initially computed the signature of the boot code and stored it.]; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical [0028—"If the computed signature from act 245 matches the corresponding signature value from ID storage 140 [act 250], processor 120 the verification code executed by processor 120 may permit further booting from boot code 180 in external memory 160 [act 255]."

Bhatt does not teach said internal non-volatile memory area containing an encryption key. Specifically, Bhatt is silent regarding the location of the key.

Kumar is cited to teach a similar method that involves secure booting. Kumar further teaches said internal non-volatile memory area containing an encryption key [0016—" a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form"]. It would have been obvious to one of ordinary skill in the art to have combined the teachings of Bhatt and Kumar because they are both directed towards securely booting. Furthermore, Bhatt does not provide teaching for the location of the

key. Kumar provides teaching that specifies the location of a key in a secure booting environment.

As to claim 2, Kumar teaches executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory [0032--"This provides the ability for a special code module, referred to as the authenticated code module (AC module), to be loaded into internal RAM (referred to as authenticated code execution area) within the processor"].

As to claim 3, Kumar teaches executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data [0029].

As to claim 4, Kumar teaches wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache [0029—It is well known in the art that booting involves loading boot data into cache in order for it to be executed by the processor].

As to claim 19, Bhatt and Kumar teach this claim according to the reasoning set forth in claim 1 supra.

As to claim 21, Bhatt and Kumar teach this claim according to the reasoning set forth in claim 1 supra.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhatt et al. (hereinafter 'Bhatt') US 2006/0107320 in view of Kumar et al. (hereinafter 'Kumar') US 2008/0159541 and in view of Tugenberg et al. (hereinafter 'Tugenberg') US 7,103,782.

As to claims 5, Bhatt and Kumar teach the method of claim 1, but do not teach locking said encryption key for external access prior to executing said boot instructions.

Tugenberg is cited to teach a method that utilizes an encryption key stored in secure memory. Tugenberg further teaches locking said encryption key for external access prior to executing said boot instructions [Fig. 3]. When blocking gates are enabled in step 314, the encryption key is "locked." It would have been obvious to one of ordinary skill in the art to have combined the teachings of Bhatt and Kumar with Tugenberg because they are all directed towards utilizing an encryption key. Tugenberg improves upon Bhatt and Kumar because Tugenberg's system is more secure. It prevents access to the encryption key when access is not needed [col. 8, lines 4-5].

As to claim 20, Tugenberg teaches this claim according to the reasoning set forth in claim 5 supra.

Allowable Subject Matter

Claims 7-18 are allowed.

Claim 6 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Applicant's arguments, see remarks, filed 6/22/2012 with respect to the rejection(s) of claim(s) 1 and 2 under 35 U.S.C. 102 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Kumar et al. US 2008/0159541.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAWEED A. ABBASZADEH whose telephone number is (571)270-1640. The examiner can normally be reached on Mon-Fri: 8:30 a.m.-6:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas C. Lee can be reached on (571) 272-3667. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAWEED A ABBASZADEH/
Examiner, Art Unit 2115
10/5/12

Notice of References Cited	Application/Control No. 12/355,900	Applicant(s)/Patent Under Reexamination GRELL ET AL.	
	Examiner JAWEED A. ABBASZADEH	Art Unit 2115	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0016348 A1	01-2008	Craft et al.	713/168
*	B	US-2008/0159541 A1	07-2008	Kumar et al.	380/278
*	C	US-2009/0055656 A1	02-2009	Mersh, John David	713/187
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

SEARCHED			
Class	Subclass	Date	Examiner
713	1, 2	10/10/2011	JA
713	176	10/10/2011	JA

SEARCH NOTES		
Search Notes	Date	Examiner
Performed EAST search, see results attached	8/29/2011	JA
Updated EAST search, see results attached	3/13/2012	JA
Performed Google Patents search, see results attached	3/13/2012	JA
Updated EAST search, see results attached	10/1/2012	JA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12355900
Filing Date	2009-01-19
First Named Inventor	Michael Grell
Art Unit	2115
Examiner Name	Jaweed A. Abbaszadeh
Attorney Docket Number	2162.162700/DE0892

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010007131	A1	2001-05-01	Galasso et al.	
	2	20050076226	A1	2005-04-07	Boivie et al.	
	3	20070192610	A1	2007-08-16	Chun et al.	
	4	20060112266	A1	2006-05-25	Little et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12355900
	Filing Date	2009-01-19
	First Named Inventor	Michael Grell
	Art Unit	2115
	Examiner Name	Jaweed A. Abbaszadeh
	Attorney Docket Number	2162.162700/DE0892

	1	1659472	EP	A1	2006-05-24			☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	PCT Search Report and Written Opinion from PCT/US2009/001289 dated August 3, 2009	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jaweed Abbaszadeh/	Date Considered	10/05/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12355900
	Filing Date	2009-01-19
	First Named Inventor	Michael Grell
	Art Unit	2115
	Examiner Name	Jaweed A. Abbaszadeh
	Attorney Docket Number	2162.162700/DE0892

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Nathan E. Black/	Date (YYYY-MM-DD)	2012-06-22
Name/Print	Nathan E. Black	Registration Number	66191

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	("20010007131" | "20050076226" | "20060112266" | "20070192610").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/05 13:02
S1	1	("20060107320").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/08/31 10:16
S2	1	("20060112266").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/01 14:17
S3	0	(11/046943).APP.	USPAT; USOCR	OR	ON	2012/10/01 14:33
S4	3	("2006/0112266").URPN.	USPAT	OR	ON	2012/10/01 14:34
S5	68	sign$3 near3 (boot adj (data or code))	USPAT	OR	ON	2012/10/01 14:45
S6	60	S5 and @ad<"20080430"	USPAT	OR	ON	2012/10/01 14:46
S7	1	("20050076226").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/01 14:55
S8	68209	("713").CLAS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/01 16:29
S9	1212	tpm and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:29
S10	172	tpm.ab. and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:40
S11	60	S10 and @ad<"20080430"	USPAT	OR	ON	2012/10/01 16:40
S12	127	S10 and @ad<"20080430"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:41
S13	351	tpm same signature and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:42
S14	14	(tpm same signature).ab. and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:42
S15	403	(tpm with (processor or cpu)) and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:55
S16	254	(tpm near5 (processor or cpu)) and S8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 16:55
S17	174	S16 and @ad<"20080430"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/01 17:07
S18	3	(tpm near2 within near3 (processor	US-PGPUB;	OR	ON	2012/10/01

		or cpu)) and S8	USPAT; USOCR; EPO; JPO			17:35
S19	68329	("713").CLAS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/02 10:04
S20	69	(key near2 within near3 (processor or cpu)) and S19	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/02 10:04
S21	44	S20 and @ad<"20080430"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/02 10:04
S22	2006	(ram near3 within near3 (processor or cpu))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/02 14:41
S23	68329	("713").CLAS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/02 14:42
S24	148	S22 and S23	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/02 14:42
S25	119	S24 and @ad<"20080430"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/10/02 14:45
S26	1	("6885867").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/03 10:35
S27	1	("20030097598").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/03 11:29

EAST Search History (Interference)

< This search history is empty>

10/ 5/ 2012 1:07:27 PM
C:\ Users\ jabbaszadeh\ Documents\ CASES\ 12355900\ amend1.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/10/2011	03/18/2012	10/05/2012						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	O						
	7	O	✓	=						
	8	O	✓	=						
	9	O	✓	=						
	10	O	✓	=						
	11	O	✓	=						
	12	O	✓	=						
	13	=	=	=						
	14	=	=	=						
	15	=	=	=						
	16	=	=	=						
	17	=	=	=						
	18	=	=	=						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL GRELL RALF FINDEISEN FRANK SCHUECKE	Group Art Unit: 2115 Examiner: JAWEED A. ABBASZADEH
Serial No.: 12/355,900	Conf. No.: 7735
Filed: January 19, 2009	Atty. Docket: 2162.162700/DE0892 CUSTOMER NO.: 10742

For: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

RESPONSE TO OFFICE ACTION DATED OCTOBER 10, 2012

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is submitted in response to the Office Action mailed October 10, 2012, for which the shortened three-month statutory response date is January 10, 2013. This response is being filed on or before the due date, therefore, it is timely filed.

If an extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, this paper is to be construed as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

No other fee is believed due as a result of the response contained herein. However, should any other fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason, the Commissioner is authorized to deduct said fees from Williams, Morgan & Amerson, P.C.'s Deposit Account No. 50-0786/2162.162700.

Amendments to the claims are found in the complete listing of claims beginning on page 3 of this paper.

Remarks begin on page 8 of this paper.

AMENDMENT TO THE CLAIMS

1. (Original) A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

2. (Original) The method of claim 1, wherein executing said instructions stored in said internal non-volatile memory area comprises initializing an internal random access memory of said central processing unit and loading said at least a portion of boot data from a non-volatile memory into said initialized random access memory.

3. (Original) The method of claim 2, wherein executing boot instructions of said signed portion of boot data comprises initializing a system memory of said computer system and loading said boot data from said non-volatile memory into said system memory and verifying an integrity of said boot data.

4. (Original) The method of claim 2, wherein initializing said internal random access memory comprises initializing a data cache and an instruction cache of said central processing unit and wherein said at least a portion of boot data is loaded into said data cache.

5. (Original) The method of claim 1, further comprising locking said encryption key for external access prior to executing said boot instructions.

6. (Original) The method of claim 5, further comprising determining whether an upgrade version of said boot data is available.

7. (Previously Presented) A method for booting a computer system, the method comprising:

upon one of a power-on and a reset event, executing instructions stored in an internal non-volatile memory area of a central processing unit, said internal non-volatile memory area containing an encryption key;

determining a current signature of at least a signed portion of boot data, said signed portion of boot data containing a stored signature of said portion of boot data, said stored signature created by applying said encryption key;

locking said encryption key for external access prior to executing said boot instructions;

determining whether an upgrade version of said boot data is available, wherein determining whether an upgrade version of said boot data is available is performed prior to locking said encryption key; and

executing boot instructions contained in said signed portion of boot data, when said current signature and said stored signature are identical.

8. (Original) The method of claim 7, further comprising verifying said upgrade version of said boot data.

9. (Original) The method of claim 8, further comprising calculating a new signature over a hash sum of said upgrade version of the boot data using said encryption key and adding said new signature to said upgrade version of the boot data.

10. (Original) The method of claim 9, further comprising enabling said upgrade version of said boot data.

11. (Original) The method of claim 10, further comprising generating a reset event.

12. (Original) The method of claim 10, further comprising locking said encryption key prior to enabling said upgrade version of the boot data.

13. (Original) A method for booting a computer system, the method comprising:

upon at least one of a power-up event and a reset event, accessing an internal non-volatile memory of a central processing unit, said internal non-volatile memory containing pre-boot instructions and data values for initializing an internal volatile memory of said central processing unit and verifying an integrity of at least a portion of boot instructions and boot data values;

loading said at least a portion of said boot instructions and boot data values from a non-volatile memory into said internal volatile memory by executing said pre-boot instructions;

verifying integrity of said at least a portion of said boot instructions and boot data values by using an encryption key stored in said internal non-volatile memory and a signature associated with said at least a portion of said boot instructions and boot data values, said signature being formed on the basis of said encryption key;

after successfully verifying integrity of said at least a portion of said boot instructions and boot data values, determining whether an upgrade version of said boot instructions and boot data values is available; and

when an upgrade version is available, generating a signature of said upgrade version by using said encryption key.

14. (Original) The method of claim 13, wherein executing said boot instructions comprises initializing a system memory of said computer system and loading a second portion of boot instructions and boot data values into said system memory.

15. (Original) The method of claim 14, further comprising verifying integrity of said second portion and continuing booting of said computer system on the basis of said second portion when verification of said second portion is successful.

16. (Original) The method of claim 13, wherein initializing said volatile internal memory comprises initializing a data cache of said central processing unit and wherein said at least a portion is loaded into said data cache and is verified therein.

17. (Original) The method of claim 13, further comprising locking said encryption key prior to executing said boot instructions when an upgrade version is not available.

18. (Original) The method of claim 13, further comprising verifying said upgrade version of the boot instructions and boot data prior to generating said new signature.

19. (Original) A central processing unit (CPU), comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory; and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key.

20. (Original) The central processing unit of claim 19, further comprising a locking mechanism configured to enable a portion of said non-volatile memory containing said symmetric encryption key upon one of a reset event and a power-on event only.

21. (Original) A computer system, comprising:

a central processing unit comprising:

a substrate having formed thereon circuit elements defining a CPU core, a volatile random access memory, a non-volatile memory and a bus system for connecting said CPU core, said volatile random access memory and said non-volatile memory, and

pre-boot information stored in said non-volatile memory, said pre-boot information including instructions executable by said CPU core and a symmetric encryption key for verifying at least a portion of a boot routine signed by using said symmetric encryption key; and

a non-volatile boot memory configured to hold at least said boot routine and a second boot routine.

REMARKS

Claims 1-21 are pending in the present application. No new matter has been introduced by way of the present response. Reconsideration of the present application is respectfully requested in view of the arguments set forth herein.

Prior Art Rejections

In the Office Action, the Examiner rejected claims 1-4, 19, and 21 under 35 U.S.C. §103(a) is allegedly being obvious over Bhatt (U.S. Patent Application Publication No. 2006/0107320) in view of Kumar (U.S. Patent Application Publication No. 2008/0159541). The Examiner rejected claims 5 and 20 under 35 U.S.C. §103(a) as being obvious over Bhatt and Kumar in view of Tugenberg (U.S. Patent No. 7,103,782). Applicants respectfully traverse the Examiner's rejections.

A finding of obviousness under 35 U.S.C. § 103 requires a determination of the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed subject matter and the prior art, and whether the differences are such that the subject matter as a whole would have been obvious to one of ordinary skill in the art at the time the invention was made. *Graham v. John Deere Co.*, 148 USPQ 459 (U.S. S.Ct. 1966). To determine whether the subject matter as a whole would have been obvious to one of ordinary skill in the art at the time the invention was made, one should determine whether the prior art reference (or references when combined) teach or suggest all the claim limitations. Furthermore, it is necessary for the Examiner to identify the reason why a person of ordinary skill in the art would have combined the prior art references in the manner set forth in the claims. Moreover, there should be a reasonable expectation of success on the part of a person of ordinary skill in the

art. Teaching away by the prior art may constitute *prima facie* evidence that the claimed invention is not obvious.

Applicants respectfully submit that the prior art of record does not teach or suggest all the limitations set forth in the pending claims, for at least the following reasons.

First, Applicants respectfully submit that the combination of Bhatt and Kumar does not teach or suggest an internal non-volatile memory area of a central processing unit that contains an encryption key that is used to determine a current signature of a portion of boot data. As admitted by the Examiner on page 3 of the Office Action, Bhatt is silent regarding the location of a key used to determine a computed signature. Paragraph [0016] of Kumar describes storing a cryptographic key called a processing unit key (PUK) in a non-volatile form in the processor. However, paragraph [0016] of Kumar also teaches that the PUK is used to encrypt and protect a third-party key (3PK). Applicants therefore respectfully submit that the PUK described by Kumar is *not* an encryption key that is used to determine a current signature of a portion of boot data, as set forth in the pending claims.

Second, Applicants respectfully submit that Bhatt does not teach or suggest determining a current signature of a portion of boot data that contains a stored signature of the portion of boot data. Paragraph [0027] of Bhatt describes forming a signature using boot code 180 and comparing the signature to a corresponding signature value from storage 140. Figure 4 of Bhatt shows that the ID storage 140 is a part of the processor package 110 while the boot code 180 is a part of the external memory 160. Consequently, the signature computed using boot code 180 cannot be computed using the corresponding signature value from ID storage 140 because the boot code 180 and the ID storage 140 are implemented in completely different devices. Kumar also fails to teach or suggest this limitation. Applicants therefore respectfully submit that the

combination of Bhatt and Kumar does not teach or suggest determining a current signature using a portion of boot data that contains a stored signature of the portion of boot data.

Tugenberg describes locking an encryption key. However, Tugenberg does not remedy the aforementioned fundamental deficiencies in the combination of Bhatt and Kumar. Applicants therefore respectfully submit that the prior art of record does not teach or suggest all the limitations set forth in the pending claims.

Applicants further submit that persons of ordinary skill in the art would not have been motivated to combine and modify the prior art of record to arrive at the claimed subject matter. To the contrary, Bhatt teaches away from the claimed subject matter. For example, Bhatt describes a technique for verifying the trustworthiness of an external memory 160. Bhatt therefore teaches that the signature of the boot code 180 should be compared to a previously calculated signature that has been stored in the ID storage 140 so that the identity or trustworthiness of the external memory 160 can be verified. Applicants therefore respectfully submit that Bhatt teaches away from storing previously calculated signatures with portions of the boot code 180 in the external memory 160. Consequently, Bhatt teaches away from determining a current signature using a portion of boot data that contains a stored signature of the portion of boot data, as set forth in the pending claims.

For at least the aforementioned reasons, Applicants respectfully submit that the pending claims would not have been obvious over the prior art of record. Applicants respectfully request that the Examiner's rejections of claims 1-5 and 19-20 under 35 U.S.C. § 103(a) be withdrawn.

Allowable Subject Matter

Applicants acknowledge and appreciate the Examiner's indication of allowable subject matter. In the Office Action, the Examiner indicated that claims 7-18 are allowable. The Examiner also indicated that claim 6 includes allowable subject matter. Pursuant to the arguments presented herein, Applicants respectfully submit that claim 6 is in condition for allowance.

Conclusion

Applicants respectfully assert that all claims of the present application are now allowable and, therefore, request that a Notice of Allowance be issued. Reconsideration of the present application is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is respectfully requested to call the undersigned at (713) 934-4052 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON

/Mark W. Sincell/
Mark W. Sincell
Reg. No. 52,226
10333 Richmond Dr., Suite 1100
Houston, Texas 77042
(713) 934-4052
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

Date: December 28, 2012

Electronic Acknowledgement Receipt

EFS ID:	14576172
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	Mark William Sincell/Kathryn Danas
Filer Authorized By:	Mark William Sincell
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	28-DEC-2012
Filing Date:	19-JAN-2009
Time Stamp:	12:36:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	RespNFOA_101012.pdf	120728 065aee99233a696528903bf5f73ef5a71d3f0473	no	11

Warnings:	
Information:	

Total Files Size (in bytes):	120728

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/355,900	01/19/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 12/28/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $ =		OR	X $62=	0
Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 0	X $ =		OR	X $250=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/FELICIA R. FARMER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

10742 7590 03/12/2013

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

EXAMINER
ABBASZADEH, JAWEED A

ART UNIT	PAPER NUMBER
2115	

DATE MAILED: 03/12/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

TITLE OF INVENTION: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	06/12/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

10742 7590 03/12/2013

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

TITLE OF INVENTION: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	06/12/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABBASZADEH, JAWEED A	2115	713-002000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

10742 7590 03/12/2013

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

EXAMINER	
ABBASZADEH, JAWEED A	
ART UNIT	PAPER NUMBER
2115	

DATE MAILED: 03/12/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 575 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 575 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	12/355,900	GRELL ET AL.	
	Examiner	Art Unit	
	JAWEED A. ABBASZADEH	2115	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 12/28/2012*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-21*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JAWEED A ABBASZADEH/
Primary Examiner, Art Unit 2115

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	**Art Unit**
	JAWEED A ABBASZADEH	2115

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/10/2011	03/18/2012	10/05/2012	03/08/2013					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
3	3	✓	✓	✓	=					
4	4	✓	✓	✓	=					
5	5	✓	✓	✓	=					
6	6	✓	✓	O	=					
7	7	O	✓	=	=					
8	8	O	✓	=	=					
9	9	O	✓	=	=					
10	10	O	✓	=	=					
11	11	O	✓	=	=					
12	12	O	✓	=	=					
13	13	=	=	=	=					
14	14	=	=	=	=					
15	15	=	=	=	=					
16	16	=	=	=	=					
17	17	=	=	=	=					
18	18	=	=	=	=					
19	19	✓	✓	✓	=					
20	20	✓	✓	✓	=					
21	21	✓	✓	✓	=					

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	Art Unit
	JAWEED A ABBASZADEH	2115

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	1, 2	10/10/2011	JA
713	176	10/10/2011	JA
713	189	3/8/2013	JA

SEARCH NOTES		
Search Notes	Date	Examiner
Performed EAST search, see results attached	8/29/2011	JA
Updated EAST search, see results attached	3/13/2012	JA
Performed Google Patents search, see results attached	3/13/2012	JA
Updated EAST search, see results attached	10/1/2012	JA
Updated EAST search, US PG Pub, see results attached	3/8/2013	JA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
713	1,2,176,189	3/8/2013	JA

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33	(symmetric adj key) with boot$3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:38
L2	147	sign$3 near3 (BOOT ADJ (DATA OR CODE))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:39
L3	707	tpm same signature	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:39
L4	19	3.ab.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:39
L5	147	sign$3 near3 (boot adj (data or code))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:40
L6	234	(key near2 within near3 (processor or cpu))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:42
L7	1020	tpm with (processor or cpu)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:43
L8	42	7.ab.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 13:43
L12	4152	(713/189).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/08 14:19
L14	32470	(key near4 ($5processor or cpu)) and "12"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/03/08 14:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	14086	(713/1,2,176).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/03/08 14:03
L10	738	(key near4 ($5processor or cpu)) and 9	US-PGPUB; USPAT; UPAD	OR	ON	2013/03/08 14:04
L11	314	(key near4 ($5processor or cpu)) same (encrypt$3 or decrypt$3) and 9	US-PGPUB; USPAT; UPAD	OR	ON	2013/03/08 14:05
L15	4160	(713/189).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/03/08 14:29
L16	685	(key near4 ($5processor or cpu)) and 15	US-PGPUB; USPAT; UPAD	OR	ON	2013/03/08 14:29

3/ 8/ 2013 2:33:27 PM
C:\ Users\ jabbaszadeh\ Documents\ CASES\ 12355900\ amend2.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	**Art Unit**
	JAWEED A ABBASZADEH	2115

CPC				
Symbol			**Type**	**Version**
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			
	/			

CPC Combination Sets						
Symbol			**Type**	**Set**	**Ranking**	**Version**
	/					
	/					

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
713	2

CROSS REFERENCE(S)					
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
713	1	176	189		

INTERNATIONAL CLASSIFICATION									
CLAIMED					**NON-CLAIMED**				
G	0	6	F	9 / 00 (2006.0)					
G	0	6	F	15 / 177 (2006.01.01)					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 21	
/JAWEED A ABBASZADEH/ Primary Examiner.Art Unit 2115 3/8/2013 (Primary Examiner) (Date)	O.G. Print Claim(s) 19	O.G. Print Figure 1b

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	**Art Unit**
	JAWEED A ABBASZADEH	2115

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/JAWEED A ABBASZADEH/ Primary Examiner.Art Unit 2115	3/8/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	19	1b

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12355900	GRELL ET AL.
	Examiner	**Art Unit**
	JAWEED A ABBASZADEH	2115

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 21	
/JAWEED A ABBASZADEH/ Primary Examiner.Art Unit 2115 (Primary Examiner)	3/8/2013 (Date)	O.G. Print Claim(s) 19	O.G. Print Figure 1b

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

10742 7590 03/12/2013
GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892	7735

TITLE OF INVENTION: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	06/12/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABBASZADEH, JAWEED A	2115	713-002000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Williams, Morgan &
2 Amerson, P.C.
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: GLOBALFOUNDRIES Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Grand Cayman, Cayman Islands

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 500786 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /J. Mike Amerson/ Date May 10, 2013

Typed or printed name J. Mike Amerson Registration No. 35,426

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	12355900
Filing Date:	19-Jan-2009
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Filer:	J. Mike Amerson/Mary Paul
Attorney Docket Number:	2162.162700/DE0892

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	1780	1780
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2080**

Electronic Acknowledgement Receipt

EFS ID:	15743008
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	J. Mike Amerson/Mary Paul
Filer Authorized By:	J. Mike Amerson
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	10-MAY-2013
Filing Date:	19-JAN-2009
Time Stamp:	12:09:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2080
RAM confirmation Number	8881
Deposit Account	500786
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Issue_fee_transmittal.pdf	111018 7482cdab086df7d499d8bc86488703c6cb5ed5a4	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32294 57c571992d86c2e8ae24da682e6c1d9d0929c4c5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	143312		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12355900
Filing Date	2009-01-19
First Named Inventor	Michael Grell
Art Unit	2115
Examiner Name	Jaweed A. Abbaszadeh
Attorney Docket Number	2162.162700/DE0892

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
Change(s) applied to document, /J.L./ 4/8/2013	1	20010007131	A1	~~2001-05-01~~	Galasso et al.	July 5, 2001
	2	20050076226	A1	2005-04-07	Boivie et al.	
	3	20070192610	A1	2007-08-16	Chun et al.	
	4	20060112266	A1	2006-05-25	Little et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/355,900	06/11/2013	8464037	2162.162700/DE0892	7735

10742 7590 05/22/2013

GLOBALFOUNDRIES INC.
c/o Williams, Morgan & Amerson
10333 Richmond , Suite 1100
Houston, TX 77042

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 1084 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Michael Grell, Dresden, GERMANY;
Ralf Findeisen, Dresden, GERMANY;
Frank Schuecke, Dresden, GERMANY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	12/355,900
Filing Date	2009-01-19
First Named Inventor	Michael Grell, et al.
Title	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
Art Unit	2115
Examiner Name	Abbaszadeh, Jaweed A.
Attorney Docket Number	251367-9018

SIGNATURE of Applicant or Patent Practitioner

Signature	/Daniel R. McClure/	Date (Optional)	April 16, 2020
Name	Daniel R. McClure	Registration Number	38,962
Title (if Applicant is a juristic entity)	Attorney of Record		
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 3 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/47 (03-09)
Approved for use through 03/31/2012. OMB 0651-0016
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

"FEE ADDRESS" INDICATION FORM

Address to:
Mail Stop M Correspondence
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

- OR -

Fax to:
571-273-6500

INSTRUCTIONS: The issue fee must have been paid for application(s) listed on this form. In addition, only an address represented by a Customer Number can be established as the fee address for maintenance fee purposes (hereafter, fee address). A fee address should be established when correspondence related to maintenance fees should be mailed to a different address than the correspondence address for the application. **When to check the first box below**: If you have a Customer Number to represent the fee address. **When to check the second box below**: If you have no Customer Number representing the desired fee address, in which case a completed Request for Customer Number (PTO/SB/125) must be attached to this form. For more information on Customer Numbers, see the Manual of Patent Examining Procedure (MPEP) § 403.

For the following listed application(s), please recognize as the "Fee Address" under the provisions of 37 CFR 1.363 the address associated with:

☑ Customer Number: 109673

OR

☐ The attached Request for Customer Number (PTO/SB/125) form.

PATENT NUMBER (if known)	APPLICATION NUMBER
8,464,037	12/355,900

Completed by (check one):

☐ Applicant/Inventor — /Daniel R. McClure/ (Signature)

☑ Attorney or Agent of record 38,962 (Reg. No.) — Daniel R. McClure (Typed or printed name)

☐ Assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96) — (678) 483-8899 (Requester's telephone number)

☐ Assignee recorded at Reel _____ Frame_____ — April 16, 2020 (Date)

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more that one signature is required, see below*.

☐ * Total of _____forms are submitted.

This collection of information is required by 37 CFR 1.363. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1. 11 and 1.14. This collection is estimated to take 5 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313- 1450. DO NOT SEND COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Mail Stop M Correspondence, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	39288096
Application Number:	12355900
International Application Number:	
Confirmation Number:	7735
Title of Invention:	COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION
First Named Inventor/Applicant Name:	Michael Grell
Customer Number:	10742
Filer:	Daniel R. McClure/Brooke French
Filer Authorized By:	Daniel R. McClure
Attorney Docket Number:	2162.162700/DE0892
Receipt Date:	28-APR-2020
Filing Date:	19-JAN-2009
Time Stamp:	14:39:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	00779646.PDF	191914 d148776aba0a141617806128ca474748caae9fe3	no	1

Warnings:

Information:					
2	Power of Attorney	00779647.PDF	700137 3221553e96c19aff4e3740ceae47c4c81dde2a3f	no	1
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	00779648.PDF	122719 c5e56788525e7b0c191d04540fbb8dc55fe466ff	no	3
Warnings:					
Information:					
4	Maintenance Fee Address Change	00782815.PDF	315319 5c396da06ced7c692cb6482efd9dd21e0a455c47	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1330089	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/80 (11-08)
Approved for use through 11/30/2020. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 109673

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 109673

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

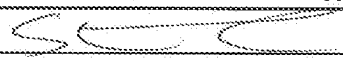
Assignee Name and Address:

MEDIATEK INC.
No. 1, Dusing 1st Rd., Hsinchu Science Park
Hsinchu City 30078, Taiwan

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	2019 Oct 2
Name	Steven-YH LIU	Telephone	
Title	Director of Intellectual Property Div. of MediaTek Inc.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: MEDIATEK INC.

Application No./Patent No.: 8,464,037 Filed/Issue Date: 2013-06-11

Titled: COMPUTER SYSTEM COMPRISING A SECURE BOOT MECHANISM ON THE BASIS OF SYMMETRIC KEY ENCRYPTION

MEDIATEK INC., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Inventors To: ADVANCED MICRO DEVICES, INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 022124, Frame 0289, or for which a copy thereof is attached.

2. From: ADVANCED MICRO DEVICES, INC. To: GLOBALFOUNDRIES INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 023120, Frame 0426, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: GLOBALFOUNDRIES INC. To: MEDIATEK INC.

The document was recorded in the United States Patent and Trademark Office at
Reel 052386, Frame 0639, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Daniel R. McClure/	April 16, 2020
Signature	Date
Daniel R. McClure	38,962
Printed or Typed Name	Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/355,900	01/19/2009	Michael Grell	2162.162700/DE0892

CONFIRMATION NO. 7735

POWER OF ATTORNEY NOTICE

10742
GLOBALFOUNDRIES INC.
c/o Amerson Law Firm, PLLC
2450 Fondren Road, Suite 260
Houston, TX 77063

OC000000116625044

Date Mailed: 05/05/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/28/2020.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ttran/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/355,900	01/19/2009	Michael Grell	251367-9018

CONFIRMATION NO. 7735

POA ACCEPTANCE LETTER

109673
McClure, Qualey & Rodack, LLP
280 Interstate North Circle SE
Suite 550
Atlanta, GA 30339

OC000000116625125

Date Mailed: 05/05/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/28/2020.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ttran/

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Central District of California on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-4969	6/17/2021	Central District of California

PLAINTIFF	DEFENDANT
MediaTek Inc. and MediaTek USA Inc.	NXP Semiconductors N.V., NXP USA, Inc., Avnet, Inc., Arrow Electronics, Inc., Denso Ten Limited, Denso Ten America Limited, Robert Bosch GmbH, Robert Bosch LLC, Continental AG, and Continental Automotive GmbH

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,738,845	5/18/2004	MediaTek Inc.
2	6,823,451	11/23/2004	MediaTek Inc.
3	8,464,037	6/11/2013	MediaTek Inc.
4	9,265,056	2/16/2016	MediaTek Inc.
5	9,538,531	1/3/2017	MediaTek Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☑ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,211,948	2/19/2019	MediaTek Inc.
2			
3			
4			
5			

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy