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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2009 (23.07.2009)

PCT

(10) International Publication Number
WO 2009/090505 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2008/050197

(22) International Filing Date: 20 January 2008 (20.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; One London Road, Staines, Middlesex TW18 4EX (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ELBAUM, Reuven** [IL/IL]; 7 Got-levin Street, 32922 Haifa (IL). **SUMNER, Reuben** [IL/IL]; 8 Egoz Street Apartment 3, 76223 Rechovot (IL).

(74) Agent: **ZVIEL, David**; Director - Intellectual Property, NDS Technologies Israel Limited, 5 Shlomo Halevi Street, 97770 Jerusalem (IL).

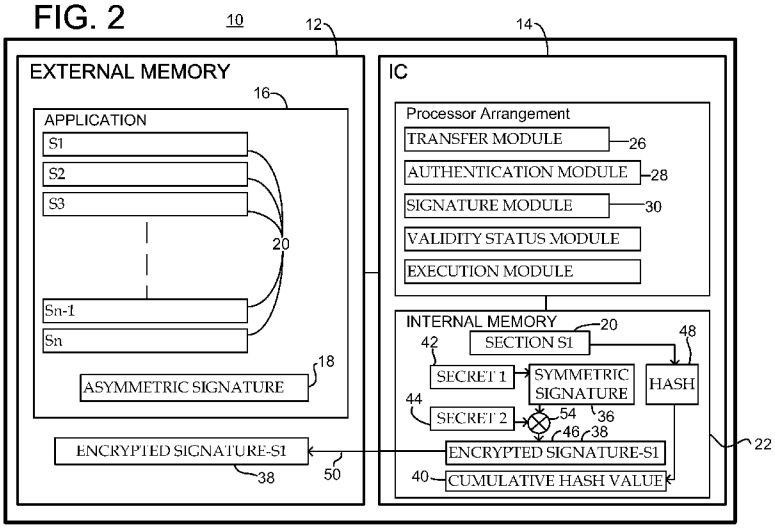
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: SECURE DATA UTILIZATION

FIG. 2



(57) Abstract: A system, comprising an external memory operative to store data therein, the data including a plurality of sections, each of the sections being associated with a signature, and an internal memory operationally connected to the external memory, and a processor arrangement operationally connected to the internal memory, the processor arrangement including a transfer module to transfer one section from the external to the internal memory, an authentication module to authenticate the signature of the section transferred from the external memory, a validity status module to identify the section as valid if the signature is authentic, and an execution module to utilize the section of the data only if the section is valid, wherein the validity status module is operative to invalidate the section, if the content of the section is changed while stored in the internal memory. Related apparatus and methods are also described.

WO 2009/090505 A1

SECURE DATA UTILIZATION

FIELD OF THE INVENTION

The present invention relates to secure data utilization.

BACKGROUND OF THE INVENTION

The following references are believed to represent the state of the art:

US Patent 7,103,779 to Kiehtreiber, at al.;

US Published Patent Application 2003/0188173 of Zimmer, et al.;

US Published Patent Application 2007/0198851 of Goto; and

Secure Video Processor IC Manufacture License Agreement, 16 May 2007.

The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved secure data utilization.

There is thus provided in accordance with a preferred embodiment of the present invention, a system including an external memory operative to store data therein, the data including a plurality of sections, each of the sections being associated with a signature, and an internal memory operationally connected to the external memory, and a processor arrangement operationally connected to the internal memory, wherein the processor arrangement includes a transfer module to transfer one of the sections from the external memory to the internal memory, an authentication module to authenticate the signature of the one section transferred from the external memory, a validity status module to identify the one section as valid if the signature is authentic, and an execution module to utilize the one section of the data only if the one section is valid, wherein the validity status module is operative to invalidate the one section, if the content of the one section is changed while stored in the internal memory.

Further in accordance with a preferred embodiment of the present invention, the system includes an integrated circuit having disposed thereon the internal memory and the processor arrangement, the integrated circuit being operationally connected to the external memory, the external memory not being on the integrated circuit.

Still further in accordance with a preferred embodiment of the present invention the data includes an executable computer program, and the execution module is operative to execute the one section of the executable computer program only if the one section is valid.

There is also provided in accordance with still another preferred embodiment of the present invention a system, including an external memory operative to store data therein, the data including a plurality of sections, at least part of the data being signed with a primary signature, the at least part of the data including at least some of the sections, and an internal memory operationally

connected to the external memory, and a processor arrangement operationally connected to the internal memory, the processor arrangement includes a transfer module, an authentication module, and a signature module, wherein during a preliminary procedure the transfer module is operative to transfer the sections from the external memory to the internal memory, the authentication module is operative to authenticate the primary signature, and the signature module is operative to create a symmetric signature for each of the sections based on a first secret, and wherein, prior to utilizing a selected one of the sections of the data the transfer module is operative to transfer the selected section from the external memory to the internal memory, and the authentication module is operative to authenticate the symmetric signature of the selected section using the first secret.

Additionally in accordance with a preferred embodiment of the present invention the transfer module is operative to transfer the at least some sections from the external memory to the internal memory only once during the preliminary procedure, so that while a cached one of the sections is in the internal memory the authentication module is operative to update a value for use in authenticating the primary signature based on the cached section, and the signature module is operative to create the symmetric signature for the cached section, and the authentication module is operative to authenticate the primary signature based on the value which has been updated based the at least some sections.

Moreover in accordance with a preferred embodiment of the present invention the authentication module is operative to calculate a hash based on the content of the cached section, and update the value based on the hash of the cached section.

Further in accordance with a preferred embodiment of the present invention the signature module is operative to encrypt the symmetric signature of the cached section using a second secret, yielding a result.

Still further in accordance with a preferred embodiment of the present invention the signature module is operative to output the result of the encryption for each of the sections to the external memory.

Additionally in accordance with a preferred embodiment of the present invention the signature module is operative to output the second secret to the external memory, only after the primary signature has been positively authenticated by the authentication module.

Moreover in accordance with a preferred embodiment of the present invention, the system includes an integrated circuit having disposed thereon the internal memory and the processor arrangement, the integrated circuit being operationally connected to the external memory, the external memory not being on the integrated circuit.

Further in accordance with a preferred embodiment of the present invention the primary signature is an asymmetric signature.

Still further in accordance with a preferred embodiment of the present invention the asymmetric signature is an RSA signature.

Additionally in accordance with a preferred embodiment of the present invention the data includes an executable computer program.

There is also provided in accordance with still another preferred embodiment of the present invention a method, including transferring a section of data from an external memory to an internal memory, authenticating a signature of the section, identifying the section as valid if the signature is authentic, utilizing the section only if the section is valid, and invalidating the section, if the content of the section is changed while stored in the internal memory.

There is also provided in accordance with still another preferred embodiment of the present invention a method, including performing a preliminary procedure including transferring a plurality of sections of data from an external memory to an internal memory, authenticating a primary signature of the at least part of the data, the at least part of the data including at least some of the sections, and creating a symmetric signature for each of the sections based on a first secret, and performing an authentication procedure for a selected one of the sections of the data, prior to utilizing the selected section, the authentication procedure including transferring the selected section from the external memory to

the internal memory, and authenticating the symmetric signature of the selected section using the first secret.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a block diagram view of a secure data utilization system constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a block diagram view of the system of Fig. 1 creating a symmetric signature;

Fig. 3 is a block diagram view of the system of Fig. 1 authenticating an asymmetric signature;

Fig. 4 is a block diagram view showing outputting of a second secret from an internal memory to an external memory of the system of Fig. 1;

Fig. 5 is a block diagram view of the system of Fig. 1 authenticating a symmetric signature of a section of an application; and

Fig. 6 is a block diagram view of the system of Fig. 1 invalidating the section of the application of Fig. 5 after the section is modified.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1, which is a block diagram view of a secure data utilization system 10 constructed and operative in accordance with a preferred embodiment of the present invention.

The system 10 preferably includes an integrated circuit (IC) 14 and an external memory 12.

The external memory 12 is preferably operative to store an application 16 therein.

Persons skilled in the art will appreciate that, throughout the present patent application, the application 16 is used by way of example of data in the form of an executable computer program, and that the present invention is not limited to a particular type of data, but rather includes any suitable data. The term "data", as used in the specification and claims, is defined herein to include an executable computer program.

The application 16 may include an executable computer program and non-executable data.

Persons skilled in the art will appreciate that, throughout the present patent application, execution of the application 16 is used by way of example only, and that the present invention is not limited to a particular type of utilization of data, but rather includes any suitable utilization of data. The term "utilization" as used in the specification and claims, is defined herein to include execution.

The application 16 is typically signed with a primary signature, such as an asymmetric signature 18, typically using an RSA signature algorithm. It will be appreciated by those ordinarily skilled in the art that the application 16 may be signed by any suitable signature method and not just with an asymmetric signature method, for example, the primary signature may be a hash of the application 16, the hash being held by the integrated circuit (IC) 14 for use in authenticating the application 16.

The application 16 typically has a plurality of sections 20. The asymmetric signature 18 is used to authenticate at least part of, and preferably the whole, application 16. Therefore, at least part of the application 16 (typically including at least two of the sections 20), and preferably the whole application 16, is signed by the primary signature.

In accordance with an alternative preferred embodiment of the present invention, the application 16 may be signed by two or more primary signatures. Each primary signature typically signs two or more sections 20 of the application 16. The sections 20 signed by one primary signature may, or may not, overlap the sections 20 of another primary signature(s).

The integrated circuit 14 typically has disposed thereon an internal memory 22 and a processor arrangement 24. The internal memory 22 is preferably operationally connected to the external memory 12 and the processor arrangement 24. The internal memory 22 generally includes a plurality of caches (not shown) for use by the processor arrangement 24 during validation and execution of the application 16.

The processor arrangement 24 may be embodied as a central processor unit (CPU) or the processor arrangement 24 may include a plurality of processing modules with or without an additional CPU. The integrated circuit 14 is preferably operationally connected to the external memory 12. The external memory 12 is not on the integrated circuit 14.

Typically, the internal memory 22, which is located on the integrated circuit 14, is generally accessed via a well defined interface. Therefore, the internal memory 22 is generally more trusted than the external memory 12 which is located off of the integrated circuit 14. Data located externally to the integrated circuit 14 is more likely to be manipulated in a malicious way than data located in the internal memory 22. Therefore, for security reasons it is desirable for the application 16 to be loaded into the internal memory 22 and authenticated and only then run from the internal memory 22.

In accordance with an alternative preferred embodiment of the present invention, the processor arrangement 24 and the internal memory 22 may

be implemented in a multi-chip module which includes a plurality of integrated circuits. The processor arrangement 24 and the internal memory 22 may be implemented in the same integrated circuit within the multi-chip module. The external memory 22 may be located on another integrated circuit within the multi-chip module or externally to the multi-chip module.

In accordance with yet another alternative preferred embodiment of the present invention, the processor arrangement 24 and the internal memory 22 may be implemented in a multi-chip module with the processor arrangement 24 and the internal memory 22 being implemented on different integrated circuits within the multi-chip module. The external memory 22 is typically located externally to the multi-chip module. It will be appreciated that if the application 16 is large enough, the whole application 16 cannot generally be loaded into the internal memory 22 at one time. Therefore, one or more of the sections 20 of the application 16 are typically loaded into the internal memory 22 by the processor arrangement 24, as necessary, depending on which of the sections 20 are needed for the execution.

If the application 16 is only authenticated on initialization, or once prior to execution, one or more of the sections 20 located in the external memory 12 may be altered (or otherwise tampered with) prior to, or during, execution of the application 16.

Symmetric signatures are generally small and fast to process, but key handling with symmetric signatures is more difficult. Asymmetric signatures, on the other hand, are typically slower to process and the signatures are larger, but key handling is generally easier. Therefore, the system 10 is generally operative to: authenticate the asymmetric signature 18 of the application 16 during a preliminary procedure, described in more detail with reference to Figs. 2 and 3; and assign symmetric signatures to each of the sections 20 so that when one of the sections 20 is selected for execution, the symmetric signature of the selected section 20 is validated after loading the selected section from the external memory 12 into the internal memory 22, prior to executing the selected section 20, described in more detail with reference to Figs. 2, 4 and 5.

The processor arrangement 24 preferably includes a transfer module 26, an authentication module 28, a signature module 30, a validity status module 32 and an execution module 34.

Reference is now made to Fig. 2, which is a block diagram view of the system 10 of Fig. 1 creating a symmetric signature 36.

During the preliminary procedure, each section 20 of the application 16 is preferably transferred only once from the external memory 12 to the internal memory 22 so that while a cached section 20 is in the internal memory 22, the symmetric signature 36 is preferably created for the cached section 20 and then generally encrypted forming an encrypted symmetric signature 38 for the cached section 20 and a cumulative hash value 40 is typically updated for use in authenticating the asymmetric signature 18 based on the cached section 20.

The above steps are now described in more detail below for each cached section.

The transfer module 26 is preferably operative to transfer one of the sections 20 from the external memory 12 to the internal memory 22 during the preliminary procedure. The transferred section 20 is referred to as the cached section 20, as the section 20 is cached in the internal memory 22.

The signature module 30 is preferably operative to create the symmetric signature 36 for the cached section 20 based on a first secret 42. The first secret 42 is preferably either embedded/programmed in the integrated circuit 14 during production of the integrated circuit 14 or the first secret 42 is produced by the signature module 30 using a random or pseudo-random number generator (not shown). The first secret is generally known by the integrated circuit 14 and not the external memory 12. The symmetric signature 36 is at least 1 bit long and typically 32 or more bits long. The first secret 42 is typically at least 20 bits long and preferably more than 100 bits long.

The signature module 30 is preferably operative to perform an exclusive-OR logic gate operation (circle 54) with: the symmetric signature 36 of the cached section 20; and a second secret 44 as input, yielding a result 46. The result 46 is the encrypted symmetric signature 38. The signature module 36 is

preferably operative to produce the second secret 44 using a random or pseudo-random number generator (not shown). The second secret 44 is not made "public" until the asymmetric signature 18 has been positively authenticated. The term "positively authenticated", as used in the specification and claims, is defined as "the signature is deemed valid after being checked".

Although, the symmetric signatures 36 are described above as being encrypted using an exclusive-OR operation, it will be appreciated by those ordinarily skilled in the art that the symmetric signatures 36 may be encrypted using the second secret 44 by any suitable scrambling method for example, but not limited to, addition, subtraction, encryption or decryption.

The signature module 30 is preferably operative to output the result 46 of the exclusive-OR logic gate operation for the cached section 20 to the external memory 12 (arrow 50).

The authentication module 28 is preferably operative to: calculate a hash 48 based on the content of the cached section 20; and update the cumulative hash value 40 based on the hash 48 of the cached section 20. The cumulative hash value 40 is used in authenticating the asymmetric signature 18, described in more detail with reference to Fig. 3.

Only copying the sections 20 once during the preliminary procedure to create the symmetric signatures 36 (and the encrypted symmetric signatures 38) and prepare the cumulative hash value 40 for use in authenticating the asymmetric signature 18 not only saves time but also helps prevent a security problem, as follows. If the asymmetric signature 18 is authenticated by first loading all the sections 20, one after the other, and then the symmetric signatures 36 (and the encrypted symmetric signatures 38) are created by loading the sections 20 a second time, the application 16 could be tampered with between authenticating the asymmetric signature 18 and creating the symmetric signatures 36.

As described above, the symmetric signatures 36 are preferably encrypted to form the encrypted symmetric signature 38 in order to prevent use of the symmetric signatures 36 before the asymmetric signature 18 has been positively authenticated. Once the asymmetric signature 18 has been positively

authenticated, the second secret 44 is typically outputted to the external memory 12 to enable decrypting the encrypted symmetric signatures 38, described in more detail with reference to Fig. 4.

Additionally, the application 16 may be encrypted in the external memory 12 and/or the internal memory 22 for added security.

Reference is now made to Fig. 3, which is a block diagram view of the system 10 of Fig. 1 authenticating the asymmetric signature 18.

Fig. 3 shows, the encrypted symmetric signatures 38 for the sections 20 stored in the external memory 12 as the internal memory 22 is generally too small to store all of the encrypted symmetric signatures 38.

During the preliminary procedure, the transfer module 26 generally transfers the asymmetric signature 18 to the internal memory 22. Then, the authentication module 28 is preferably operative to authenticate the asymmetric signature 18 of the application 16 based on a public key 52 and the cumulative hash value 40 which has been updated based on the hash's 40 (Fig. 2) of all the sections 20. The public key 52 may be stored in any suitably secure fashion, for example, but not limited to, in read only memory (ROM) or one-time programmable memory on the integrated circuit 14. By way of example only, in a multi-chip module the public key 52 may be stored on the same integrated circuit as the internal memory 22 (or the IC of the processor arrangement 24, if the internal memory 22 and the processor arrangement 24 are disposed on different ICs) or on another IC.

Alternatively, the public key 52 may come from an unknown non-trusted source. However, in such a case the public key is signed by a private key associated with a public key which is trusted by the system 10. The trusted public key can then be used to verify that the public key 52.

Reference is now made to Fig. 4, which is a block diagram view showing outputting the second secret 44 from the internal memory 22 to the external memory 12 of the system 10 of Fig. 1.

The signature module 30 is preferably operative to output the second secret 44 from the internal memory 22 to the external memory 12, only after the asymmetric signature 18 has been positively authenticated by the authentication module 28.

Then, the symmetric signature 36 for each of the sections 20 is typically recovered by decryption using the second secret 44, for example, but not limited to, performing an exclusive-OR logic gate operation (circle 56) with: the result 46 (the encrypted symmetric signature 38) of the exclusive-OR logic gate operation (circle 54 of Fig. 2) for each of the sections 20; and the second secret 44. The XOR logic gate operation (circle 56) is typically performed by the processor arrangement 24 or any other suitable processor.

The resulting recovered symmetric signatures 36 are typically either embedded in the respective section 20 or stored elsewhere in the external memory 12. However, it will be appreciated by those ordinarily skilled in the art that the symmetric signatures 36 may be stored in any suitable location.

Reference is now made to Fig. 5, which is a block diagram view of the system 10 of Fig. 1 authenticating the symmetric signature 36 of one of the sections 20 (section S3 in the example of Fig. 5) of the application 16.

Prior to executing a selected section 58 of the sections 20 of the application 16, the following is preferably performed: the transfer module 26 is operative to transfer the selected section 58 and the symmetric signature 36 of the selected section 58 from the external memory 12 to the internal memory 22; the authentication module 28 is operative to authenticate the symmetric signature 36 of the selected section 58 using the first secret 42 (oval 62); and the validity status module 32 is generally operative to identify the selected section 58 as valid if the symmetric signature 36 is authentic, typically by using a flag 60.

The execution module 34 is preferably operative to execute/utilize the selected section 58 of the application 16 cached in the internal memory 22 only if the section 58 is valid. Similarly, any other sections 20 of the application 16 cached in the internal memory 22 will only generally be executed/utilized if the relevant section 20 is valid.

Reference is now made to Fig. 6, which is a block diagram view of the system 10 of Fig. 1 invalidating the section 58 of the application 16 of Fig. 5 after the section 58 is modified.

The selected section 58 has been modified while cached in the internal memory 22 (oval 66). The validity status module 58 is preferably operative to invalidate the section 58, if the content of the section 58 is changed while stored in the internal memory 22. The invalidating preferably includes removing the flag 60 of Fig. 5 and/or flagging the section 58 as invalid with a flag 64.

Once the section 58 is no longer valid, the execution module 34 will generally no longer execute/utilize the section 58.

It is appreciated that software components of the present invention may, if desired, be implemented in hardware, using conventional techniques, or implemented partially in hardware and partially in software. A hardware implementation may be particularly advantageous for security and/or performance acceleration reasons.

It will be appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable sub-combination. It will also be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow.

What is claimed is:

CLAIMS

1. A system, comprising:

an external memory operative to store data therein, the data including a plurality of sections, each of the sections being associated with a signature; and

an internal memory operationally connected to the external memory; and

a processor arrangement operationally connected to the internal memory, wherein the processor arrangement includes:

a transfer module to transfer one of the sections from the external memory to the internal memory;

an authentication module to authenticate the signature of the one section transferred from the external memory;

a validity status module to identify the one section as valid if the signature is authentic; and

an execution module to utilize the one section of the data only if the one section is valid,

wherein the validity status module is operative to invalidate the one section, if the content of the one section is changed while stored in the internal memory.

2. The system according to claim 1, further comprising an integrated circuit having disposed thereon the internal memory and the processor arrangement, the integrated circuit being operationally connected to the external memory, the external memory not being on the integrated circuit.

3. The system according to claim 1 or claim 2, wherein: the data includes an executable computer program; and the execution module is operative to

execute the one section of the executable computer program only if the one section is valid.

4. A system, comprising:

an external memory operative to store data therein, the data including a plurality of sections, at least part of the data being signed with a primary signature, the at least part of the data including at least some of the sections; and

an internal memory operationally connected to the external memory; and

a processor arrangement operationally connected to the internal memory, the processor arrangement includes a transfer module, an authentication module, and a signature module,

wherein during a preliminary procedure:

the transfer module is operative to transfer the sections from the external memory to the internal memory;

the authentication module is operative to authenticate the primary signature; and

the signature module is operative to create a symmetric signature for each of the sections based on a first secret, and

wherein, prior to utilizing a selected one of the sections of the data:

the transfer module is operative to transfer the selected section from the external memory to the internal memory; and

the authentication module is operative to authenticate the symmetric signature of the selected section using the first secret.

5. The system according to claim 4, wherein:

the transfer module is operative to transfer the at least some sections from the external memory to the internal memory only once during the preliminary procedure, so that while a cached one of the sections is in the internal memory:

the authentication module is operative to update a value for use in authenticating the primary signature based on the cached section; and

the signature module is operative to create the symmetric signature for the cached section; and

the authentication module is operative to authenticate the primary signature based on the value which has been updated based the at least some sections.

6. The system according to claim 5, wherein the authentication module is operative to: calculate a hash based on the content of the cached section; and update the value based on the hash of the cached section.

7. The system according to any of claims 4-6, wherein the signature module is operative to encrypt the symmetric signature of the cached section using a second secret, yielding a result.

8. The system according to claim 7, wherein the signature module is operative to output the result of the encryption for each of the sections to the external memory.

9. The system according to claim 8, wherein the signature module is operative to output the second secret to the external memory, only after the primary signature has been positively authenticated by the authentication module.

10. The system according to any of claims 4-9, further comprising an integrated circuit having disposed thereon the internal memory and the processor arrangement, the integrated circuit being operationally connected to the external memory, the external memory not being on the integrated circuit.

11. The system according to any of claims 4-10, wherein the primary signature is an asymmetric signature.

12. The system according to claim 11, wherein the asymmetric signature is an RSA signature.

13. The system according to any of claims 4-12, wherein the data includes an executable computer program.

14. A method, comprising:

transferring a section of data from an external memory to an internal memory;

authenticating a signature of the section;

identifying the section as valid if the signature is authentic;

utilizing the section only if the section is valid; and

invalidating the section, if the content of the section is changed while stored in the internal memory.

15. A method, comprising:

performing a preliminary procedure including:

transferring a plurality of sections of data from an external memory to an internal memory;

authenticating a primary signature of the at least part of the data, the at least part of the data including at least some of the sections; and

creating a symmetric signature for each of the sections based on a first secret; and

performing an authentication procedure for a selected one of the sections of the data, prior to utilizing the selected section, the authentication procedure including:

transferring the selected section from the external memory to the internal memory; and

authenticating the symmetric signature of the selected section using the first secret.

FIG. 1

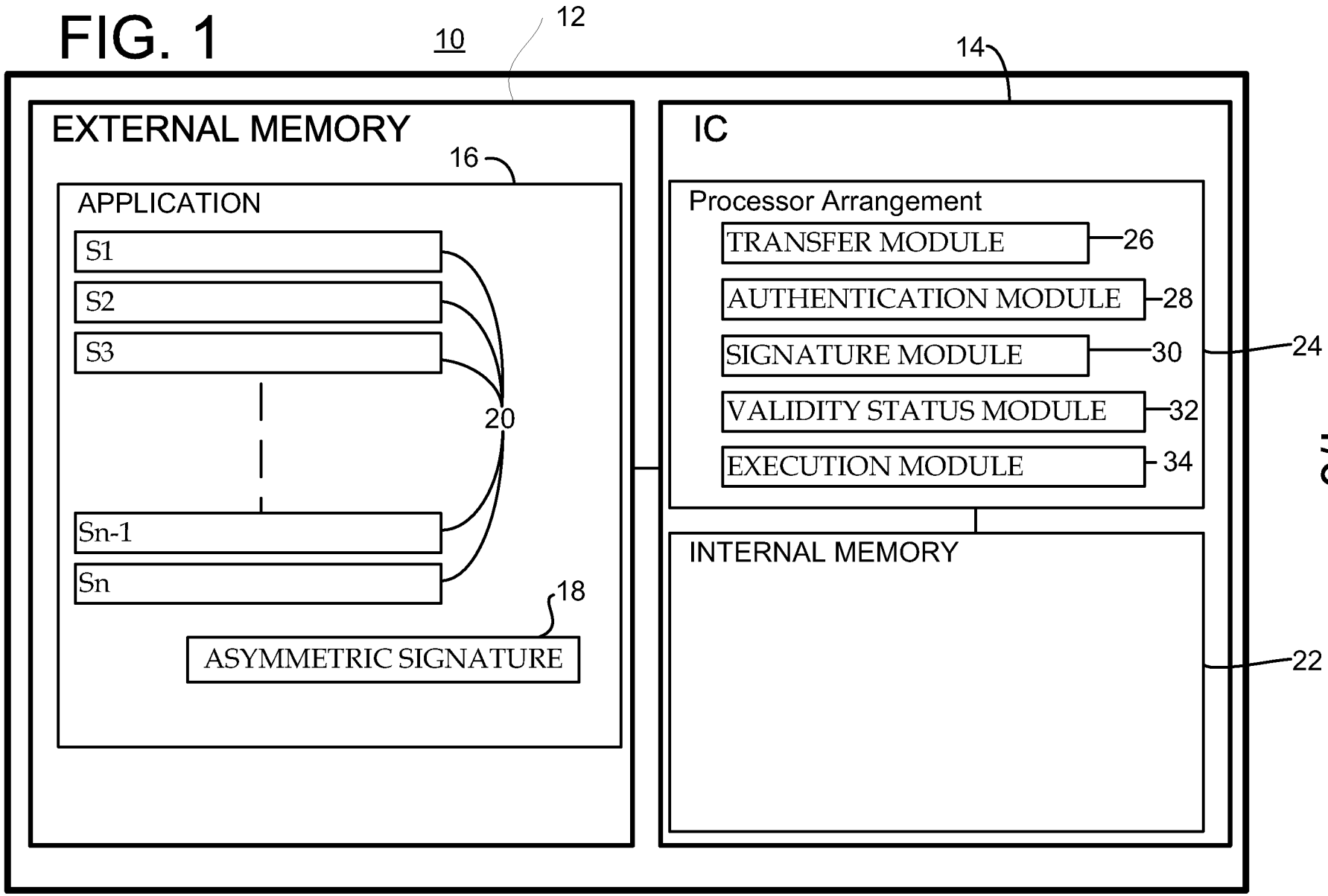

10
12
14
EXTERNAL MEMORY
16
APPLICATION
S1
S2
S3
Sn-1
Sn
20
18
ASYMMETRIC SIGNATURE
IC
Processor Arrangement
TRANSFER MODULE
26
AUTHENTICATION MODULE
28
SIGNATURE MODULE
30
VALIDITY STATUS MODULE
32
EXECUTION MODULE
34
24
INTERNAL MEMORY
22

FIG. 2

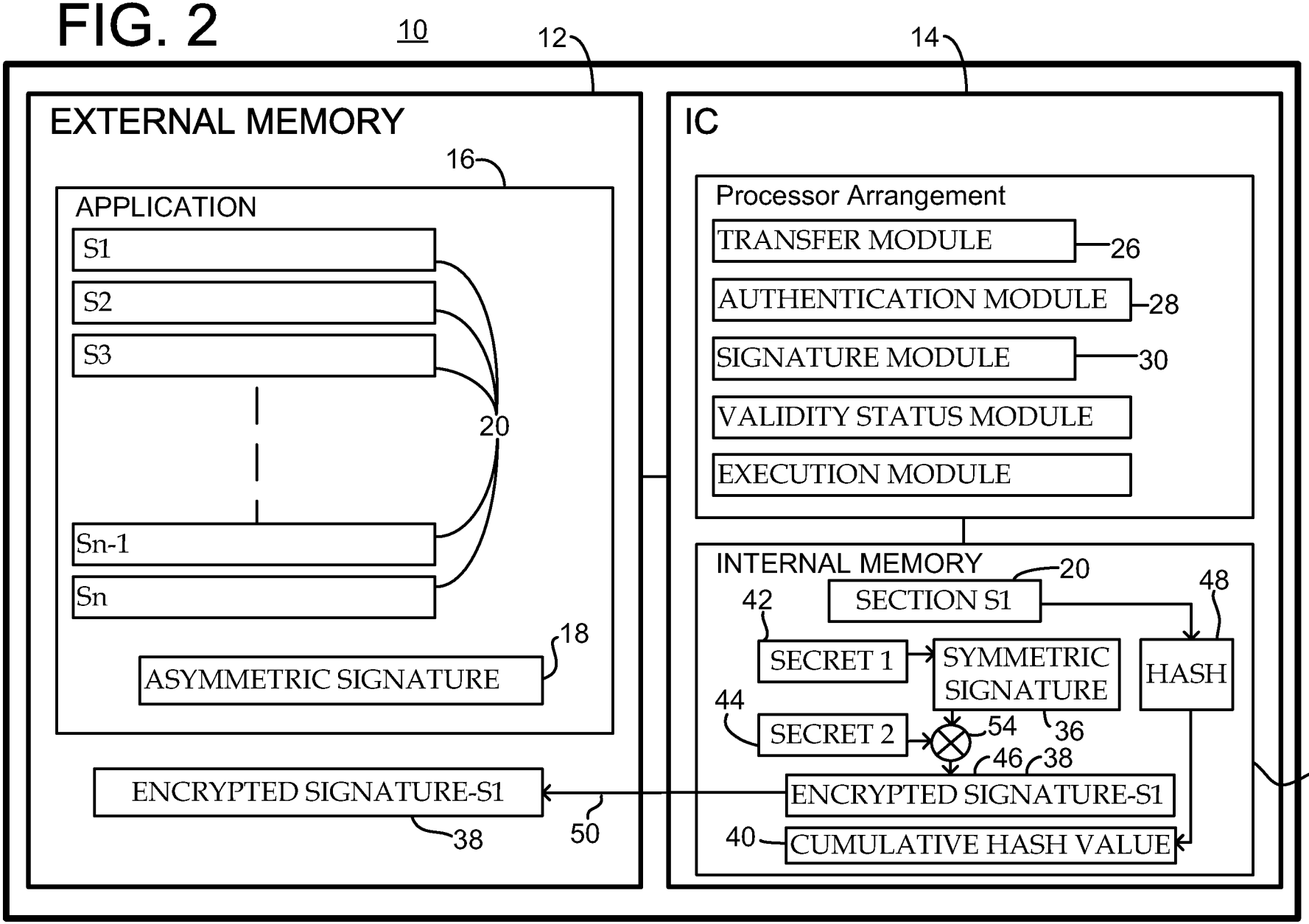

10
12
14
EXTERNAL MEMORY
16
APPLICATION
S1
S2
S3
20
Sn-1
Sn
18
ASYMMETRIC SIGNATURE
ENCRYPTED SIGNATURE-S1
38
50
IC
Processor Arrangement
TRANSFER MODULE
26
AUTHENTICATION MODULE
28
SIGNATURE MODULE
30
VALIDITY STATUS MODULE
EXECUTION MODULE
INTERNAL MEMORY
20
SECTION S1
48
42
SECRET 1
SYMMETRIC SIGNATURE
HASH
44
SECRET 2
54
36
46
38
ENCRYPTED SIGNATURE-S1
40
CUMULATIVE HASH VALUE
22

FIG. 3

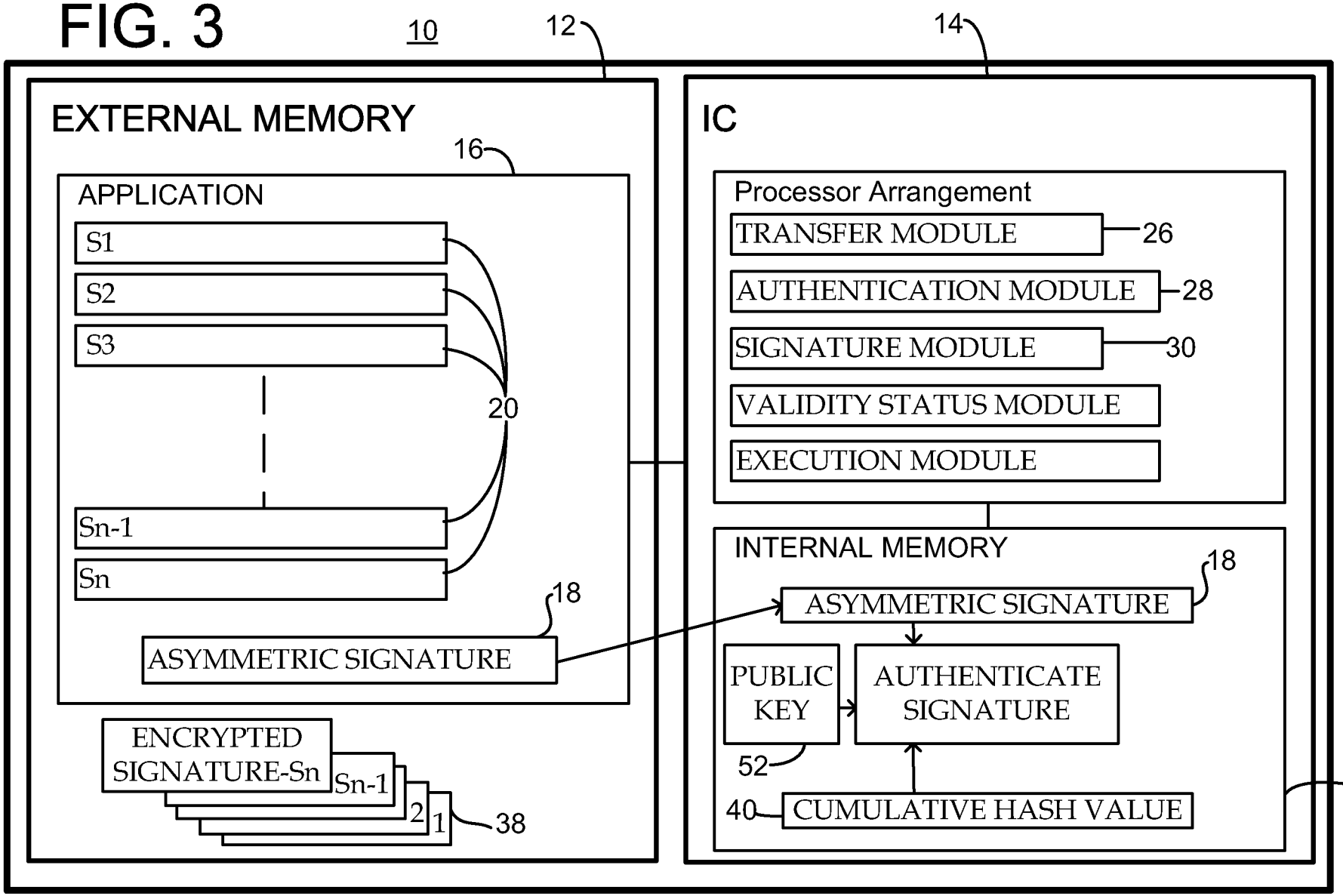

10
12
14
EXTERNAL MEMORY
16
APPLICATION
S1
S2
S3
20
Sn-1
Sn
18
ASYMMETRIC SIGNATURE
ENCRYPTED SIGNATURE-Sn
Sn-1
2
1
38
IC
Processor Arrangement
TRANSFER MODULE
26
AUTHENTICATION MODULE
28
SIGNATURE MODULE
30
VALIDITY STATUS MODULE
EXECUTION MODULE
INTERNAL MEMORY
18
ASYMMETRIC SIGNATURE
PUBLIC KEY
52
AUTHENTICATE SIGNATURE
40
CUMULATIVE HASH VALUE
22

FIG. 4

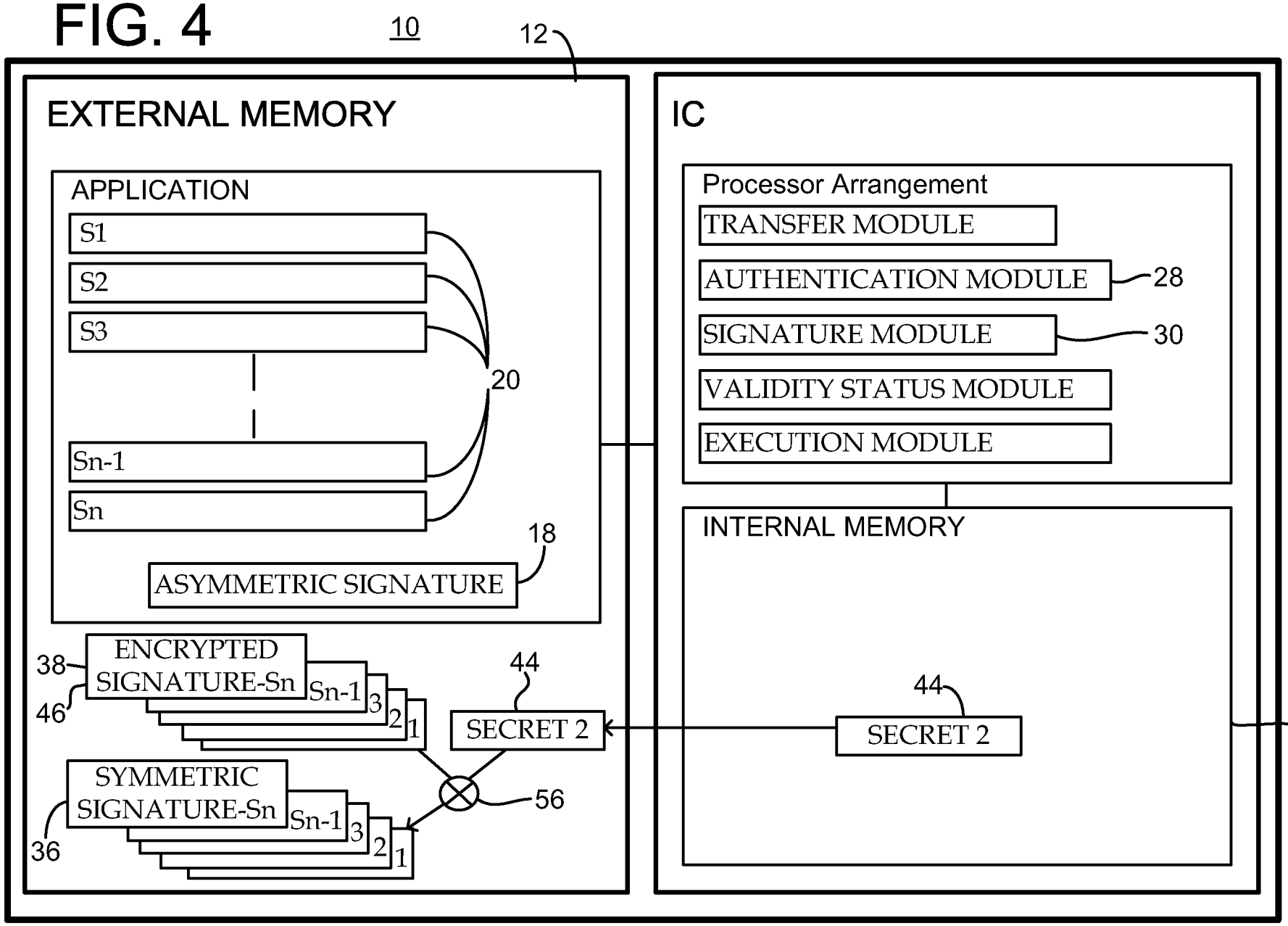

10
12
EXTERNAL MEMORY
APPLICATION
S1
S2
S3
Sn-1
Sn
20
18
ASYMMETRIC SIGNATURE
ENCRYPTED SIGNATURE-Sn
Sn-1
3
2
1
38
46
SYMMETRIC SIGNATURE-Sn
Sn-1
3
2
1
36
44
SECRET 2
56
IC
Processor Arrangement
TRANSFER MODULE
AUTHENTICATION MODULE
28
SIGNATURE MODULE
30
VALIDITY STATUS MODULE
EXECUTION MODULE
INTERNAL MEMORY
44
SECRET 2
22

FIG. 5

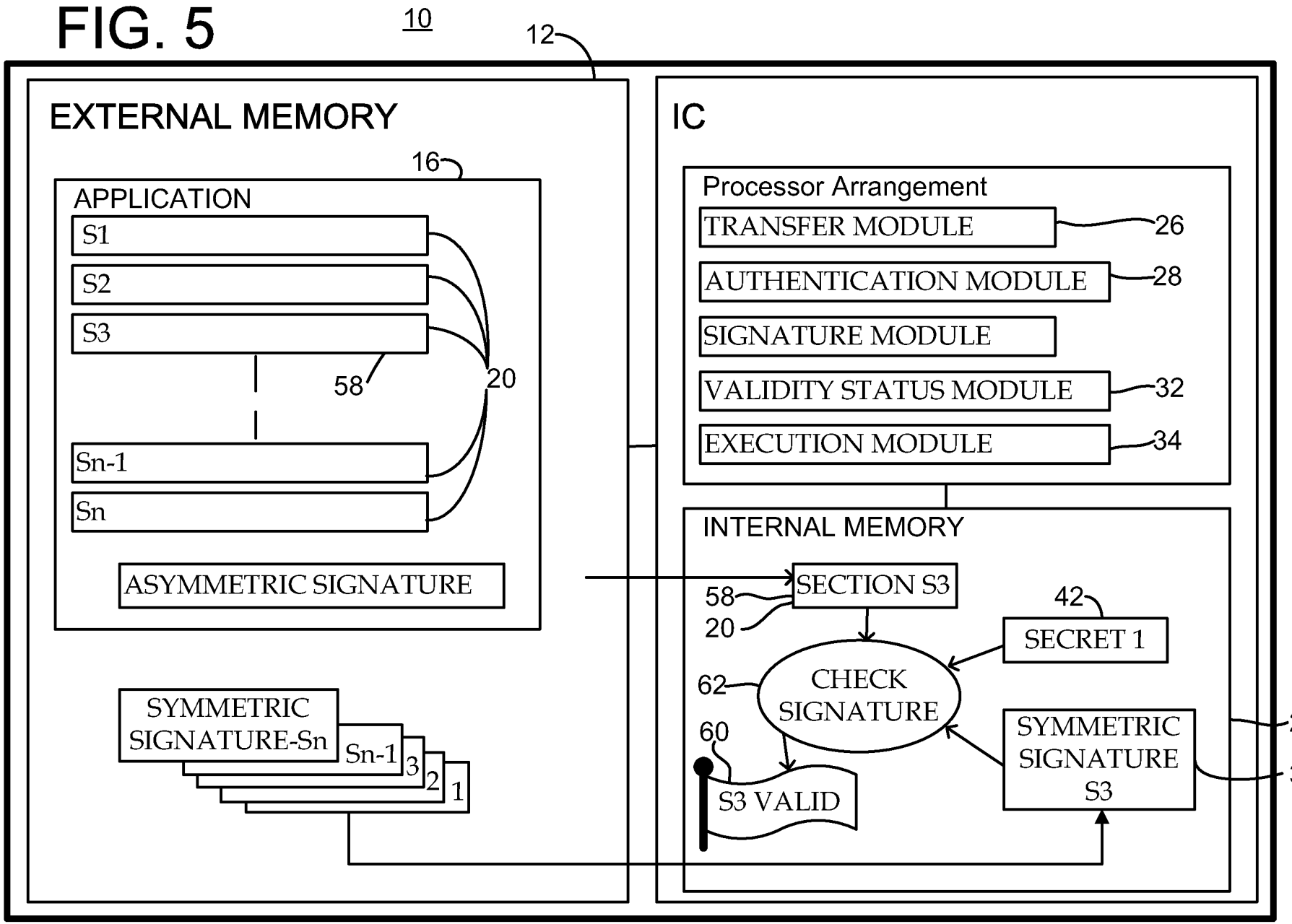
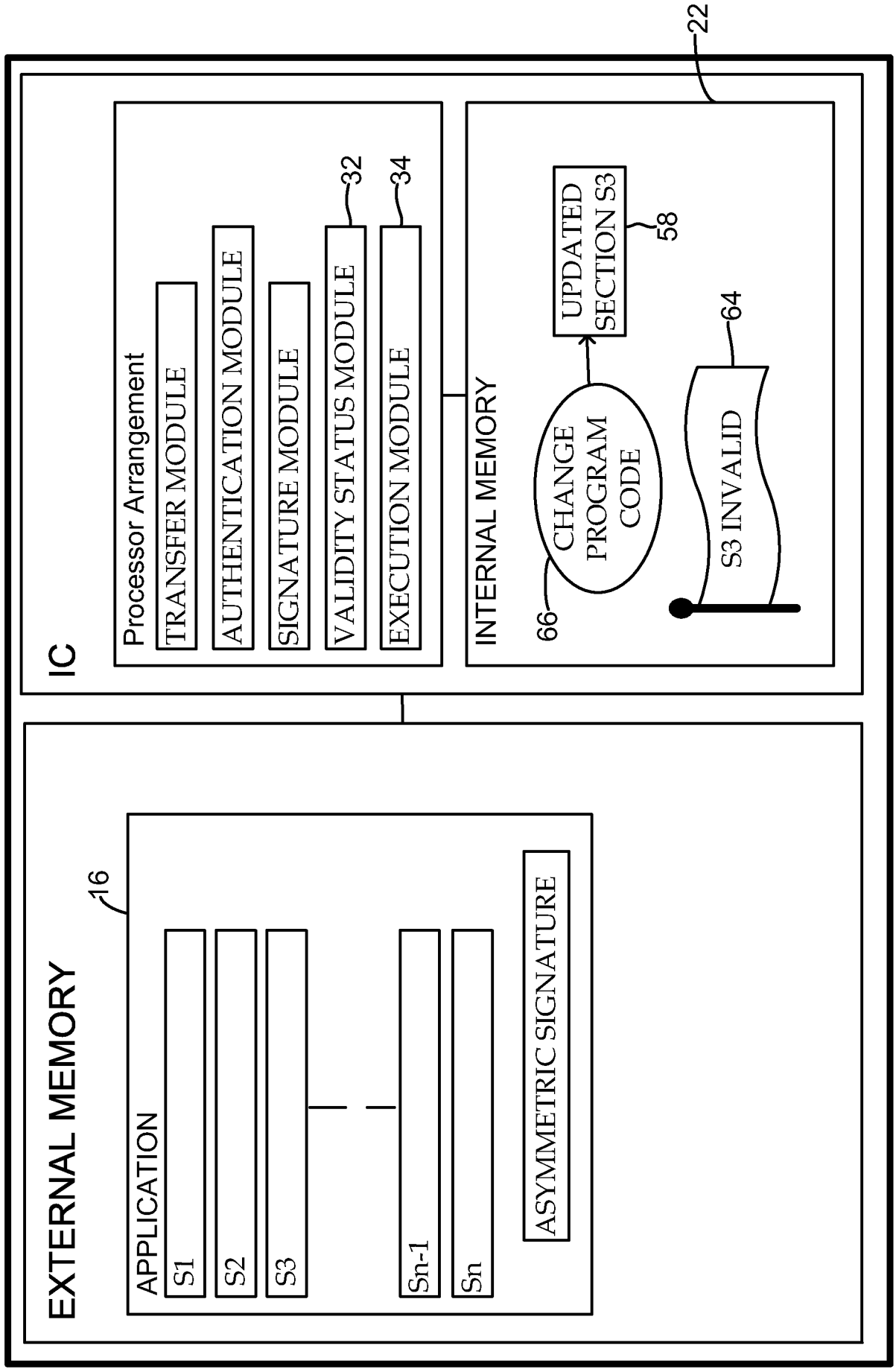

10
12
EXTERNAL MEMORY
16
APPLICATION
S1
S2
S3
58
20
Sn-1
Sn
ASYMMETRIC SIGNATURE
SYMMETRIC SIGNATURE-Sn
Sn-1
3
2
1
IC
Processor Arrangement
TRANSFER MODULE
26
AUTHENTICATION MODULE
28
SIGNATURE MODULE
VALIDITY STATUS MODULE
32
EXECUTION MODULE
34
INTERNAL MEMORY
SECTION S3
58
20
42
SECRET 1
62
CHECK SIGNATURE
60
S3 VALID
SYMMETRIC SIGNATURE S3
22
36

FIG. 6


10
EXTERNAL MEMORY
16
APPLICATION
S1
S2
S3
Sn-1
Sn
ASYMMETRIC SIGNATURE
IC
22
Processor Arrangement
TRANSFER MODULE
AUTHENTICATION MODULE
SIGNATURE MODULE
VALIDITY STATUS MODULE
32
EXECUTION MODULE
34
INTERNAL MEMORY
CHANGE PROGRAM CODE
66
UPDATED SECTION S3
58
S3 INVALID
64

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/050197

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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.
X	US 2003/126454 A1 (GLEW ANDREW F [US] ET AL) 3 July 2003 (2003-07-03) abstract claims 1-34; figures 1-8 paragraphs [0014] - [0081]	1-15
A	US 2003/196096 A1 (SUTTON JAMES A [US]) 16 October 2003 (2003-10-16) abstract paragraphs [0010] - [0039]	1-15
A	US 2006/090084 A1 (BUER MARK [US]) 27 April 2006 (2006-04-27) abstract paragraphs [0010] - [0021]	1-15

☐ 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
2 December 2008	12/12/2008

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	Kleiber, Michael

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/050197

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003126454 A1	03-07-2003	AU 2002364106 A1	24-07-2003
		CN 1608234 A	20-04-2005
		EP 1502168 A2	02-02-2005
		JP 2006507548 T	02-03-2006
		KR 20060120291 A	24-11-2006
		WO 03058412 A2	17-07-2003
US 2003196096 A1	16-10-2003	AU 2003224803 A1	27-10-2003
		CN 1659494 A	24-08-2005
		DE 10392528 T5	15-09-2005
		GB 2403047 A	22-12-2004
		GB 2419990 A	10-05-2006
		HK 1068423 A1	21-07-2006
		WO 03088019 A2	23-10-2003
US 2006090084 A1	27-04-2006	NONE	