UnifiedPatents

PATROLL Winning Submission

U.S. Patent 8,127,145

U.S. Patent 8,127,145 ("*Speir*" or the "patent-at-issue") was filed on March 23, 2006. Claim 1 of the patent-at-issue is generally directed to a method of providing a secure file service in a computer system comprising a secure file services module and a secure user processor. The system includes first and second communication paths which are separate from each other and between the services module and secure processor. The secure file services module includes file system control interface, client access interface, a cryptographic processor, and a secure file system hosted by the cryptographic processor. The method includes authenticating a user using the file system control interface and issuing a request for a classified data file from the secure user processor to the client access interface. Once the file system containing the classified data file is accessed, the cryptographic processor will then decrypt the data file. The decrypted data file is then transferred to the secure user processor.

The primary reference, U.S. Patent 8,099,769 ("*Blackberry*"), was filed on March 27, 2007 and claims priority on July 16, 2001. According to the paragraph in the specification entitled "Cross-Reference to Related Applications," the patent-at-issue is a divisional of U.S. patent application Ser. No. 09/905,113 filed on July 16, 2000, now U.S. Pat. 7,216,237, and is hereby incorporated by reference. The patent is directed to a method of establishing a trusted path for data between correspondents in a public-key cryptographic scheme, and one of the correspondents is a personalized device. The personalized device includes a secure module which stores a said secret key and is connected via a first secure path to a secure input device and being connected via a second secure path to a secure display of the personalized device.

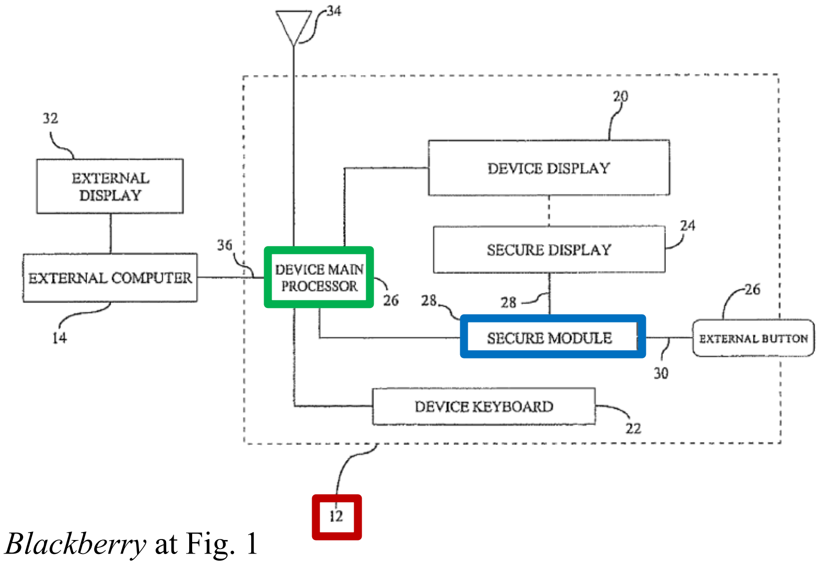
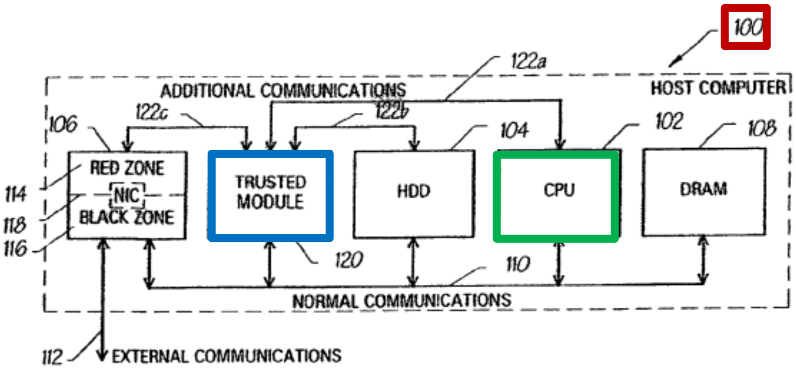
The primary reference, U.S. Patent 7,236,455 ("*Hewlett Packard*"), was filed on February 15, 2000 and claims priority on February 15, 1999. The patent is directed to a system of improving trust and security between various modules in a computing device. A computing device is composed of hardware modules and a shared communication infrastructure and to improve the security in the device, a trusted hardware module is provided and connected to other modules via communication paths distinct from the communication infrastructure. With this, each module can directly communicate with the trusted module instead of communicating directly with any other modules.

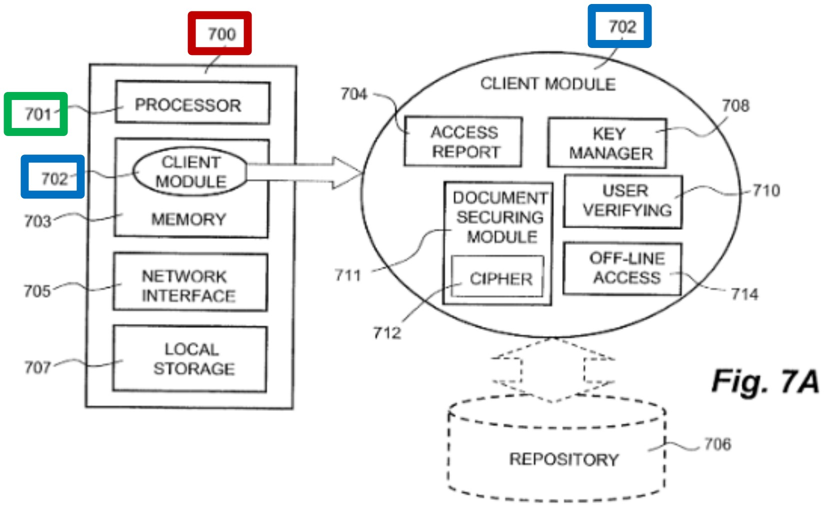
The secondary reference, U.S. Patent 7,681,034 ("*Intellectual Ventures*"), was filed on February 12, 2002 and claims priority on December 12, 2001. According to the paragraph in the specification entitled "Cross-Reference to Related Applications," the patent-at-issue claims the benefits of U.S. Provisional Application 60/339,634, filed on December 12, 2001, and entitled "Pervasive Security Systems," which is hereby incorporated by reference for all purposes. The patent is directed to a method of securing a file which involves determining if the file being accessed in a file system is secured. If secured, a document-securing module obtains a user or group key to decrypt the security information in the secured document for access rules. If the user accessing the document is authorized, a file key is retrieved, and a cipher module is activated to decrypt the encrypted data portion.

The secondary reference, U.S. Patent 7,167,982 ("*Lenovo*"), was filed on September 14, 2001 and claims priority on the same date. The patent is directed to a method of securing decrypted files in a sharing environment. The method includes a filter driver in a kernel space receiving a request to open a document in a file system. If the request is to open an encrypted file in a shared area, the filter driver may block the request to a file system driver. The filter driver may issue the file system driver to read the encrypted data and upon reading, the file system driver may transfer the encrypted data to the filter driver. The filter driver may then decrypt the data and store the data in a non-shared area which is accessible only to authorized users.

A sample claim chart comparing claim 1 of *Speir* to *Blackberry*, *Hewlett Packard*, *Intellectual Ventures*, and *Lenovo* is provided below.

US8127145 (“*Speir*”)	**A. US8099769** (*“Blackberry”*) **B. US7236455** (*“Hewlett Packard”*) **C. US7681034** (*“Intellectual Ventures”*) **D. US7167982** (*“Lenovo”*)
1.pre. A method for providing **a secure file service**, comprising:	**A. US8099769** “In accordance with one of its aspects, the invention provides **a method of establishing a trusted path for data** between correspondents in a public-key cryptographic scheme, one of the correspondents being a personalized device.” *Blackberry* at col. 3:15-18 **B. US7236455** “Assuming all is well, in steps 685 and 690, the user and the trusted platform use other protocols to **set up secure communications for other data**, where the data from the platform is preferably signed by the trusted device 24.” *Hewlett Packard* at col. 12:9-12 **C. US7681034** “1. A computer implemented method for **securing a file**, the method comprising: . . . .” *Intellectual Ventures* at claim 1 **D. US7167982** “FIG. 5 illustrates a filter driver 503 in kernel space 402 configured to **protect decrypted files in a file sharing environment** in accordance with the present invention.” *Lenovo* at col. 5:29-31
1.a. providing a computer system for operation in an unsecure environment, **said computer system comprising a secure file services module and a secure user processor which is separate and distinct from said secure file services module**, **each configured to secure data contained therein wherein said secure file services module and said secure user processor are embodied on the same computing device**;	**A. US8099769** “In this embodiment **the personalized device** 12 **is a mobile phone controlled by the device main processor** 16 **including a secure module** 18.” *Blackberry* at col. 4:12-14 “The **secure module** 18 **is adapted to operate independently of the device main processor** 16, so that the internal state of the secure module 18 can not be readily reverse engineered and/or that its interactions with the underlying hardware are not maliciously intercepted and reinterpreted.” *Blackberry* at col. 4:15-19

(cont.) 1.a. providing a computer system for operation in an unsecure environment, said **computer system comprising a secure file services module and a secure user processor which is separate and distinct from said secure file services module**, **each configured to secure data contained therein wherein said secure file services module and said secure user processor are embodied on the same computing device;**	"In accordance with one of its aspects, the invention provides **a method of establishing a trusted path for data** between correspondents in a public-key cryptographic scheme, one of the correspondents being a personalized device." *Blackberry* at col. 3:15-18  34 20 32 EXTERNAL DISPLAY DEVICE DISPLAY 24 SECURE DISPLAY 36 EXTERNAL COMPUTER DEVICE MAIN PROCESSOR 26 28 28 26 SECURE MODULE EXTERNAL BUTTON 14 30 DEVICE KEYBOARD 22 12 *Blackberry* at Fig. 1 **B. US7236455** "The **host computer** 100 **also includes a trusted module** 120 **which is connected**, not only to the normal communication paths 110, but also **by mutually separate additional communication paths** 122 (sub-referenced 122 a,122 b,122 c) **to the CPU** 102, hard disk drive 104 and the red zone 114 of the network interface card 106." *Hewlett Packard* at col. 14:26-31  100 122a ADDITIONAL COMMUNICATIONS HOST COMPUTER 106 122c 122b 104 102 108 RED ZONE NIC BLACK ZONE TRUSTED MODULE HDD CPU DRAM 114 118 116 120 110 NORMAL COMMUNICATIONS 112 EXTERNAL COMMUNICATIONS *Hewlett Packard* at Fig. 7

(cont.) 1.a. providing a computer system for operation in an unsecure environment, said **computer system comprising a secure file services module and a secure user processor which is separate and distinct from said secure file services module**, **each configured to secure data contained therein wherein said secure file services module and said secure user processor are embodied on the same computing device**;	**C. US7681034** "According to one embodiment, **the client machine** 700 **includes a processor** 701, **a client module** 702, a memory space 703, a network interface 705 and a local store 707." *Intellectual Ventures* at col. 30:45-48 "According to one embodiment, **the client computer** 100 **is loaded with a client module** that is a linked and compiled, or interpreted, version of one embodiment of the present invention and is capable of communicating with a server 104 or 106 over a data network (i.e., the Internet or a local area network). According to another embodiment, the client computer 100 is coupled to the server 104 through a private link. As will be further explained below, **a document created by an authoring tool is secured by the client module** that will be described in detail below. **The client module, when executed, is configured to ensure that a secured document is secured at all times** in a store (e.g., a hard disk or other data repository)." *Intellectual Ventures* at col. 8:20-32  700 701 702 PROCESSOR CLIENT MODULE MEMORY 703 705 NETWORK INTERFACE 707 LOCAL STORAGE 702 704 CLIENT MODULE 708 ACCESS REPORT KEY MANAGER DOCUMENT SECURING MODULE USER VERIFYING 710 711 CIPHER OFF-LINE ACCESS 714 712 REPOSITORY 706 *Fig. 7A* *Intellectual Ventures* at Fig. 7A **D. US7167982** "**Client** 102 **has a central processing unit (CPU)** 210 coupled to various other components by system bus 212. An operating system 230 runs on CPU 110 and provides control and coordinates the function of the various components of FIG. 2." *Lenovo* at col. 3:39-43

<table>
<tr>
<td>

1.b. providing **first and second secure communication paths** in said unsecure environment **directly between said secure file services module and said secure user processor**,

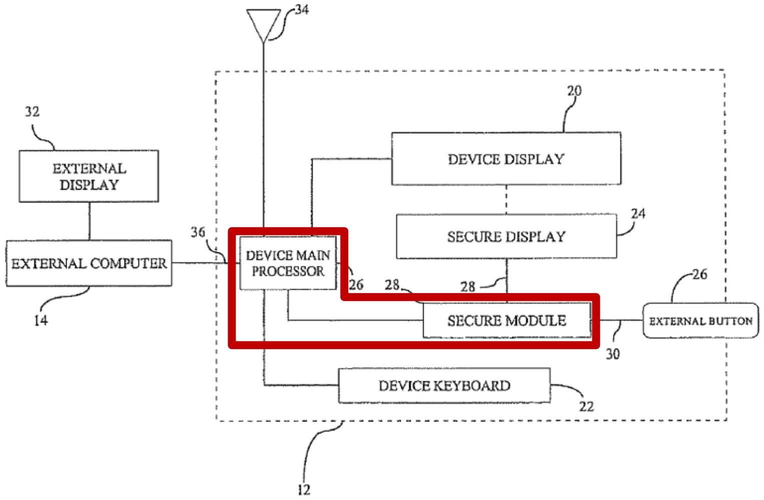
said **first secure communication path being separate from said second secure communication path and configured to physically secure data communicated thereover by employing physically secure communication path hardware**,

said **second secure communication path configured to exclusively support user sign-on services and to only software secure data communicated thereover**;

</td>
<td>

A. US8099769

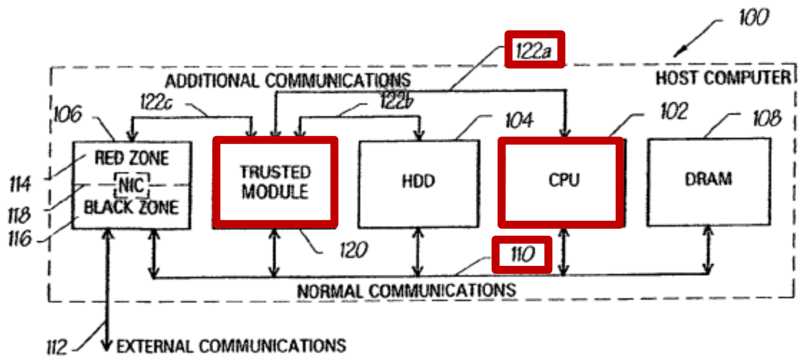
"The **secure module** 18 **may be equipped with a verification manager to identify the user using the system** 10. The **verification manager determines the access rights and privileges through passwords** or biometrics. For example, the **external trusted button** 26 **may also be used to enter a PIN should access control to the secure module** 18 **be required**." *Blackberry* at col. 5:6-11



Blackberry at Fig. 1

B. US7236455

"The host computer 100 also includes a **trusted module** 120 **which is connected, not only to the normal communication paths** 110, **but also by mutually separate additional communication paths** 122 (sub-referenced 122 a,122 b,122 c) **to the CPU** 102, hard disk drive 104 and the red zone 114 of the network interface card 106. By way of example, the trusted module 120 does not have such a separate additional communication path 122 with the memory 108." *Hewlett Packard* at col. 14:26-33



Hewlett Packard at Fig. 7

</td>
</tr>
</table>

(cont.) 1.b. providing **first and second secure communication paths** in said unsecure environment **directly between said secure file services module and said secure user processor**, said **first secure communication path being separate from said second secure communication path and configured to physically secure data communicated thereover by employing physically secure communication path hardware**, said **second secure communication path configured to exclusively support user sign-on services and to only software secure data communicated thereover**;	"In accordance with the present invention, there is provided a computing apparatus, comprising a trusted hardware module; a plurality of further hardware modules; **a shared communication infrastructure** (such as normal EISA and PCI buses) **by which the modules can communicate with each other; and a first communication path, distinct from the communication infrastructure**, by which a first one of the further modules can communicate directly with the trusted module but cannot communicate directly with any other of the further modules." *Hewlett Packard* at col. 2:20-29 "The **first communication path may be implemented as a single dedicated physical wire that permits serial communications**, or multiple wires, or optical connections, or very short distance wireless transmissions on different frequencies, and so on." *Hewlett Packard* at col. 2:34-39 "In this example of a trusted platform, there is provided the incorporation into a **computing platform of a physical trusted device** whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform." *Hewlett Packard* at col. 5:53-57 "**Keys may be used for communications** between the internal modules 102,104,106,120 of the platform **over the normal communication paths** 110." *Hewlett Packard* at col. 15:18-21 "The trusted module 120 performs the **authentication and integrity checks using the long term keys** inside the trusted module 120 that must not revealed outside the trusted module 120, and sends a protocol data unit 150 containing an 'OK' indication to the red zone 114 of the network interface card 106 using the additional communication path 122 c." *Hewlett Packard* at col. 15:64-67 through col. 16:1-3 **C. US7681034** "According to one embodiment, the **client module includes a document-securing module** that is implemented to operate in an operating system. In particular, the **document-securing module operates in a path through which a document being accessed would pass**, as such, the document can be examined or detected for the security nature." *Intellectual Ventures* at col. 3:67 through col. 4:1-5

(cont.) 1.b. providing **first and second secure communication paths** in said unsecure environment **directly between said secure file services module and said secure user processor**, said **first secure communication path being separate from said second secure communication path and configured to physically secure data communicated thereover by employing physically secure communication path hardware**, said **second secure communication path configured to exclusively support user sign-on services and to only software secure data communicated thereover**;	“As described above, the **user may login on any time from a client machine** when he/she needs to access a secured document. When such contact does happen, the server will receive the credential information from the user to ensure that the user is who he/she claims to be. After the user is authenticated, the new keys are encrypted with the credential information at 524.” *Intellectual Ventures* at col. 25:19-25 “As will be further described below, to access a secured document, **a user needs a user key or keys to decrypt the encrypted security information** or header first. In one embodiment, **the key or keys are associated with a user's login to a local server or a central server**. Appropriate **access privilege associated with the user is validated if the user has been authenticated or previously registered with the server and properly logged in**.” *Intellectual Ventures* at col. 12:51-58
1.c. communicating **an authentication request to said secure file services module** over said **second secure communication path**, said secure file services module including **a file system control interface**, **a client access interface**, **a cryptographic processor** and **a secure file system hosted by said cryptographic processor**;	**A. US8099769** “The **data message for authentication is transmitted** from the external computer via a communication path **to the personalized device** 12 and received by the message transceiver 34.” *Blackberry* at col. 4:42-45 “In this embodiment the **personalized device** 12 **is a mobile phone** controlled by the device main processor 16 **including a secure module** 18.” *Blackberry* at col. 4:12-14 “The **secure module** 18 may be **equipped with a verification manager to identify the user using the system** 10. The verification manager determines the access rights and privileges through passwords or biometrics.” *Blackberry* at col. 5:6-9 “Step 100: The **secure module** 18 **accepts data from device main processor** 16, the data comprises the portion of the data message to be signed and may have been assembled on the personalized device 12 or assembled externally by a external computer 14 and then conveyed to the personalized device 12; . . . .” *Blackberry* at col. 5:38-42

(cont.) 1.c. communicating **an authentication request to said secure file services module** over said **second secure communication path**, said secure file services module including **a file system control interface**, **a client access interface**, **a cryptographic processor** and **a secure file system hosted by said cryptographic processor**;	"1. A method for controlling use of a secret key in a personalized device communicatively coupled to a main processor, said personalized device adapted to receive and transmit data messages, said method comprising: . . . upon receipt of an external input via said secure input device indicative of a favorable comparison of said first and second outputs as displayed, controlling operation of said personalized device to obtain access to said secret key in said **secure module for performing cryptographic operations**." *Blackberry* at claim 1 "In order to mitigate the drawbacks of prior art devices, the method of establishing a trusted communication path for data between authenticating device and its user comprises the steps of: logically isolating the secure module from the main processor of the personalized device; **storing the private key within the secure module**; providing trusted paths between the user and the secure module of the personalized device, ..." *Blackberry* at col. 3:30-36 **B. US7236455** "Beforehand, a platform configured for use by users of in this way will typically be operating under the control of its standard operating system and executing the **authentication process, which waits for a user to insert their smart card** 19." *Hewlett Packard* at col. 12:47-50 "The network interface card 106 sends a protocol data unit 148 (to be described in further detail later) containing some data and **a request for an authentication and integrity check to the trusted module** 120 using the normal communication paths 110." *Hewlett Packard* at col. 15:60-64 "FIG. 8 illustrates the **physical architecture of the trusted module** 120. A **first switching engine** 124 **is connected separately to the additional communication paths** 122 a,b,c and also to an internal communication path 126 of the trusted module 120. This switching engine 124 is under control of a policy loaded into the trusted module 120. Other **components of the trusted module** 120 **are**: a computing engine 128 that manages the trusted module 120 and performs general purpose computing for the trusted module 120; **volatile memory** 130 **that stores temporary data**; **non-volatile memory** 132 **that stores long term data**; **cryptographic engines** 134 that perform specialist crypto functions such as encryption and key

(cont.) 1.c. communicating **an authentication request to said secure file services module** over said **second secure communication path**, said secure file services module including **a file system control interface**, **a client access interface**, **a cryptographic processor** and **a secure file system hosted by said cryptographic processor**;	generation; a random number source 136 used primarily in crypto operations; a **second switching engine** 138 **that connects the trusted module** 120 **to the normal communication paths** 110; and tamper detection mechanisms 140, all connected to the internal communication path 126 of the trusted module 120. The trusted module 120 is based on a trusted device or module 14 as described in more detail above with reference to FIGS. 1 to 6." *Hewlett Packard* at col. 14:51-67 through col. 15:1-8 **C. US7681034** "19. A computer implemented method for providing access control to a file, the method comprising: forwarding a **request to access the file to a file system manager** in an operating system; activating a **document securing module** by the file system manager to determine whether the file stored in a file system driver and being accessed is secured, wherein the file includes a header having a file key, the file key is encrypted with a user key, and the user key is different from the file key; activating a **cipher module** if the file is determined to be secured; and **loading the file from the file system driver** through the cipher module into an application." *Intellectual Ventures* at claim 19 "According to one embodiment, the **client module includes a document-securing module** that is implemented to operate in an operating system. In particular, **the document-securing module operates in a path** through which a document being accessed would pass, as such, the document can be examined or detected for the security nature. If the document is secured, the document-securing module obtains a user or group key to decrypt the security information in the header thereof for the access rules. If a user accessing the document is determined to have the access privilege to the secured document, a file key is retrieved from the security information and **a cipher module** is activated to decrypt the encrypted data portion with the file key. Likewise, **if a document is to be secured, the cipher module encrypts clear data from the document to create the encrypted data portion**. The document-securing module integrates proper or desired security information with the encrypted data portion to produce the secured document. As the document securing module operates in an operating system, the en/decryption process is transparent to the user." *Intellectual Ventures* at col. 3:67 through col. 4:1-20

(cont.) 1.c. communicating **an authentication request to said secure file services module** over said **second secure communication path**, said secure file services module including **a file system control interface**, **a client access interface**, **a cryptographic processor** and **a secure file system hosted by said cryptographic processor**;	“Essentially, the **account manager is a database or an interface to a database** 507 (e.g., an Oracle database) **maintaining all the registered users and their respective access privileges**, and perhaps corresponding user keys (e.g., private and public keys).” *Intellectual Ventures* at col. 22:37-41 **D. US7167982** “Referring to FIG. 5, a user of client 102 **may issue a service request** 501 **to open a document**, e.g., document.enc, to server 101 **which may be received by a command interpreter** 502 in user space 401 of server 101. Command interpreter 502 may be configured to interpret the request. For a request to open a document, e.g., document.enc, **command interpreter** 502 **may be configured to transfer the request to kernel space** 402 **of server** 101. In accordance with the principles of the present invention, this request may be intercepted by a **filter driver** 503 in kernel space 402 that may be configured to filter the request. That is, filter driver 503 may be **configured to control service requests to encrypted files** as described in greater detail below.” *Lenovo* at col. 5:32-44 “In step 601, **filter driver** 503 (FIG. 5) **may receive a service request to open a document**, e.g., document.enc, **in a file system** 505 (FIG. 5) issued from a user of client 102.” *Lenovo* at col. 6:58-60
1.d. providing **an authentication of said user using said file system control interface**;	**A. US8099769** “The **secure module** 18 **may be equipped with a verification manager to identify the user using the system** 10. The **verification manager determines the access rights and privileges through passwords or biometrics**. For example, the external trusted button 26 may also be used to enter a PIN should access control to the secure module 18 be required.” *Blackberry* at col. 5:6-11 **B. US7236455** “The **trusted device** 24 **can also perform** secure data transfer and, for example, **authentication between it and a smart card via encryption/decryption and signature/verification**.” *Hewlett Packard* at col. 8:8-11

(cont.) 1.d. providing **an authentication of said user using said file system control interface**;	**C. US7681034** “In essence, the secured document 208 includes two parts, the document itself and the corresponding security information therefor, both are in encrypted form. To access the document, one needs to obtain the file key that is used to encrypt the document and is now included in the encrypted security information. **To obtain the file key, one needs to be authenticated to get a user or group key and pass an access test in which the access rules in the security information are measured against the user's access privilege**.” *Intellectual Ventures* at col. 11:50-58 “In operation, **the account manager** 508 **authenticates a user when the user logs onto the server** 500 **and also determines if the user can access secured documents** from the location the user is currently at.” *Intellectual Ventures* at col. 22:41-44 **D. US7167982** “**Filter driver** 503 **may then determine if the user** of client 102 **is authorized** to open document.enc by accessing the access control list that stores a current listing of documents with associated authorized users and applications.” *Lenovo* at col. 7:5-9
1.e. **communicating to said client access interface** over said **first secure communication path a request from said secure user processor** for **a classified data file**;	**A. US8099769** “Step 100: The **secure module** 18 **accepts data from device main processor** 16, **the data comprises the portion of the data message to be signed and may have been assembled on the personalized device** 12 or assembled externally by a external computer 14 and then conveyed to the personalized device 12; . . . .” *Blackberry* at col. 5:38-42 **B. US7236455** “14. An apparatus as claimed in claim 13, wherein: the first further hardware module is operable to supply to the trusted hardware module **a request for a transfer of data between the first and second further hardware modules**; and in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first or second further hardware module **via the first** or second **communication path**, respectively, and not via the shared communication infrastructure.” *Hewlett Packard* at claim 14

(cont.) 1.e. **communicating to said client access interface** over said **first secure communication path a request from said secure user processor** for **a classified data file**;	“A **first switching engine** 124 **is connected separately to the additional communication paths** 122 a,b,c and also to an internal communication path 126 **of the trusted module** 120.” *Hewlett Packard* at col. 14:52-55 **C. US7681034** “Essentially, **the account manager is** a database or **an interface** to a database 507 (e.g., an Oracle database) **maintaining all the registered users and their respective access privileges, and perhaps corresponding user keys** (e.g., private and public keys).” *Intellectual Ventures* at col. 22:37-41 “26. The computer readable storage medium of claim 24, wherein the program code stored on the medium, if executed, causes the application to be launched when **a request to access the file is received**.” *Intellectual Ventures* at claim 26 “30. A computer-readable storage medium having stored thereon, computer-executable instructions that, if executed by a computing device, cause **the computing device to** perform a method comprising: **determining whether the file stored in a file system and being accessed is secured**, wherein **the file includes** a header and **an encrypted portion**, the header including or pointing to security information including a file key used to decrypt the encrypted portion . . . .” *Intellectual Ventures* at claim 30 **D. US7167982** “Referring to FIG. 5, **a user** of client 102 **may issue a service request** 501 **to open a document**, e.g., document.enc, to server 101 **which may be received by a command interpreter** 502 in user space 401 of server 101. Command interpreter 502 may be configured to interpret the request. For a request to open a document, e.g., document.enc, **command interpreter** 502 **may be configured to transfer the request to kernel space** 402 **of server** 101. In accordance with the principles of the present invention, **this request may be intercepted by a filter driver** 503 in kernel space 402 that may be configured to filter the request. That is, **filter driver** 503 **may be configured to control service requests to encrypted files** as described in greater detail below.” *Lenovo* at col. 5:32-44

1.f. **responsive to said request, accessing said secure file system containing said classified data file**;	**A. US8099769** "2. The method according to claim 1 wherein said **secret key is used for verifying the integrity of a data message handled by said personalized device**." *Blackberry* at claim 2 **B. US7236455** "14. An apparatus as claimed in claim 13, wherein: the first further hardware module is operable to supply to the trusted hardware module a **request for a transfer of data** between the first and second further hardware modules; and **in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first or second further hardware module via the first or second communication path**, respectively, and not via the shared communication infrastructure." *Hewlett Packard* at claim 14 **C. US7681034** "1. A computer implemented method for securing a file, the method comprising: determining whether the **file stored in a file system and being accessed is secured**; . . . ." *Intellectual Ventures* at claim 1 **D. US7167982** "Filter driver 503 may be configured to **issue a call to file system driver** 504 **to read the encrypted data in the requested file stored in a shared area**, e.g., a shared directory on disk unit 320 of server 101, **from file system** 505. File system driver 504 may then be configured to transfer the encrypted data to filter driver 503." *Lenovo* at col. 5:56-61 "**Upon receiving the service request, the filter driver may determine if the request has been transmitted by an authorized user to open a document in an authorized application**. If the request has been transmitted by an authorized user to open a document in an authorized application, then **the filter driver may determine if the service request is a request to open an encrypted file**." *Lenovo* at col. 1:66-67 through col. 2:1-5
1.g. **decrypting said classified data file with said cryptographic processor**;	**A. US8099769** "1. A method for controlling use of a secret key in a personalized device communicatively coupled to a main processor, said personalized device adapted to receive and transmit data messages, said method comprising: . . . upon

(cont.) 1.g. **decrypting said classified data file with said cryptographic processor**;	receipt of an external input via said secure input device indicative of a favorable comparison of said first and second outputs as displayed, controlling operation of said **personalized device to obtain access to said secret key in said secure module for performing cryptographic operations**." *Blackberry* at claim 1 **B. US7236455** "Specifically, **the trusted device comprises**: a controller 30 programmed to control the overall operation of the trusted device 24, and interact with the other functions on the trusted device 24 and with the other devices on the motherboard 20; a measurement function 31 for acquiring the integrity metric from the platform 10; **a cryptographic function** 32 **for** signing, encrypting or **decrypting specified data**; . . . . " *Hewlett Packard* at col. 8:14-21 **C. US7681034** "22. The method of claim 21, wherein the activating the cipher module comprises **decrypting an encrypted portion of the file with the file key**." *Intellectual Ventures* at claim 22 "9. A computer implemented method for securing a file, the method comprising: . . . if the file is determined to be secured, **activating a cipher module, loading the file from the file system through the cipher module into an application, retrieving the file key, obtaining the user key, decrypting the security information with the user key to retrieve the file key, and decrypting the encrypted portion with the file key in the cipher module**, and sending the file in clear mode to the application; and . . . ." *Intellectual Ventures* at claim 9 **D. US7167982** "Upon receiving the encrypted data, **filter driver** 503 **may be configured to decrypt the encrypted data**. Filter driver 503 may further be configured to store the decrypted data in a file in a non-shared area, e.g., a non-shared directory on disk unit 320 of server 101. The non-shared area may be accessible only by the authorized user that requested access to the encrypted file. By storing the decrypted data in a file in the non-shared area, a file once decrypted may be protected in a file sharing environment." *Lenovo* at col. 5:62-67 through col. 6:1-3

1.h. and **communicating said classified data file to said secure user processor in decrypted form through said first secure communication path**.	**A. US8099769** “16. A system for verifying data integrity between at least two correspondents in a cryptographic scheme, said system comprising at least one of said at least two correspondents, said at least one of said at least two correspondents having a main processor and a secure module, said secure module being independently operative of said main processor, said secure module, when coupled to said personalized device, being connected via a first secure path to a secure input device and being connected via a second secure path to a secure display or secure portion of a display of said personalized device, wherein said first and second secure paths are logically isolated from said main processor, said at least one of said at least two correspondents being configured for: . . . **forwarding said data to said secure module and displaying said data from said secure module to produce a second output on said secure display or secure portion of said display of said personalized device to permit comparison of said first output and said second output**; and . . . .” *Blackberry* at claim 16 **B. US7236455** “16. An apparatus as claimed in claim 14, wherein: in response to an appropriate such transfer response, the first or second further **hardware module is operable to supply the data to the trusted hardware module via the first** or second **communication path**, respectively; and . . . .” *Hewlett Packard* at claim 16 **C. US7681034** “The encrypted security information in the header is then **decrypted with the retrieved private user key** at 536. As a result, **the access rules for this secured document are obtained** at 538.” *Intellectual Ventures* at col. 25:67 through col. 26:1-3 “The encrypted new keys are then uploaded or transmitted to the client machine at 526. Upon receiving the encrypted new keys, the client machine is caused at 528 to **decrypt the encrypted new keys to make the new user keys readily available for accessing secured documents** or securing documents.” *Intellectual Ventures* at col. 25:31-35

(cont.) 1.h. and **communicating said classified data file to said secure user processor in decrypted form through said first secure communication path**.	**D. US7167982** "**Filter driver** 503 **may then be configured to transfer the decrypted data**, i.e., decrypted file, **to the user** of client 102 **via command interpreter** 502 in user space 401." *Lenovo* at col. 6:14-17