

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
5 February 2009 (05.02.2009)

PCT

(10) International Publication Number
WO 2009/018481 A1

(51) International Patent Classification:
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/US2008/071821

(22) International Filing Date: 31 July 2008 (31.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/962,821 31 July 2007 (31.07.2007) US
60/962,822 31 July 2007 (31.07.2007) US
60/962,848 31 July 2007 (31.07.2007) US
61/026,438 5 February 2008 (05.02.2008) US

(71) Applicant (for all designated States except US): **VIASAT, INC.** [US/US]; 6155 El Camino Real, Carlsbad, California 92009 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **OWENS, John, R.** [US/US]; 1928 High Ridge Avenue, Carlsbad, California 92008 (US). **ANDOLINA, John, C.** [US/US]; 1981 Pinewood Road, Vista, California 92081 (US). **SHANKEN, Stuart, N.** [US/US]; 5028 Almondwood Way, San Diego, California 92130 (US). **QUINTANA, Richard, L.** [US/US]; 6482 Kite Place, Carlsbad, California 92011 (US).

(74) Agents: **FRANKLIN, Thomas D.** et al.; Townsend And Townsend And Crew Llp, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(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,

[Continued on next page]

(54) Title: MULTI-LEVEL KEY MANAGER

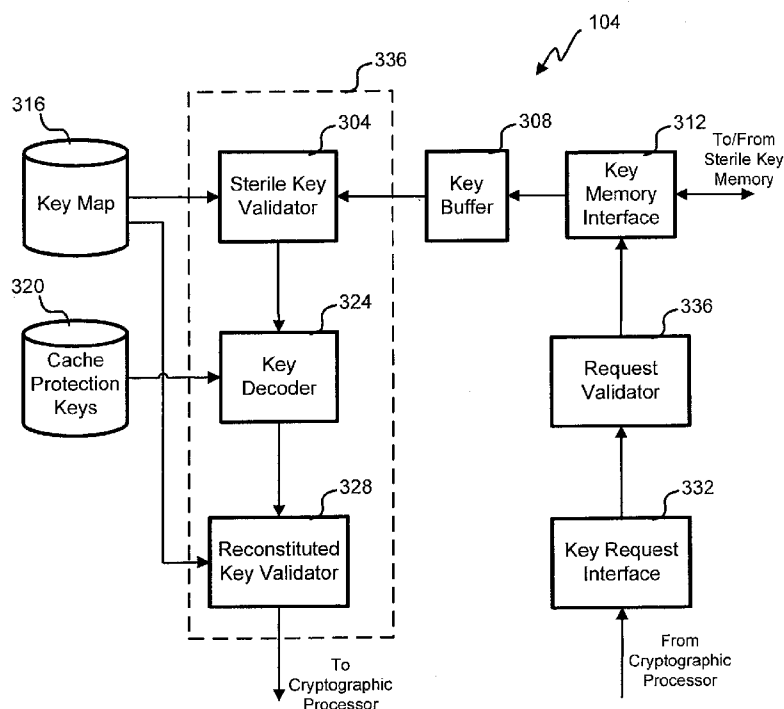


Fig. 3

(57) Abstract: A cryptographic device and method are disclosed for processing different levels of classified information. A memory caches keys for use in a cryptographic processor. The cryptographic processor requests a key associated with a particular classification level when processing a packet of the particular classification level. The cryptographic device confirms that the key and the packet are of the same classification level in a high-assurance manner. Checking header information of the keys one or more times is performed in one embodiment. Some embodiments authenticate the stored key in a high-assurance manner prior to providing the key to the cryptographic device.



RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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).

(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),

Published:

- *with international search report*
- *with amended claims*

MULTI-LEVEL KEY MANAGER

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of and is a non-provisional of co-pending: US Provisional Application Serial No. 60/962,848 filed on July 31, 2007; US Provisional
5 Application Serial No. 61/026,438 filed on February 5, 2008; US Provisional Application Serial No. 60/962,821 filed on July 31, 2007; and US Provisional Application Serial No. 60/962,822 filed on July 31, 2007; which are all hereby expressly incorporated by reference in their entirety for all purposes.

[0002] This application expressly incorporates by reference: US Application Serial No.
10 _____, filed on an even day herewith, entitled "INPUT OUTPUT ACCESS CONTROLLER" (temporarily referenced by Attorney Docket No. 017018-017210US/VS-0245); and, US Application Serial No. _____, filed on an even day herewith, entitled "TRUSTED LABELER" (temporarily referenced by Attorney Docket No. 017018-014610US/VS-0246); in their entirety for all purposes.

15 BACKGROUND

[0003] This disclosure relates in general to secure computing systems and, more specifically to high-assurance access to keys at different classification levels amongst other things.

[0004] Governments classify information at different levels generally according to their
20 sensitivity, for example, SECRET versus TOP SECRET. Users of the information are also classified by what level they are able to get access to. For example, someone with a SECRET clearance is not given access to TOP SECRET information. Procedures are put in place to avoid exposure to persons without the proper classification level.

[0005] In processing systems, physical security is used to prevent information of different
25 classification levels from bleeding over to a different classification level. To process at multiple classification levels, there may be several devices running in parallel for each classification level. Devices that may be capable of running at multiple classification levels are run at one classification level, cleared out and then run at a different classification level. Intermixing of different classified information is generally taboo in these systems.

[0006] There are situations that require smaller cryptographic devices that can process different classification levels. Switching between classification levels takes time and slows down processing. Some have proposed trusted operating systems that can process information with more flexibility, but these solutions are avoided due to a lack of trust.

- 5 [0007] Different keys are required for each classification level to maintain the security of information in each classification level. The keys may be simply different values or could be used with different algorithms. Even if security is breached for one classification level, the unique keys and algorithms can keep information protected in the other classification levels safe.

10

SUMMARY

- [0008] In an embodiment, a cryptographic device and method are disclosed for processing different levels of classified information. A memory caches keys for use in a cryptographic processor. The cryptographic processor requests a key associated with a particular classification level when processing a packet of the particular classification level. The
15 cryptographic device confirms that the key and the packet are of the same classification level in a high-assurance manner. Checking header information of the keys one or more times is performed in one embodiment. Some embodiments authenticate the stored key in a high-assurance manner prior to providing the key to the cryptographic device.

- [0009] In one embodiment, a cryptographic device for processing classified information
20 having a number of different classification levels is disclosed. The cryptographic device includes a memory, a cryptographic processor and a key manager. The memory holds a number of keys outside of an integrated circuit. The plurality of keys are for the plurality of different classification levels. The cryptographic processor is part of the integrated circuit and uses the plurality of keys to process packets of information that are categorized
25 according to the number of different classification levels. The key manager can access a plurality of rules associated with the plurality of different classification levels that regulate interaction with the plurality of keys. A first rule of the number of rules is used by the key manager in a first classification level of the number of different classification levels. A second rule of the number of rules is used by the key manager in a second classification
30 level of the number of different classification levels.

[0010] In another embodiment, a method for processing classified information in a high-assurance manner is disclosed. In one step, a request is received for a first key by a cryptographic processor. A first rule from a number of rules is applied to a first sterile key retrieved from a memory. The first sterile key is decrypted with a first protection key to
5 produce the first key. The first key is also checked with the first rule. The first key is provided to the cryptographic processor if the checking the first sterile key step and the checking the first key step are completed successfully. A request is received for a second key by the cryptographic processor. A second rule from the number of rules is applied to a second sterile key retrieved from the memory. The second sterile key is decrypted with a
10 second protection key to produce the second key. The second key is also checked with the second rule. The second key is provided to the cryptographic processor if the checking the second sterile key step and the checking the second key step are completed successfully.

[0011] In yet another embodiment, a cryptographic device for processing information with a plurality of classification levels is disclosed. The cryptographic device includes a
15 memory, a cryptographic processor and a key manager. The memory holds a number of keys that are used by a cryptographic processor to process packets of information that are correlated to the plurality of classification levels. The key manager includes a rule enforcement circuit and a key decryption circuit. The key manager retrieves a first key for a first packet being processed by the cryptographic processor. The first packet and the first
20 key are of a first classification level. The rule enforcement circuit checks that the first key is designated for the first classification level before providing the first key to the cryptographic processor for processing the first packet. The key manager retrieves a second key for a second packet being processed by the cryptographic processor. The second packet and the second key are of a second classification level. The rule enforcement circuit checks
25 that the second key is designated for the second classification level before providing the second key to the cryptographic processor for processing the second packet.

[0012] Further areas of applicability of the present disclosure will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating various embodiments, are intended for
30 purposes of illustration only and are not intended to necessarily limit the scope of the disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The present disclosure is described in conjunction with the appended figures:
FIG. 1 depicts a block diagram of an embodiment of a cryptographic device;
FIG. 2 depicts a block diagram of an embodiment of a partitioned key cache;
5 FIG. 3 depicts a block diagram of an embodiment of a key manager;
FIG. 4 depicts a diagram of an embodiment of a key unscrambling process; and
FIG. 5 illustrates a flowchart of an embodiment of a process for operating the
cryptographic device.

[0014] In the appended figures, similar components and/or features may have the same
10 reference label. Further, various components of the same type may be distinguished by
following the reference label by a dash and a second label that distinguishes among the
similar components. If only the first reference label is used in the specification, the
description is applicable to any one of the similar components having the same first
reference label irrespective of the second reference label.

15 DETAILED DESCRIPTION

[0015] The ensuing description provides preferred exemplary embodiment(s) only, and is
not intended to limit the scope, applicability or configuration of the disclosure. Rather, the
ensuing description of the preferred exemplary embodiment(s) will provide those skilled in
the art with an enabling description for implementing a preferred exemplary embodiment.
20 It being understood that various changes may be made in the function and arrangement of
elements without departing from the spirit and scope as set forth in the appended claims.

[0016] Referring first to **FIG. 1**, a block diagram of an embodiment of a cryptographic
device 100 is shown. The cryptographic device 100 processes information of different
classifications. Information in each classification level is kept separate or partitioned from
25 information of other classification levels throughout the cryptographic device 100.
Additionally, each classification level can use different cryptographic algorithms and/or
keys. Several integrated circuits could be used to implement the cryptographic device 100
where at least a cryptographic processor 120 is in one integrated circuit and the partitioned
key cache 116 is in another. Other embodiments could have the partitioned key cache 116
30 and cryptographic processor 120 as part of the same integrated circuit.

[0017] A cryptographic processor 120 is the circuit that performs encryption, decryption
and/or bypass for the information that passes through it. Information may be a stream or

packetized in cryptographic processor 120. The packets or streams are of different classification levels. The cryptographic processor 120 can reconfigure itself for the appropriate processing on a packet-by-packet basis. Different processing steps are set up for each classification level in a pipeline fashion by the cryptographic processor 120. The processing steps perform formatting and cryptographic processing with a number of different algorithms and/or keys. Some of these processing steps can be common to multiple classification levels such that the cryptographic processor 120 can potentially reuse the sub-circuits performing processing steps for the multiple classification levels.

[0018] A system bus 124 allows the processor 108 to communicate with a key manager 104, a partitioned key cache 116, an input/output (IO) access controller 112, and other peripherals that are not shown in the figure. The processor 108 communicates with the key manager 104, via the IO access controller 112, to access the partitioned key cache 116. Keys are loaded into the partitioned key cache 116 by the processor 104 in this embodiment and read by the cryptographic processor 120. Other embodiments could load the keys from an external source, for example.

[0019] The IO access controller 112 checks that the processor 108 or anything else using the system bus 124 is operating as expected. The processor 108 writes a state to the IO access controller 112. Each state is able to access peripherals defined by addresses or ranges of addresses. The IO access controller 112 checks that only the designated addresses are accessed by the processor 108 in a given state to assure that the interaction with the key manager 104 and partitioned key cache 116 to write keys is authorized. Each address or range of addresses can be designated for read only, write only or read and write accessible. The IO access controller 112 further understands how states transition through the state machine such that state transitions are also checked when the processor 108 is using the system bus 124.

[0020] There are states defined exclusive to the various classification levels. The cryptographic processor 120 performs certain key operations in certain states. The IO access controller 112 checks if an address range of a partitioned key cache 116 has been properly written by the processor based upon the current state. Table I gives an example of the states used for various classification levels. Additionally, the algorithm and key address is given in the table. These entries in the table serve as rules. For example, states four, seven and nine operate in a CONFIDENTIAL classification level using a DES

cryptographic algorithm and the key at address forty-three in the partitioned key cache. The IO access controller 112 in this example would make sure the current states were one of states four, seven or nine when the processor 108 writes the key at address forty-three in the partitioned key cache 116. Where a violation were determined the IO access controller 112,
 5 the key could be zeroized and/or other remedial action could be taken.

Table I. State Enforcement Rules

State(s)	Classification	Algorithm	Key Address
1	TS	AES 256	11
2, 19	S	AES 196	5
3, 21	NC	Triple DES	21
4, 7, 9	C	DES	43

[0021] As a packet passes through the cryptographic processor 120 certain algorithms use keys to perform the desired processing for that packet. The partitioned key cache 116 holds keys in a sterile or encrypted form. Sterilization puts the keys in a form that protects the
 10 encapsulated key even if recovered improperly. Various encryption algorithms could be used for sterilizing the keys. A key manager 104 is capable of deriving the key from the sterilized version. The partitioned key cache 116 could use dynamic random access memory (DRAM) or static random access memory (SRAM). This embodiment uses
 15 volatile RAM for the partitioned key cache 116 that is in a separate integrated circuit, but could be integral with the integrated circuit of the key manager 104 and/or cryptographic processor 120. The partitioned key cache 116 could be a segment of a larger memory used for other purposes in other embodiments.

[0022] A key manager 104 receives requests from the cryptographic processor 120 for keys used to process the various packets. The key manager 104 checks the requests,
 20 retrieves the sterilized key, reconstitutes the key, performs checks, and returns the key to the cryptographic processor 120. The key manager 104 is implemented in logic that is not reprogrammable during normal operation. To load keys into the partition key cache 116, the processor 108 interacts with the key manager 104 under the supervision of the IO access controller 112.

25 [0023] With reference to FIG. 2, a block diagram of an embodiment of a partitioned key cache 116 is shown. The partitioned key cache 116 has a number of partitions 204 defined.

Those partitions map to peripherals or address ranges used by the IO access controller 112. A given classification level stores its keys in one partition 204 and is prevented from accessing other partitions 204. Although the partitioned key cache 116 is a single integrated circuit with a common interface in this embodiment, the partitioning enforces a logical separation in a high-assurance manner. Table II gives an example of the mapping between state, classification and partition 204. These mappings serve as rules. For example, state one operates at a TOP SECRET classification level and has access to partition B 204-2, which includes addresses eleven through twenty.

Table II. State to Partition Mapping		
State(s)	Classification	Partition Addresses
1	TS	11-20
2, 19	S	1-10
3, 21	NC	21-30
4, 7, 9	C	31-45

10 [0024] Referring next to FIG. 3, a block diagram of an embodiment of a key manager 104 is shown. In a high-assurance manner, the key manager enforces logical separation of the partitioned key cache 116 where no physical separation of the interface to the partitioned key cache 116 exists. A key request interface 332 is coupled to the cryptographic processor 120 to receive requests for one or more particular key located at specified addresses in the partitioned key cache 116.

15 [0025] This embodiment includes a request validator 336 that checks the request to make sure the request is formatted correctly. Other embodiments of the request validator 336 could check that the classification level of the requesting packet matches the classification level of the partition 204 of the requested key. With a specified key location, a key memory interface 132 couples to the partitioned key cache 116 to retrieve the requested key. The sterile key is returned to a key buffer 308.

20 [0026] A rule enforcement circuit 336 includes a sterile key validator 304, a key decoder 324 and a reconstituted key validator 328. Multiple levels of checks are performed on the key before the key is provided to the cryptographic processor 120.

[0027] The sterile key validator 304 checks the classification level of the sterile key against the classification level of the packet that precipitated the request of the key. Essentially, the sterile key is checked to make sure it matches the type of processing being performed in the cryptographic processor 120 to provide high-assurance. The sterile key validator 304 could also match the algorithm and/or state as further rule checks in some embodiments.

[0028] A CRC, checksum or other validity value is appended to the sterile key in this embodiment when stored in the partitioned key cache 116. The software determines the validity value when writing the sterile key into the partitioned key cache 116. A check of the validity value allows conformation that information stored by the processor 108 was delivered accurately to the sterile key validator 304.

[0029] A key map database 316 holds information to validate the keys in their sterile or reconstituted form. The state, classification, address, algorithm, key length, header information, and/or other information could be stored in the key map database 316. A look-up table is used in one embodiment of the key map database 316. Where several keys are used for a given classification level, the finer granularity of state can confirm that the key is the correct one for a particular situation. For example, there could be a different state for each key. Other embodiments could provide granularity using two or more partitions 204 for a particular classification level.

[0030] A key decoder 324 converts the sterilized key from the partitioned key cache 116 into a reconstituted key that is ready for use by the cryptographic processor 120. A payload of the sterilized key is decrypted to produce a reconstituted key. A cache protection key store 320 holds a cache protection key for each classification level. Table III shows an example of the information stored in the cache protection key store 320. Other embodiments could have a different cache protection key for each sterilized key or one cache protection key for all keys.

Table III. Cache Protection Keys

State(s)	Classification	Random Key
1	TS	19A5E9F45609DC90h
2, 19	S	AA5119A456870190h
3, 21	N	78A5E49B56A093D0h
4, 7, 9	C	15E456894309AE9F0h

[0031] Within the decrypted payload of the sterilized key is information that is checked by a reconstituted key validator 328. Additionally, a CRC, checksum or other validity value is embedded in the decrypted payload as a second validity value. The reconstituted key validator 328 also checks the second validity value. This additional check provides a further layer of high-assurance. Should the process pass all of its checks, the decrypted key is provide to the cryptographic processor 120 for use in processing the particular packet that requested the key.

[0032] With reference to FIG. 4, a diagram demonstrating an embodiment of a key unscrambling process 400 is shown. A sterile key 416 includes a sterile key header, a sterile key payload and a sterile key CRC, which serves as a validity value. All this information is stored in the partitioned key cache 116 by the processor 108. The sterile key header holds the classification level, the applicable encryption algorithm(s), and any additional key identifiers. Some embodiments may also include the memory address of the sterile key. The sterile key CRC is a validity value that is calculated on the whole sterile key header and sterile key payload such that any corruption can be discerned.

[0033] The sterile key payload is exclusive-ORed 324 with a cache protection key 420 from the cache protection key store 320 to decrypt the reconstituted key header, reconstituted key payload and reconstituted key CRC. Those items along with the sterile key header and sterile key CRC form the reconstituted key 404. The reconstituted key payload is the actual key that will be used by the cryptographic processor 120. The reconstituted key CRC is a validity value that allows checking that the fields of the reconstituted key 404 has not changed. The exclusive-OR key decoder 324 is just one example of a simple decryption function. Other embodiments may use any type of decryption function(s).

[0034] Referring next to FIG. 5, a flowchart of an embodiment of a process 500 for operating the cryptographic device 100 is shown. The depicted portion of the process is initiated in block 504 where the cryptographic processor 120 has a packet that uses a particular key, which is requested from the key manager 104. Some embodiments check the key request. In any event, the key is requested from the partitioned key cache 116 by the key manager 104. The address of the key requested falls within a particular partition 204.

[0035] The sterile key 416 is retrieved in block 516 from the partitioned key cache 116 in block 516. The sterile key header is checked in block 520 to determine if the classification matches the classification of the packet requesting the key. Additional checks are possible, for example, the sterile key CRC or validity value could be checked. Presuming the check in block 520 is successful, processing continues to block 524 where the sterile key payload is decrypted.

[0036] In the reconstituted key 404, the reconstituted key header is checked in block 528. Prior to the decoding block 524, the reconstituted key header was scrambled. Additionally, a reconstituted key CRC or validity value can be checked in some embodiments. If the check in block 528 passes, processing continues to block 532 where the key is returned the cryptographic processor 120.

[0037] Should any of the checks fail in blocks 520 or 528, the partitioned key cache 116 is erased and/or the cache protection key store 320 in block 536. Without the cache protection keys, the keys remain in a sterile form. Erasure of the cache protection keys can typically be performed much more quickly than the partitioned key cache 116. Further remedial action can be taken in block 540.

[0038] The above embodiments discuss processing at different classification levels. These classification levels could be government classification levels, but need not be necessarily so. A classification level is just a logical partition in the information passed. Any information that needs to be kept separate from other information could be in a separate classification level or logical partition.

[0039] While the principles of the disclosure have been described above in connection with specific apparatuses and methods, it is to be clearly understood that this description is made only by way of example and not as limitation on the scope of the disclosure.

CLAIMS

WHAT IS CLAIMED IS:

- 1 1. A cryptographic device for processing classified information having
2 a plurality of different classification levels, the cryptographic device comprising:
3 a memory holding a plurality of keys outside of an integrated circuit,
4 wherein the plurality of keys are for the plurality of different classification levels;
5 a cryptographic processor that is part of the integrated circuit, wherein the
6 cryptographic processor uses the plurality of keys to process packets of information that are
7 categorized according to the plurality of different classification levels; and
8 a key manager, wherein:
9 the key manager can access a plurality of rules associated
10 with the plurality of different classification levels,
11 the plurality of rules regulate interaction with the plurality of
12 keys,
13 a first rule of the plurality of rules is used by the key manager
14 in a first classification level of the plurality of different classification levels,
15 and
16 a second rule of the plurality of rules is used by the key
17 manager in a second classification level of the plurality of different
18 classification levels.
- 1 2. The cryptographic device for processing classified information
2 having the plurality of different classification levels as recited in claim 1, wherein:
3 a first key accessed in the first classification level includes a header that is
4 checked against the first rule, and
5 the first key includes a coded header that is checked against the first rule.
- 1 3. The cryptographic device for processing classified information
2 having the plurality of different classification levels as recited in claim 1, wherein the first
3 and second keys are encrypted in the memory.
- 1 4. The cryptographic device for processing classified information
2 having the plurality of different classification levels as recited in claim 1, wherein the
3 plurality of keys are stored in an encrypted state.

1 5. The cryptographic device for processing classified information
2 having the plurality of different classification levels as recited in claim 1, wherein the key
3 manager further comprises a key decoder, which decrypts the plurality of keys before
4 passing them to the cryptographic processor.

1 6. The cryptographic device for processing classified information
2 having the plurality of different classification levels as recited in claim 1, further comprising
3 an access controller, wherein the access controller checks that a predetermined state of
4 operation is active while writing the first key to a partition of the memory.

1 7. A method for processing classified information in a high-assurance
2 manner, the method comprising steps of:
3 receiving a request for a first key by a cryptographic processor;
4 choosing a first rule from a plurality of rules;
5 retrieving a first sterile key from a memory;
6 checking the first sterile key with the first rule;
7 decrypting the first sterile key with a first protection key to produce the first
8 key;
9 checking the first key with the first rule;
10 providing the first key to the cryptographic processor if the checking the first
11 sterile key step and the checking the first key step are completed successfully;
12 receiving a request for a second key by a cryptographic processor;
13 choosing a second rule from the plurality of rules;
14 retrieving the second sterile key from the memory;
15 checking the second sterile key with the second rule;
16 decrypting the second sterile key with a second protection key to produce a
17 second key;
18 checking the second key with the second rule; and
19 providing the second key to the cryptographic processor if the checking the
20 second sterile key step and the checking the second key step are completed successfully.

1 8. The method for processing classified information in the high-
2 assurance manner as recited in claim 7, further comprising a step of erasing the first and
3 second protection keys to zeroize utility of the first and second keys.

1 9. The method for processing classified information in the high-
2 assurance manner as recited in claim 7, wherein the cryptographic processor is capable of
3 processing multiple classification levels simultaneously in different packets.

1 10. The method for processing classified information in the high-
2 assurance manner as recited in claim 7, wherein the first rule requires a classification level
3 of a packet being processed with the cryptographic processor to match the classification
4 level of the first key.

1 11. The method for processing classified information in the high-
2 assurance manner as recited in claim 7, wherein:
3 the first and second sterile keys are stored in a second integrated circuit, and
4 the decrypting steps are performed in a first integrated circuit.

1 12. A cryptographic device for processing information with a plurality of
2 classification levels, the cryptographic device comprising:
3 a memory holding a plurality of keys;
4 a cryptographic processor that uses the plurality of keys to process packets
5 of information that are correlated to the plurality of classification levels; and
6 a key manager that comprises a rule enforcement circuit and a key
7 decryption circuit, wherein:
8 the key manager retrieves a first key for a first packet being
9 processed by the cryptographic processor,
10 the first packet is of a first classification level,
11 the first key is associated with the first classification level,
12 the rule enforcement circuit checks that the first key is
13 designated for the first classification level before providing the first key to
14 the cryptographic processor for processing the first packet,
15 the key manager retrieves a second key for a second packet
16 being processed by the cryptographic processor,
17 the second packet is of a second classification level,
18 the second key is associated with the second classification
19 level, and

20 the rule enforcement circuit checks that the second key is
21 designated for the second classification level before providing the second
22 key to the cryptographic processor for processing the second packet.

1 13. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein at least one of the first and
3 second keys are stored in the memory in an unusable form.

1 14. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein the key manager further
3 comprises a key decoder that descrambles the first key before providing the first key to the
4 cryptographic processor.

1 15. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein the memory and the
3 cryptographic processor are in different integrated circuit.

1 16. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein:
3 the plurality of keys are divided among a plurality of partitions in the
4 memory, and
5 each classification level has a different partition to logically separate keys of
6 different classification levels.

1 17. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein the plurality of classification
3 levels includes a plurality of protection values that are each used to descramble the plurality
4 of keys.

1 18. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein the rule enforcement circuit
3 checks the first key twice to confirm that the first classification level of the key matches the
4 first classification level of the packet.

1 19. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein the first and second keys are
3 decrypted in the key manager.

1 20. The cryptographic device for processing information with the
2 plurality of classification levels as recited in claim 12, wherein a header is used to designate
3 the first key for the first classification level.

AMENDED CLAIMS

received by the International Bureau on 29 December 2008 (29.12.2008)

1. A cryptographic device for processing classified information having a plurality of different classification levels, the cryptographic device comprising:

a memory holding a plurality of keys outside of an integrated circuit, wherein the plurality of keys are for the plurality of different classification levels, wherein the plurality of keys are stored in the memory in an encrypted state, the plurality of keys include an encrypted header and an encrypted key payload, and further wherein decrypting the encrypted key payload results in a reconstituted key header and a reconstituted key payload;

a cryptographic processor that is part of the integrated circuit, wherein the cryptographic processor uses the plurality of keys to process packets of information that are categorized according to the plurality of different classification levels; and

a key manager, wherein:

the key manager can access a plurality of rules associated with the plurality of different classification levels,

the plurality of rules regulate interaction with the plurality of keys,

a first rule of the plurality of rules is used by the key manager in a first classification level of the plurality of different classification levels,

a second rule of the plurality of rules is used by the key manager in a second classification level of the plurality of different classification levels;

the encrypted header and the reconstituted key header of a key associated with the first classification level are checked against the first rule; and

the encrypted header and the reconstituted key header of a key associated with the second classification level are checked against the second rule.

2. The cryptographic device for processing classified information having the plurality of different classification levels as recited in claim 1, wherein the plurality of keys further include a first encrypted cyclical redundancy check (CRC) value that is calculated on the encrypted header and the encrypted key payload, and the key manager calculates a second

encrypted CRC value based on the encrypted header and the encrypted key payload and discards the encrypted key payload if the second encrypted CRC and the firsts encrypted CRC are different.

3. The cryptographic device for processing classified information having the plurality of different classification levels as recited in claim 1, wherein the key manager further comprises a key decoder, which decrypts the encrypted key payload of the plurality of keys before passing the reconstituted key payload to the cryptographic processor.

4. The cryptographic device for processing classified information having the plurality of different classification levels as recited in claim 1, further comprising an access controller, wherein the access controller checks that a predetermined state of operation is active while writing the first key to a partition of the memory.

5. A method for processing classified information in a high-assurance manner, the method comprising steps of:

- receiving a request for a first key by a cryptographic processor;
- choosing a first rule from a plurality of rules;
- retrieving a first sterile key from a memory, wherein the first sterile key includes a first sterile header and a first sterile key payload;
- checking the first sterile header with the first rule;
- decrypting the first sterile key payload with a first protection key to produce the first key and a first reconstituted header;
- checking the first reconstituted header with the first rule;
- providing the first key to the cryptographic processor if the checking the first sterile header step and the checking the first reconstituted header step are completed successfully;
- receiving a request for a second key by the cryptographic processor;
- choosing a second rule from the plurality of rules;
- retrieving a second sterile key from the memory, wherein the second sterile key includes a second sterile header and a second sterile key payload;
- checking the second sterile header with the second rule;

decrypting the second sterile key payload with a second protection key to produce a second key and a second reconstituted header;
checking the second reconstituted header with the second rule; and
providing the second key to the cryptographic processor if the checking the second sterile header step and the checking the second reconstituted header_step are completed successfully.

6. The method for processing classified information in the high-assurance manner as recited in claim 5, further comprising a step of erasing the first and second sterile keys to zeroize utility of the first and second keys.

7. The method for processing classified information in the high-assurance manner as recited in claim 5, wherein the cryptographic processor is capable of processing multiple classification levels simultaneously in different packets.

8. The method for processing classified information in the high-assurance manner as recited in claim 5, wherein the first rule requires a classification level of a packet being processed with the cryptographic processor to match the classification level of the first key.

9. The method for processing classified information in the high-assurance manner as recited in claim 5, wherein:
the first and second sterile keys are stored in a second integrated circuit, and
the decrypting steps are performed in a first integrated circuit.

10. A cryptographic device for processing information with a plurality of classification levels, the cryptographic device comprising:
a memory holding a plurality of keys, wherein the plurality of keys are divided among a plurality of partitions in the memory, and each classification level has a different partition to logically separate keys of different classification levels;
a cryptographic processor that uses the plurality of keys to process packets of information that are correlated to the plurality of classification levels; and
a key manager that comprises a rule enforcement circuit, wherein:

the key manager retrieves a first key for a first packet being processed by the cryptographic processor,
the first packet is of a first classification level,
the first key is associated with the first classification level,
the rule enforcement circuit checks that the first key is designated for the first classification level before providing the first key to the cryptographic processor for processing the first packet,
the key manager retrieves a second key for a second packet being processed by the cryptographic processor,
the second packet is of a second classification level,
the second key is associated with the second classification level,

and

the rule enforcement circuit checks that the second key is designated for the second classification level before providing the second key to the cryptographic processor for processing the second packet.

11. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein at least one of the first and second keys are stored in the memory in an unusable form.

12. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein the key manager further comprises a key decoder that descrambles the first key before providing the first key to the cryptographic processor.

13. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein the memory and the cryptographic processor are in different integrated circuit.

14. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein the plurality of classification levels includes a plurality of protection values that are each used to descramble the plurality of keys.

15. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein the rule enforcement circuit checks the first key twice to confirm that the first classification level of the key matches the first classification level of the packet.

16. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein the first and second keys are decrypted in the key manager.

17. The cryptographic device for processing information with the plurality of classification levels as recited in claim 10, wherein a header is used to designate the first key for the first classification level.

1 / 4

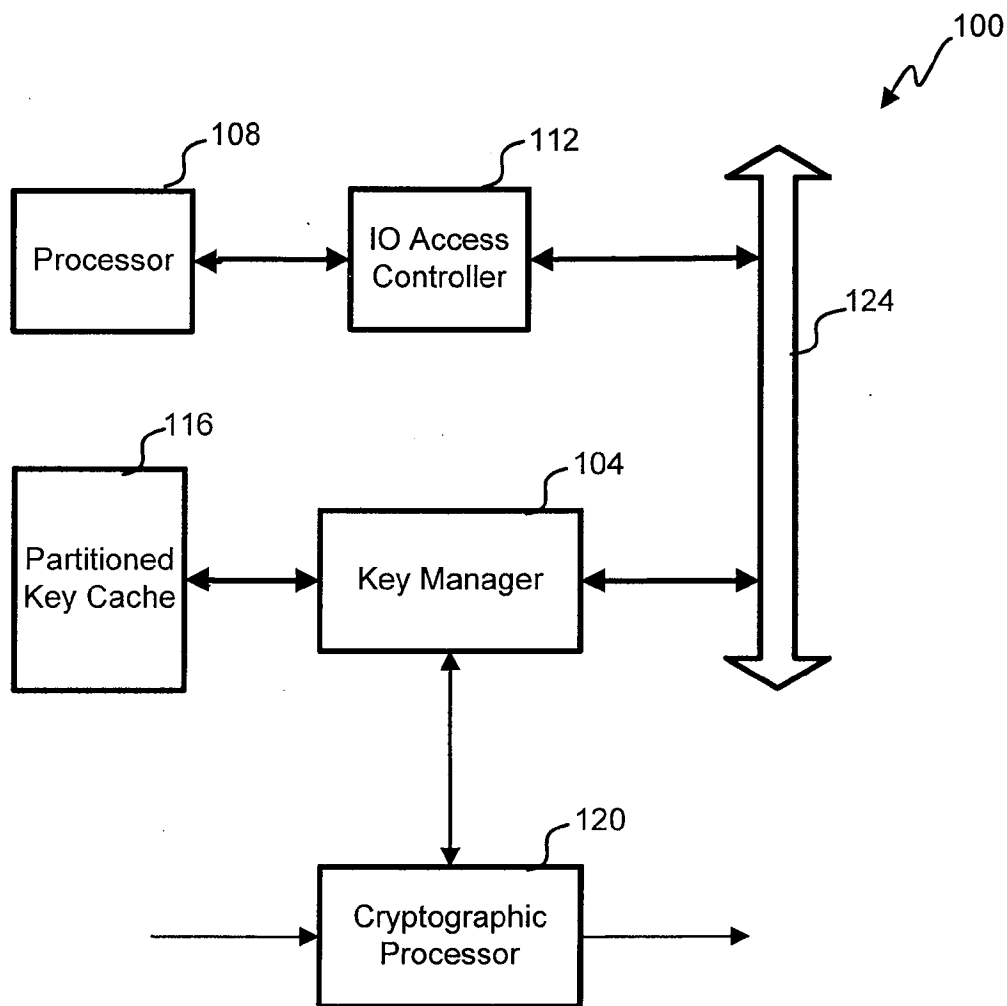


Fig. 1

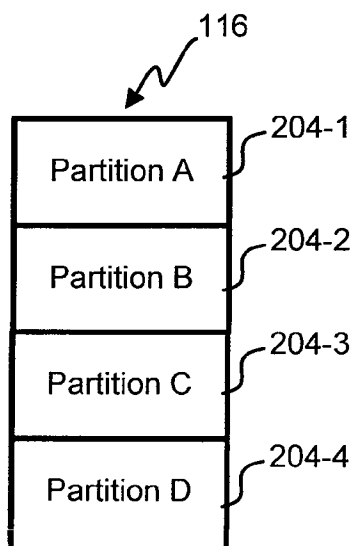


Fig. 2

2/4

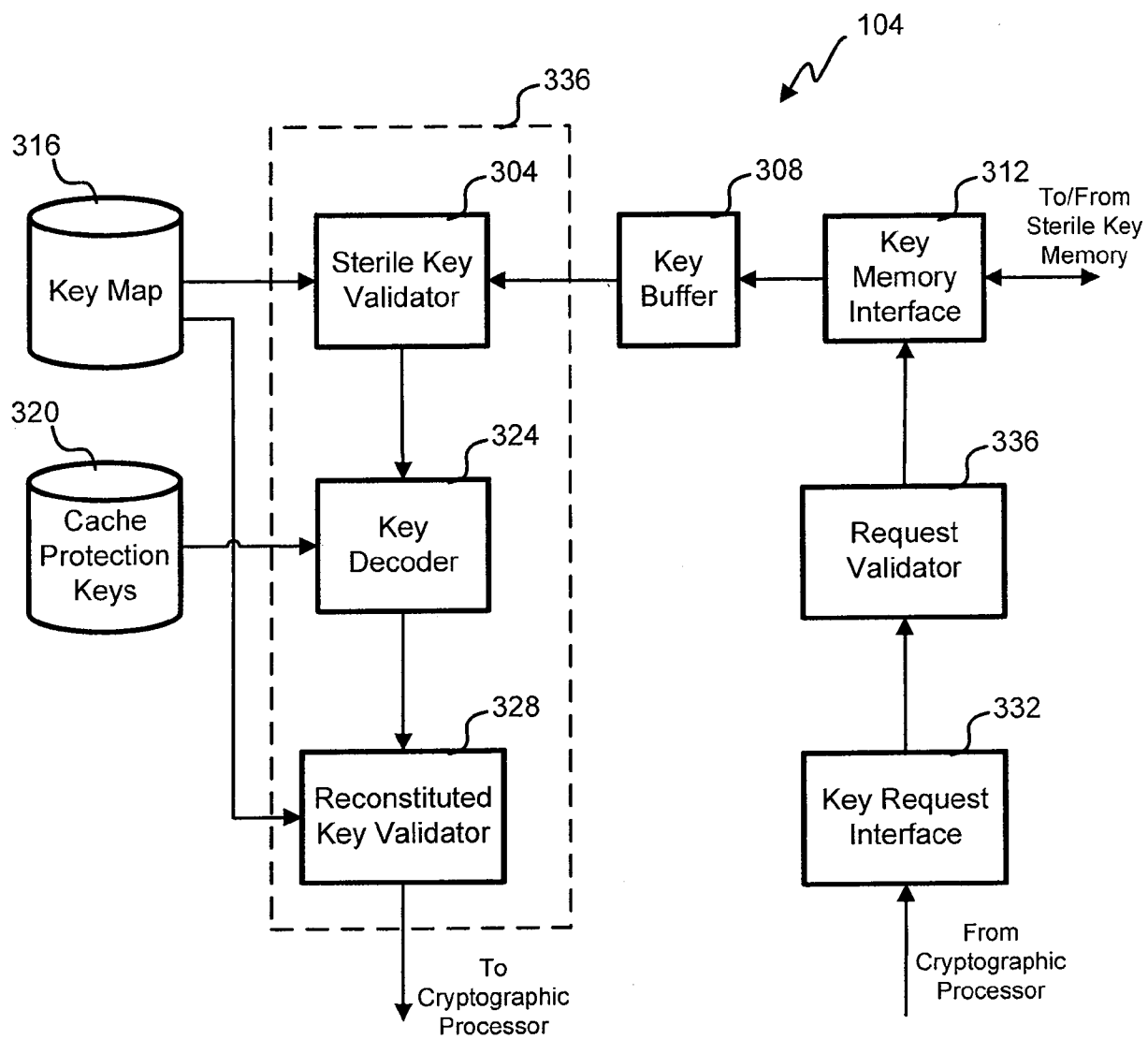


Fig. 3

3/4

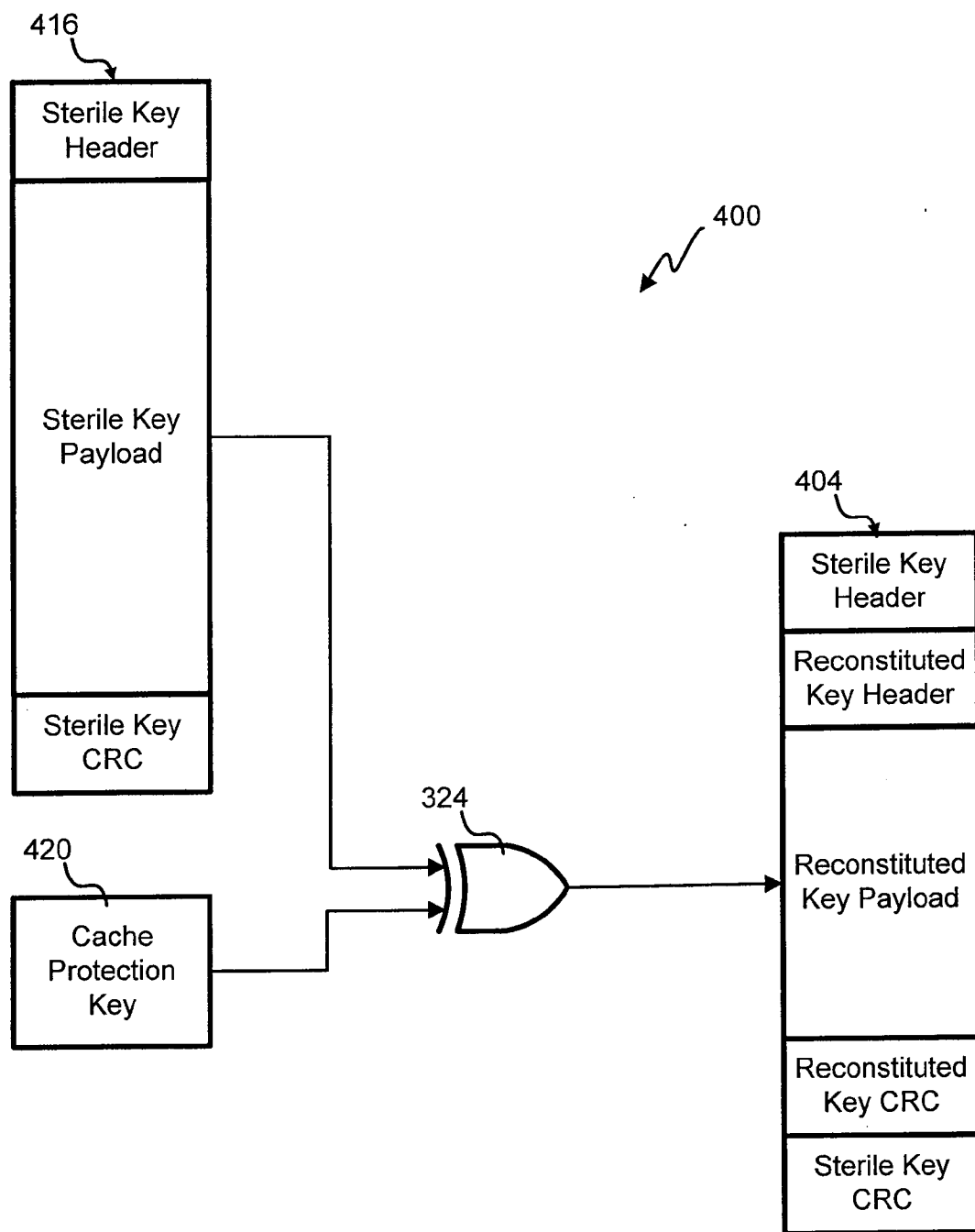


Fig. 4

4 / 4

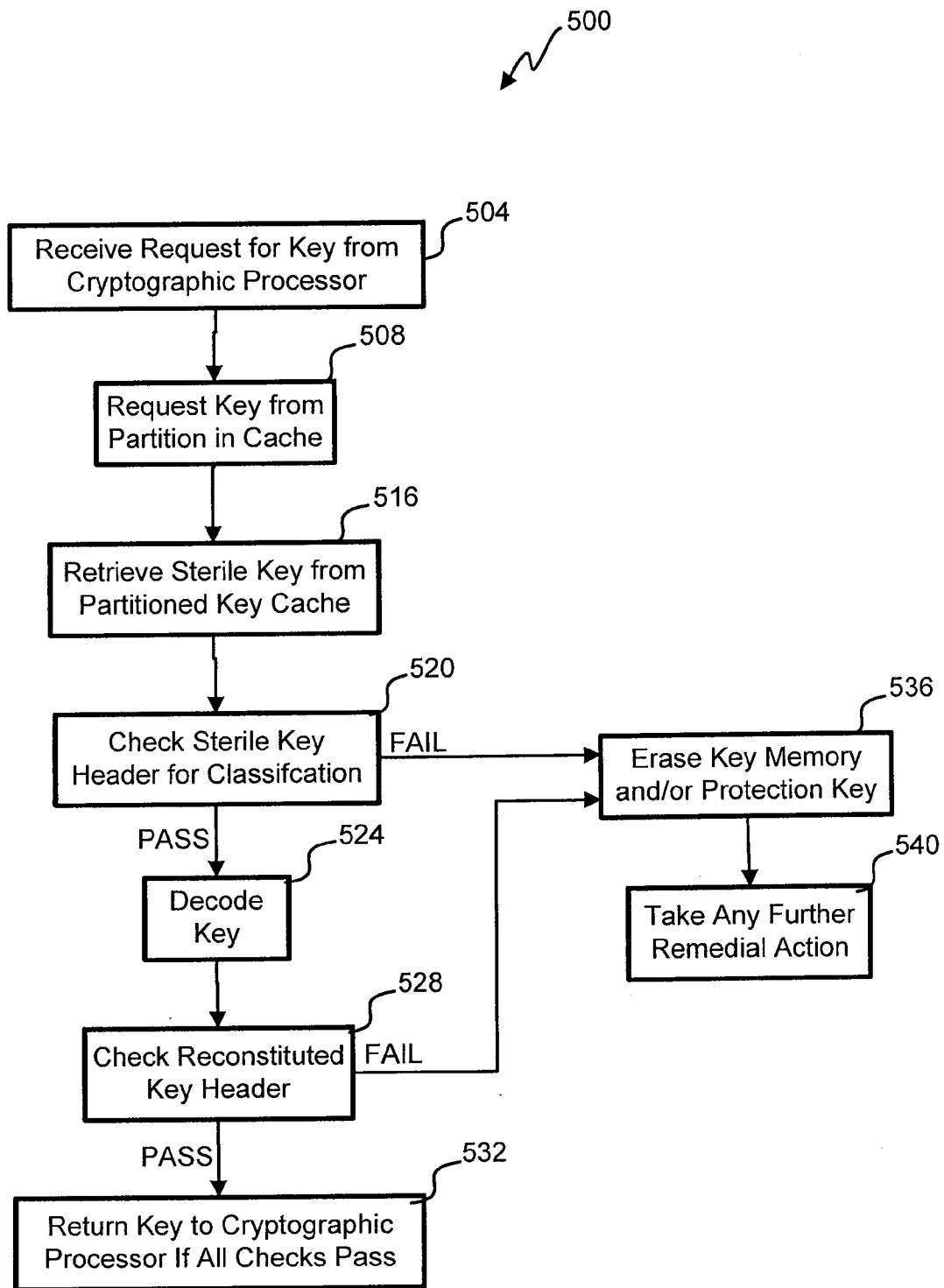


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/071821

A. CLASSIFICATION OF SUBJECT MATTER

INV. 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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 876 026 A (MOTOROLA INC [US]) 4 November 1998 (1998-11-04) the whole document	1-20
X	US 6 836 548 B1 (ANDERSON MARK STEPHEN [AU] ET AL) 28 December 2004 (2004-12-28) column 5, line 15 - column 8, line 51 figures 2,3	1,3-5,7
A	EP 1 326 157 A (PERVASIVE SECURITY SYSTEMS INC [US]) 9 July 2003 (2003-07-09) paragraph [0015] - paragraph [0063]	1-20

☐ 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

22 October 2008

Date of mailing of the international search report

29/10/2008

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Segura, Gustavo

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2008/071821

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
EP 0876026	A	04-11-1998	JP	10320191 A		04-12-1998
			TW	386202 B		01-04-2000
			US	6101255 A		08-08-2000
US 6836548	B1	28-12-2004	CA	2082146 A1		03-12-2003
			NZ	245020 A		28-04-2006
EP 1326157	A	09-07-2003	JP	2003218851 A		31-07-2003
			US	7178033 B1		13-02-2007