PATROLL Winning Submission

U.S. Patent 7,779,252

U.S. Patent 7,779,252 ("*Speir Technologies Ltd*" or the "patent-at-issue") was filed on March 21, 2006 and claims priority on the same date. Claim 1 of the patent-at-issue is generally directed to a mobile PDA computer system consisting of a non-secure user processor, a secure user processor, and a cryptographic engine. The non-secure processor has a non-trusted commercial-off-the-shelf (COTS) microprocessor hardware, a non-trusted COTS operating system, and non-trusted COTS application software. The secure processor has a trusted microprocessor hardware (HW), a trusted operating system and a trusted application software. In addition to providing encryption and decryption services, the cryptographic engine provides a first data communication link that communicates data between the secure processor and the cryptographic engine and a second data communication link that communicates data between the non-secure processor and the cryptographic engine. The mobile PDA computer system includes a shared human/machine interface to allow a user to input control commands and input data, and at least one output device to allow the mobile PDA computer system to inform a user. The shared human/machine interface can be configured for bi-directional communication of information between each of the secure user processor, the non-secure user processor, and the cryptographic engine

The primary reference, U.S. Patent 7,734,933 ("*Rockwell*"), was filed on June 17, 2005 and claims priority on the same date. The patent is directed to a system for providing a trusted environment for untrusted computing systems. The system may include a HAC subsystem managing shared resources and a trusted bus switch for controlling a COTS processor to access the shared resources. The shared resources such as memory and several I/O resources reside on the trusted side of the trusted bus switch. Alternatively, the system may include a SCM as an add-on module to an untrusted host environment. Only authenticated applications including COTS OS execute on the SCM while untrusted applications execute on the untrusted host environment. The SCM may control secure resource access from the untrusted host through a plug-in module interface. All secure resources may be maintained on the trusted side of the plug-in module interface.

The primary reference, U.S. Patent 8,499,171 ("*Qualcomm*"), was filed on February 25, 2011 and claims an earliest priority date of November 18, 2005. The patent is directed to a method or providing a secure environment for mobile telephones and other devices are disclosed. The system and method may utilize trust zoning, layered memory, and a secure matrix model having, for example, a memory protection module for protecting memory; a secure debug module for ensuring security of the debug module; a secure file system module for protecting the secure file system; and a trusted time source module for protecting components. Embodiments of the present invention may protect against security attacks on a variety of hardware and software components while permitting suitable levels of accessibility for developmental and maintenance purposes.

The secondary reference, U.S. Patent 8,566,612 ("*Exelis*"), was filed on January 29, 2010 and claims an earliest priority date of October 2, 2003. The patent is directed to a security processor that performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security

processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets. A modulo engine may be coupled to the local data bus.

A sample claim chart comparing claim 1 of *Speir Technologies Ltd* to *Rockwell*, *Qualcomm*, and *Exelis* is provided below.

US7779252 (“*Speir Technologies Ltd*”)	**A. US7734933** (*“Rockwell”*) **B. US8499171** (*“Qualcomm”*) **C. US8566612** (*“Exelis”*)
1. A **mobile PDA computer system**, comprising: 1.a a **secure user processor**, comprising: a **trusted microprocessor**; a **trusted operating system executing on said trusted microprocessor**; a **trusted application software executing on said trusted microprocessor**;	**A. US7734933** “Consequently, a system suitable for highly assured military applications employing widely available and cost effective **commercial off-the-shelf (COTS)** components is necessary.” *Rockwell* at col. 1:40-42 “In an additional exemplary aspect of the present invention, a system including a **Secure Computing Module (SCM)** provides a trusted environment for COTS host platforms.” *Rockwell* at col. 2:4-6 “Moreover, **the SCM is suitable for providing secure wireless network connections when the SCM is added on** wireless devices such as **PDAs,** cell phones, and **other mobile devices**.” *Rockwell* at col. 11:53-56 “A **secure COTS computing environment** is provided by a system including a **High Assurance Controller (HAC)** subsystem to control execution of COTS functions and enforce security partitioning for applications running on the untrusted COTS processor.” *Rockwell* at col. 4:15-18 “Referring now to FIG. 7, a block diagram of a computing environment 700 implementing SCM architecture in accordance with an exemplary embodiment of the present invention is shown. The **SCM** 702 **may include** a first subsystem 703 and **a second subsystem** 704 residing on the trusted environment.” *Rockwell* at col. 8:51-56 “The first subsystem 703 may be an Authenticated COTS environment subsystem (ACE) and the **second subsystem** 704 **may be a Trusted Security Manager subsystem (TSM)** 704.” *Rockwell* at col. 8:64-67 “**The TSM** 704 **may include a trusted processor** 705 for providing a brick-wall partitioning of memory, time, and device resources, and enforcing predetermined security policies.” *Rockwell* at col. 9:31-34

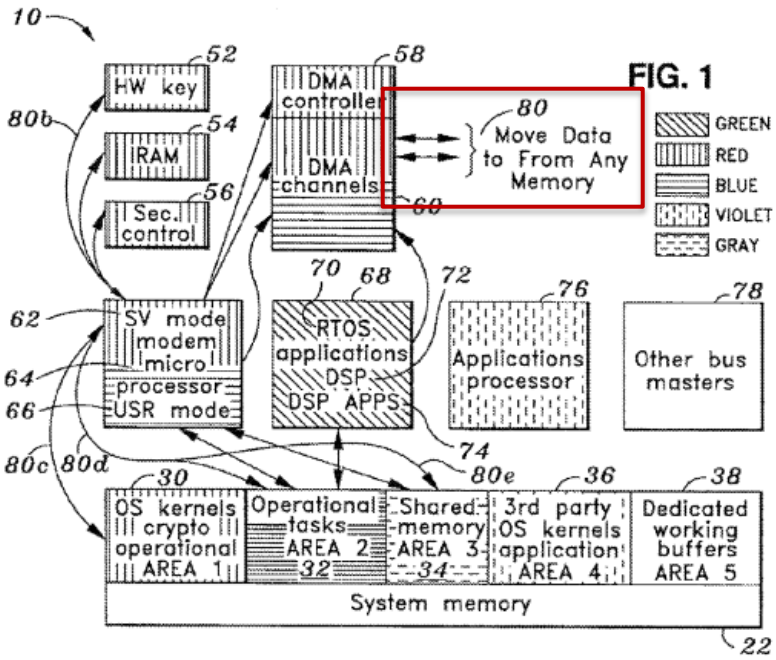
(cont.) 1. A **mobile PDA computer system**, comprising: 1.a a **secure user processor**, comprising: a **trusted microprocessor**; a **trusted operating system executing on said trusted microprocessor**; a **trusted application software executing on said trusted microprocessor**;	"In a particular embodiment of the present invention, **the trusted processor** 705 **may include ROCKWELL COLLINS AAMP7™** microprocessor and the like." *Rockwell* at col. 10:12-14 "**AAMP7 microprocessor is configured to provide intrinsic partitioning**, which allows the integration of multiple applications in a way that allows for their assured separation. As discussed above, the intrinsic partitioning mechanism operates much like a separation kernel implemented in microcode. **Rather than manage operating system tasks, however, the intrinsic partitioning mechanism maintains appropriate separation between a set of system partitions implemented directly in the microarchitecture** and associated microcode. Further, **AAMP7 may enforce a communication policy between partitions** that ensures that improper communication is not allowed, thereby providing the system designer a useful and dependable building block for designing and implementing secure systems." *Rockwell* at col. 10:14-30 **B. US8499171** "Each layer may include nested layers; for example, peripheral memory may be defined as **secure peripherals** and non-secure peripherals. Associations between various layers and various trust zones are then established to optimize functionality and security." *Qualcomm* at col. 4:43-47 "**Zone 1** (12), **for example, may be for completely trusted code** and may be the smallest possible code size. It may execute core **operating system functions** and cryptography (crypto) operations involving the hardware key or private keys from the secure file system." *Qualcomm* at col. 5:6-10 Zone 2: Application **digital signal processing (DSP) real time operating system (RTOS)** mode: trusted code and access to system memory space permitted;" *Qualcomm* at col. 4:62-64 "The **applications DSP RTOS** 70, 72 can execute any mix of **trusted** and non-trusted **applets**. To support individual access rights per applet the RTOS provides driver functionality to request memory transfers/accesses." *Qualcomm* at col. 6:10-14 **C. US8566612A** "Architecture 100 includes **security processing system** 102 **comprising security processor** 104, which may consolidate

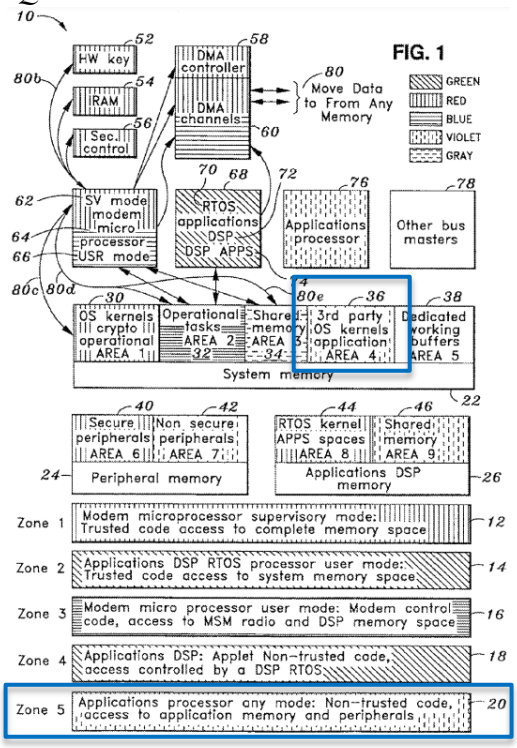
(cont.) 1. A **mobile PDA computer system**, comprising: 1.a a **secure user processor**, comprising: a **trusted microprocessor**; a **trusted operating system executing on said trusted microprocessor**; a **trusted application software executing on said trusted microprocessor**;	the processing of discrete or consolidated security functions and maintain the relationships and integrity of the stored security context and other information in memories 106, 108, and 110." *Exelis* at col. 4:4-9 "The **boot code** used to load **firmware** **for execution by security processor** 104 may optionally be authenticated using a mechanism internal to security processor 104 prior to its operation." *Exelis* at col. 7:28-32 "Each computer or computing device (not shown) connected, for example, to **internal network** 116 **may be protected by security processing system** 102, such as, for example, using an NIC containing security processing system 102 for all I/O traffic for each device." *Exelis* at col. 18:50-54
1.b a **non-secure user processor**, comprising: a **non-trusted microprocessor**; a **non-trusted operating system executing on said non-trusted microprocessor**; a **non-trusted application software executing on said non-trusted microprocessor**;	**A. US7734933** "In an additional exemplary aspect of the present invention, a system including a Secure Computing Module (SCM) provides a trusted environment for COTS host platforms." *Rockwell* at col. 2:4-6 "Referring now to FIG. 7, a block diagram of a computing environment 700 implementing SCM architecture in accordance with an exemplary embodiment of the present invention is shown. The **SCM** 702 **may include a first subsystem** 703 and a second subsystem 704 residing on the trusted environment." *Rockwell* at col. 8:51-56 "**The first subsystem** 703 **may be an Authenticated COTS environment subsystem (ACE)** and the second subsystem 704 may be a Trusted Security Manager subsystem (TSM) 704." *Rockwell* at col. 8:64-67 "This invention relates generally to computing environments and more particularly to a system for providing a secure and trusted **commercial-off-the-shelf COTS** computing environment." *Rockwell* at col. 1:8-11 "The **ACE** 703 **includes an embedded COTS OS running on a compatible embedded COTS processor**. Examples of the embedded COTS OS include WINDOWS® CE, LINUX, or PALM OS®, or the like." *Rockwell* at col. 9:4-7

(cont.) 1.b a **non-secure user processor**, comprising: a **non-trusted microprocessor**; a **non-trusted operating system executing on said non-trusted microprocessor**; a **non-trusted application software executing on said non-trusted microprocessor**;	"The **ACE** 703 **may include COTS applications**, manufacturer-supplied software and the like." *Rockwell* at col. 9:13-14 **B. US8499171** "**Zone 5** (20), for example, **may be completely untrusted**." *Qualcomm* at col. 5:23 "Specific details of this embodiment include the following interrelationships. The **application processor execution** 76 **is untrusted in any mode**. Hence the application memory management units (MMU) settings are not trusted and no assumptions are made upon their configuration; i.e., the **third-party OS** can use the application MMU freely (area 4 at 36)." *Qualcomm* at col. 6:1-6 **C. US8566612** "Security processing system 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a **host system**. Security processing system 102 may be coupled to **host processor** 130 using host bridge or interface 128. Host processor 130 may be coupled to hard drive 132, digital content input device 134, and authentication input device 136. **Hard drive** 132 **may store**, for example, **a software application** that communicates with the application program interface (API) of security processing system 102." *Exelis* at col. 5:36-46 "**By routing all or substantially all I/O to and from host processor** 130 and/or internal network 116 **through security processing system** 102, **host processor** 130 and internal network 116 **are substantially protected against unauthorized access or other security breaches, protecting the security information integrity**, and providing processing and storage efficiency from information consolidation." *Exelis* at col. 4:40-47
1.c a **cryptographic engine configured for encrypting and decrypting data comprising**: a **trusted cryptographic processor**; a **trusted operating system executing on said trusted cryptographic processor**;	**A. US7734933** "In an additional exemplary aspect of the present invention, a system including a **Secure Computing Module (SCM)** provides a trusted environment for COTS host platforms." *Rockwell* at col. 2:4-6 "Referring now to FIG. 7, a block diagram of a computing environment 700 implementing SCM architecture in accordance with an exemplary embodiment of the present

(cont.) 1.c a **cryptographic engine configured for encrypting and decrypting data comprising**: a **trusted cryptographic processor**; a **trusted operating system executing on said trusted cryptographic processor**;	invention is shown. **The SCM** 702 **may include a first subsystem** 703 **and a second subsystem** 704 **residing on the trusted environment**. The untrusted host environment may include commercial software environments and applications, having minimal or no Common Criteria (CC) certification and no assurance of isolation between tasks. Conventionally, a host platform employing COTS processors is assumed to be untrusted. The trusted environment may include trusted hardware and software ensuring access to certain resources, or parts of shared resources to be controlled in a structured manner to prevent compromising classified data. The **first subsystem** 703 **may be an Authenticated COTS environment subsystem (ACE)** and the **second subsystem** 704 **may be a Trusted Security Manager subsystem (TSM)** 704." *Rockwell* at col. 8:51-67 "The **TSM** 704 **also includes** a local encrypted storage, **a cryptographic engine** 706, and multiple I/O channels for all I/O paths to the SCM 702. The **cryptographic engine** 706 **may aid the trusted processor** 705 to provide a robust security interface. The **cryptographic engine** 706 **may include a reprogrammable cryptographic engine**." *Rockwell* at col. 9:37-42 "The **cryptographic engine** 706 of the SCM 702 **may include ROCKWELL COLLINS Janus Crypto Engine**, and the like." *Rockwell* at col. 10:31-35 **B. US8499171** "The **secure file system module** 90 **may use**, for example, **trusted software to encrypt sensitive data before storing it in external**, non-volatile memory using a device-specific hardware key 52, thus preventing security breaches of multiple devices. The on-chip memory module 92 (embedded memory) may be used to provide, for example, storage for secret information such as **cryptographic keys**, thus preventing unauthorized access to such information via probes, for example." *Qualcomm* at col. 7:27-35 "Various embodiments of the present invention may utilize security hardware 90 a to implement the hardware key 52 to facilitate the SFS. **Various embodiments also implement a cryptography engine** 90 b and DMA controller blocks 90 c used to accelerate encoding and decoding of data stored in an SFS." *Qualcomm* at col. 11:7-12

(cont.) 1.c a **cryptographic engine configured for encrypting and decrypting data comprising**: a **trusted cryptographic processor**; a **trusted operating system executing on said trusted cryptographic processor**;	**C. US8566612** "Architecture 100 includes **security processing system** 102 **comprising security processor** 104, which may consolidate the processing of discrete or consolidated security functions and maintain the relationships and integrity of the stored security context and other information in memories 106, 108, and 110. **Memories** 106, 108 **and** 110 **are coupled** to **security processor** 104. Memories 106, 108 and 110 store, for example, **cryptographic keys and other data used in security functions by security processor** 104, and also store security associations and connection entries used in maintaining multiple security sessions with other computers." *Exelis* at col. 4:4-15 "**Security processing system** 102 may also serve as a trusted hardware device to authenticate another hardware security token connected on, for example, a common network. Security processing system 102 may be authenticated using authentication input device 136 and may provide the **cryptographic processing for such authentication**." *Exelis* at col. 6:20-25 "Memory 106 may be made available to **cryptographic core** 232 to store security association and key information." *Exelis* at col. 7:16-18 "**Cryptographic cores** 232 **may provide security processing to perform**, for example, **IPSec and/or SSL processing**. Each **cryptographic core** 232 **may provide high-speed fixed function encryption** and authentication hash **processing for packet data**. Each cryptographic core 232 may receive instructions and key address information affixed to a packet for applying appropriate transforms." *Exelis* at col. 11:23-29
1.d **a first data communication link for communicating data between said secure user processor and said cryptographic engine**;	**A. US7734933** "**The TSM** 704 **also includes** a local encrypted storage, **a cryptographic engine** 706, and multiple I/O channels for all I/O paths to the SCM 702. The **cryptographic engine** 706 **may aid** the **trusted processor** 705 to provide a robust security interface." *Rockwell* at col. 9:37-42 **B. US8499171** "The aforementioned shading further correlates to the **arrows between system components** (as depicted in the legend 80),

(cont.) 1.d **a first data communication link for communicating data between said secure user processor and said cryptographic engine**;	**the arrows representing the channels in which data or code can be moved to or from areas of memory and relative to modes of operation.**" *Qualcomm* at col. 5:52-57  "In another example, a hardware key 52 may be moved in supervisory mode 62 (shown as arrow 80 b) to areas 1, 2 or 3 (shown at 30, 32, and 34 respectively) of system memory 22 as depicted by arrows 80 c, 80 d, and 80 e, respectively. In this particular embodiment, as shown in the foregoing example, **components of a certain level of trust may access memory layers having the same level of trust** or lower (less trusted zones)." *Qualcomm* at col. 5:60-67 **C. US8566612** "Also, in a preferred embodiment according to the present invention, all **I/O data to security processor** 104 **transits one of cryptographic cores** 232 whether or not the data needs encryption/decryption or other security processing." *Exelis* at col. 11:53-57
1.e a **second data communication link for communicating data between said non-secure user processor and said cryptographic engine**; and	**A. US7734933** "In an additional exemplary aspect of the present invention, a system including a **Secure Computing Module (SCM)** provides a trusted environment for COTS host platforms." *Rockwell* at col. 2:4-6 "Referring now to FIG. 7, a block diagram of a computing environment 700 implementing SCM architecture in

(cont.) 1.e a **second data communication link for communicating data between said non-secure user processor and said cryptographic engine**; and	accordance with an exemplary embodiment of the present invention is shown. The **SCM** 702 **may include a first subsystem** 703 and a second subsystem 704 residing on the trusted environment." *Rockwell* at col. 8:51-56 "**The first subsystem** 703 **may be an Authenticated COTS environment subsystem (ACE)** and **the second subsystem** 704 **may be a Trusted Security Manager subsystem (TSM)** 704." *Rockwell* at col. 8:64-67 "The **TSM** 704 **also includes** a local encrypted storage, **a cryptographic engine** 706, and multiple I/O channels for all I/O paths to the SCM 702."*Rockwell* at col. 9:37-40 "**I/O paths between the TSM** 704 **and the ACE** 703 **may include virtual I/O paths**. In an embodiment, **the virtual I/O paths** between the TSM and the ACE **may be implemented through a dual port RAM** 707, with each I/O path and a memory-mapped resource being controlled by a dedicated TSM partition." *Rockwell* at col. 9:66 through col. 10:4 **B. US8499171** "For example, the **application processor** 76 **can move data or code such as third-party OS kernels and applications to and from area 4** shown at 36, the movement depicted by arrow 80 a." *Qualcomm* at col. 5:57-60 

(cont.) 1.e a **second data communication link for communicating data between said non-secure user processor and said cryptographic engine**; and	**C. US8566612** "**Outbound packets may be buffered after transit through packet engine** 228 **and cryptographic core** 232 **for sending out to** streaming interface 200 or to **host interface** 206." *Exelis* at col. 20:22-24 "**Host interface** 206 **may be coupled to physical host bridge** 128 **and supports slow path data flow and system management by host processor** 130." *Exelis* at col. 6:48-51
1.f a **shared human/machine interface comprising a digital multiplexer that is exclusively responsive to said cryptographic engine for selectively enabling exclusive bi-directional communication of information between a user and one of said secure user processor, said non-secure user processor and said cryptographic engine**; and	**B. US8499171** "Zone 2 (14), for example, may be for completely trusted code and may **control the access rights of individual applications DSP applets**." *Qualcomm* at col. 5:11-13 "Zone 4 (18), for example, may be trusted for certain address ranges depending on the applet. Zone 2 (RTOS) may be responsible for **determining the access rights of Zone 4.**" *Qualcomm* at col. 5:20-22 "In various embodiments, the memory protection module 84 may protect main memory 84 a, for example, via one or more combined actions associated with the following memory protection elements: a predetermined number of main memory protection units (MPU) blocks; for example, three; **modem processor memory management unit (MMU)**; modem subsystem **secure mode multiplexer (SMM)** block; applications **digital signal processor (applications DSP 72)** MPU; DMA controller security features (embedded MPU, shadow registers, security identification (ID)); **general purpose input/output expansion interface (GPIO)** security features (shadow registers, bitmasks); and Main Memory MPU blocks." *Qualcomm* at col. 7:63-67 through col. 8:1-8 "The **RTOS is trusted to identify access rights per applet and configure** the assigned DMA controller channel's 60 MPU accordingly. Separate Memory Protection Units (MPUs) are used to protect Zones 1 to 4 from invalid accesses from other zones (such as one or more of Zones 3, 4 and 5) since the application MMU is not trusted." *Qualcomm* at col. 6:14-19 "**The applications DSP** 72 MPU **may prevent applications DSP applications, such as those Zone** 4, **from accessing various registers**, thus the applications must issue RTOS

(cont.) 1.f a **shared human/machine interface comprising a digital multiplexer that is exclusively responsive to said cryptographic engine for selectively enabling exclusive bi-directional communication of information between a user and one of said secure user processor, said non-secure user processor and said cryptographic engine**; and	system calls to perform memory access." *Qualcomm* at col. 8:23-26 "Applications DSP 72 may run multitasking RTOS 70 that may be trusted and might always run in privileged mode. The DSP 72 may **execute applications using up to, for example**, 32 **user mode execution threads**. Some applications are not trusted." *Qualcomm* at col. 13:24-27 **C. US8566612** "**Authentication input device** 136 may be, for example, a physical key or token, a smart card, or a biometric identification sensor. **Authentication input device** 136 **may enable the authentication of a user attempting to access host processor** 130. Authentication input device 136 may be directly attached, for example, to a serial, network, or EEPROM interface of host processor 130 using a physically segregated or covered transmission channel. **Authentication input device** 136 **may act as a mechanism for enabling or modifying the functions of security processor** 104, **or as an information-loading mechanism, used for example in loading keys, uncovering keys, or modifying rules for device operation**. **Digital content input device** 134 **may be, for example, a CD-ROM, portable storage device, or keyboard and provides digital data such as program code or security data to host processor** 130." *Exelis* at col. 5:56-57 through col. 6:1-4

1.g a **third data communication link for communicating control information between said cryptographic engine to said shared human/machine interface**;	**B. US8499171** "The applications DSP RTOS 70, 72 can execute any mix of trusted and non-trusted applets. To support individual **access rights per applet the RTOS provides driver functionality to request memory transfers/accesses**. The RTOS is trusted to identify **access rights per applet** and configure the assigned DMA controller channel's 60 MPU accordingly." *Qualcomm* at col. 6:10-16 **C. US8566612** "**Authentication input device** 136 **may be directly attached, for example, to a serial, network, or EEPROM interface of host processor** 130 using a physically segregated or covered transmission channel. **Authentication input device** 136 **may act as a mechanism for enabling or modifying the functions of security processor** 104, **or as an information-loading mechanism, used for example in loading keys, uncovering keys, or modifying rules for device operation**." *Exelis* at col. 5:60-67 "Security processing system 102 may also serve as a trusted hardware device to authenticate another hardware security token connected on, for example, a common network. **Security processing system** 102 **may be authenticated using authentication input device** 136 **and may provide the cryptographic processing for such authentication**. **Security processing system** 102 **may communicate verification or other information regarding the authentication status of input device** 136 **to host processor** 130." *Exelis* at col. 6:20-28 "By routing all or substantially all **I/O to and from host processor** 130 and/or internal network 116 **through security processing system** 102, host processor 130 and internal network 116 are substantially protected against unauthorized access or other security breaches, protecting the security information integrity, and providing processing and storage efficiency from information consolidation." *Exelis* at 4:40-47 "**Security processing system** 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a host system. **Security processing system** 102 **may be coupled to host processor** 130 **using host bridge or interface** 128." *Exelis* at col. 5:37-42

1.h.i wherein said **non-secure user processor is operatively connected to a communications transceiver, said secure processor is configured to utilize said non-secure processor to exchange information with said communications transceiver**,	**A. US7734933** "The SCM may be connected as a USB, CF, or Personal Computer Memory Card International Association (PCMCIA) device for a laptop host platform. Moreover, the SCM is suitable for providing secure wireless network connections when the **SCM is added on wireless devices such as PDAs, cell phones, and other mobile devices**." *Rockwell* at col. 11:50-56 "The **TSM** 704 also includes a local encrypted storage, a cryptographic engine 706, and **multiple I/O channels for all I/O paths to the SCM** 702." *Rockwell* at col. 9:37-40 "In an additional exemplary aspect of the present invention, a system including a **Secure Computing Module (SCM)** provides a trusted environment for COTS host platforms." *Rockwell* at col. 2:4-6 "Referring now to FIG. 7, a block diagram of a computing environment 700 implementing SCM architecture in accordance with an exemplary embodiment of the present invention is shown. The **SCM** 702 **may include** a first subsystem 703 and **a second subsystem** 704 residing on the trusted environment." *Rockwell* at col. 8:51-56 "The first subsystem 703 may be an Authenticated COTS environment subsystem (ACE) and **the second subsystem** 704 **may be a Trusted Security Manager subsystem (TSM)** 704." *Rockwell* at col. 8:64-67 **B. US8499171** "**Zone 3 (16), for example, may permit trusted access to the radio control registers** while in modem supervisory mode, and may contain all of the core control code such as Code Division Multiple Access (CDMA), **global system for mobile communications (GSM); and universal mobile telecommunications service (UMTS)**." *Qualcomm* at col. 5:14-19

1.h.ii and said **cryptographic engine is further configured** **to command said shared human/machine interface to delete sensitive information contained therein and** to **command said digital multiplexer to connect to said non-secure user processor only after said sensitive information has been deleted from said shared human/machine interface**.	**A. US7734933** "A secure COTS computing environment is provided by a system including a **High Assurance Controller (HAC) subsystem to control execution of COTS functions and enforce security partitioning for applications running on the untrusted COTS processor**." *Rockwell* at col. 4:15-19 "The HAC subsystem 312 is responsible for control of COTS CPU execution as well as enforcing access to shared resources 313 such as memory and I/O. The HAC subsystem 312 may monitor and manage partitions for the COTS CPU. The **HAC subsystem** 312 **is responsible for zeroizing, loading, configuring, and controlling the COTS CPU for time-sliced real time execution of Multiple Independent Level of Security (MILS) computing functions**. **Zeroizing the COTS CPU may include approved zeroization procedures configured to erase sensitive information (e.g. keys for a cryptographic module) or decrypted secure data to prevent its disclosure**." *Rockwell* at col. 5:5-13 "As a result, the COTS CPU is ready to execute a next scheduled computing function. For example, a first computing function at TS security level may be executed in a first time slice 316. **Before a second computing function at security level being executed in a second time slice** 320, **a processing partition for the first computing function may be "scrubbed" by the HAC subsystem** 312. **The HAC subsystem** 312 **causes the COTS CPU to zeroize its internal states and reestablish the PMU state**. **Then, the COTS CPU** 302 **is ready for executing the second computing function in the second time slice** 320." *Rockwell* at col. 6:4-14 "Each micro-fob may be coded to the corresponding SCM device that it protects. If the signal is lost for a preset amount of time, **the SCM device may** lock out user access or **start auto-zeroizing**." *Rockwell* at col. 12:67 through col. 13:1-4