US 20130080791A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2013/0080791 A1

(43) Pub. Date: Mar. 28, 2013

Brizek

(54) SECURITY PROTOCOLS FOR PROCESSOR-BASED SYSTEMS

(71) Applicant: **John P. Brizek**, Placerville, CA (US)

(72) Inventor: **John P. Brizek**, Placerville, CA (US)

(21) Appl. No.: **13/662,986**

(22) Filed: **Oct. 29, 2012**

Related U.S. Application Data

(63) Continuation of application No. 13/021,880, filed on Feb. 7, 2011, now Pat. No. 8,352,748, which is a continuation of application No. 10/105,201, filed on Mar. 25, 2002, now Pat. No. 7,900,054.

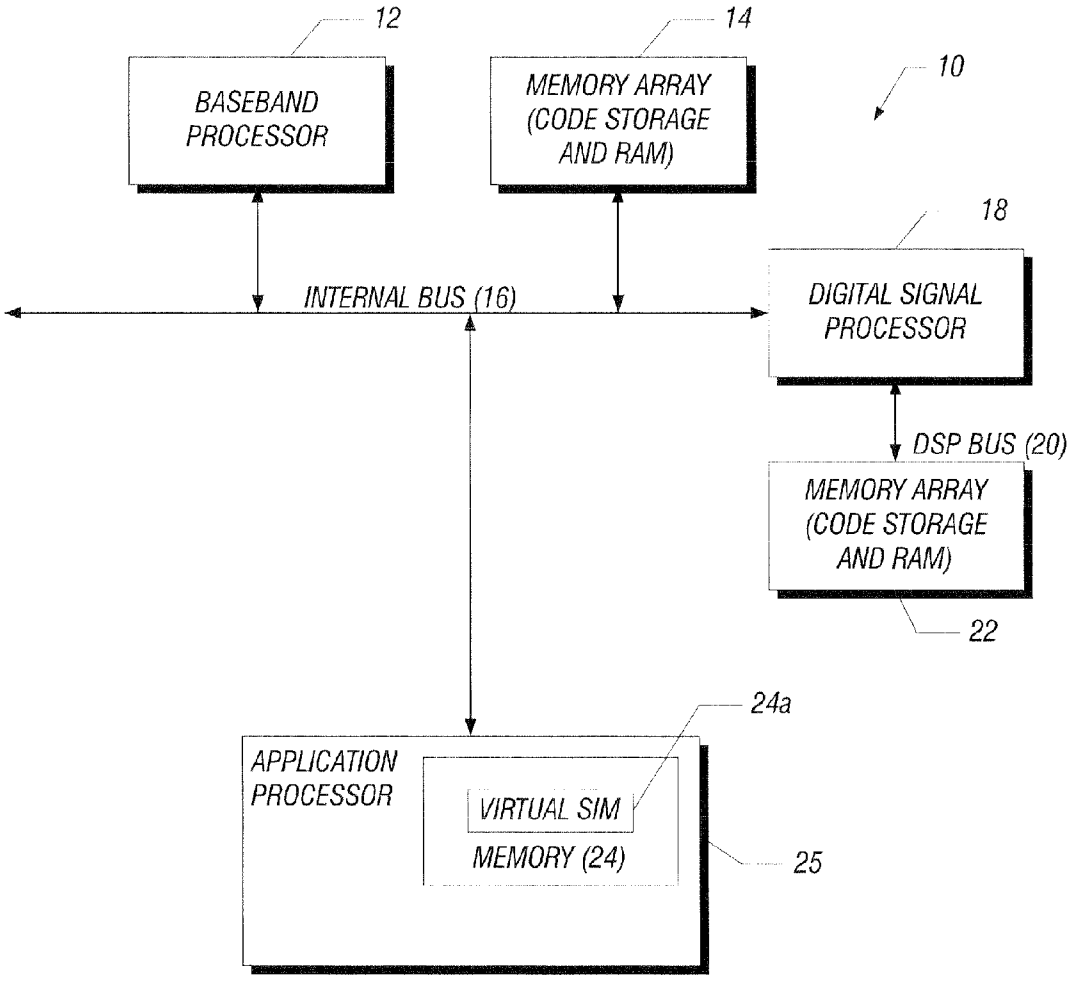
Publication Classification

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.**
USPC **713/190**

(57) **ABSTRACT**

A processor-based system such as a wireless communication module may implement security functions in a cost effective fashion by providing a virtual memory space whose addresses may be recognized. The memory is integrated with an application processor. When those addresses are recognized, access to special security protocols may be allowed. In another embodiment, a variety of dedicated hardware cryptographic accelerators may be provided to implement security protocols in accordance with a variety of different standards. By optimizing the hardware for specific standards, greater performance may be achieved.



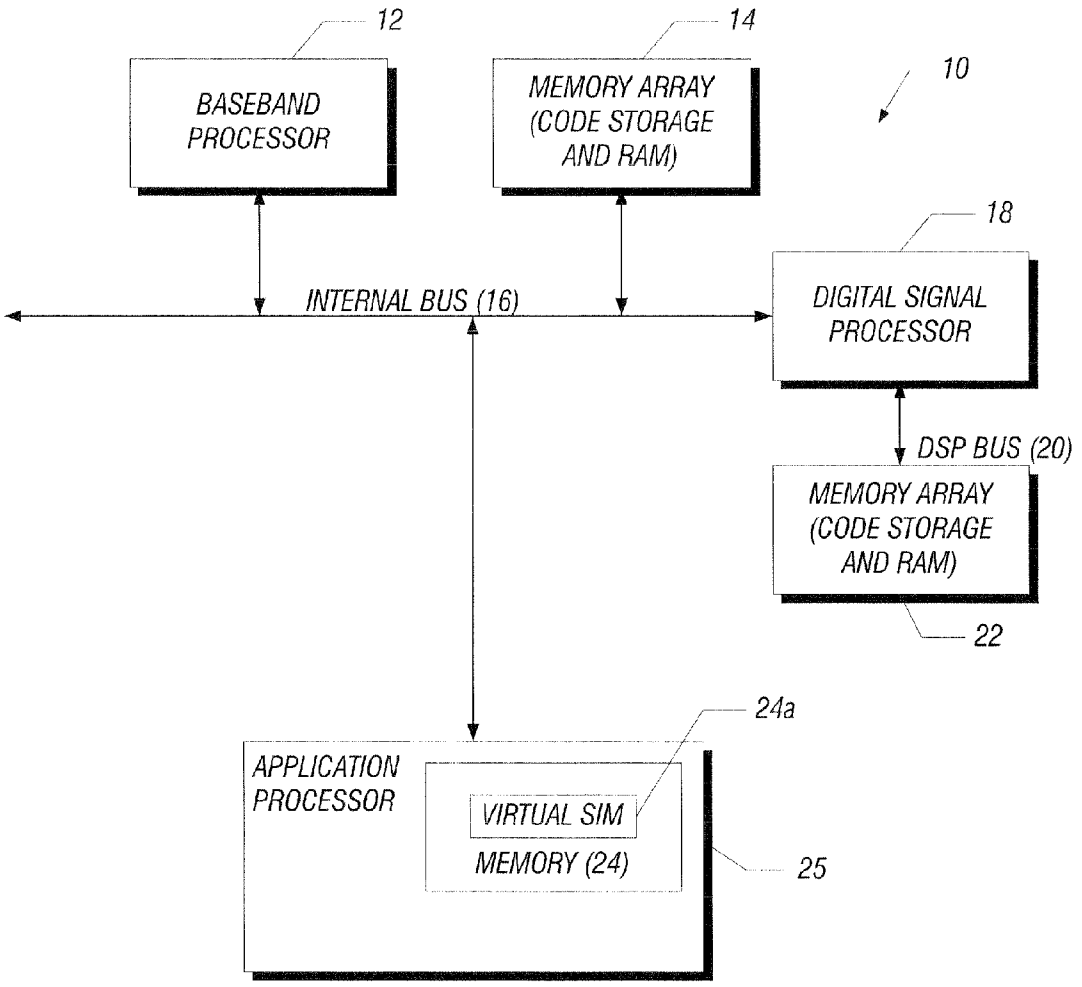

12
14
10
BASEBAND PROCESSOR
MEMORY ARRAY (CODE STORAGE AND RAM)
18
INTERNAL BUS (16)
DIGITAL SIGNAL PROCESSOR
DSP BUS (20)
MEMORY ARRAY (CODE STORAGE AND RAM)
22
24a
APPLICATION PROCESSOR
VIRTUAL SIM
MEMORY (24)
25

FIG. 1

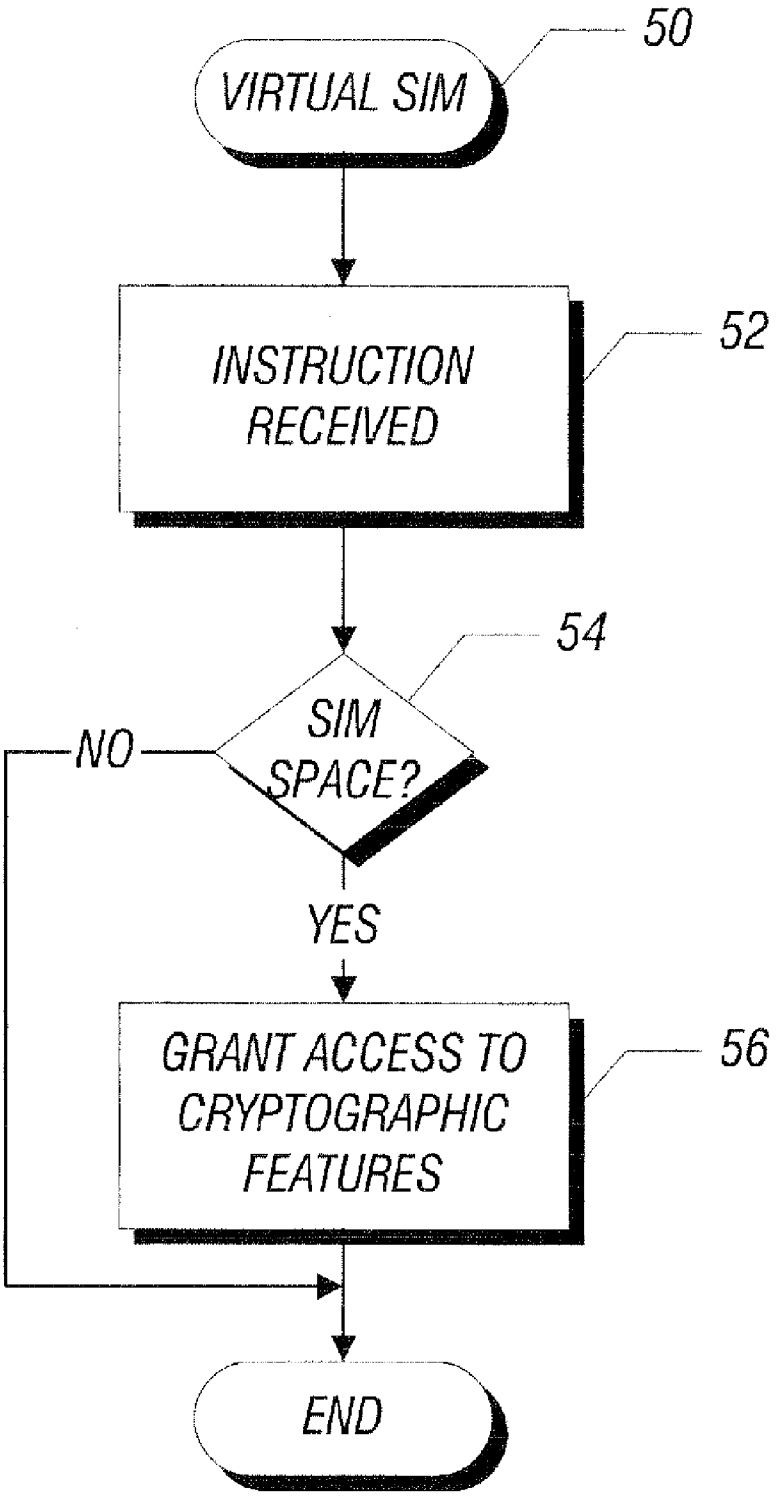

50
VIRTUAL SIM
INSTRUCTION RECEIVED
52
54
SIM SPACE?
NO
YES
GRANT ACCESS TO CRYPTOGRAPHIC FEATURES
56
END

FIG. 2

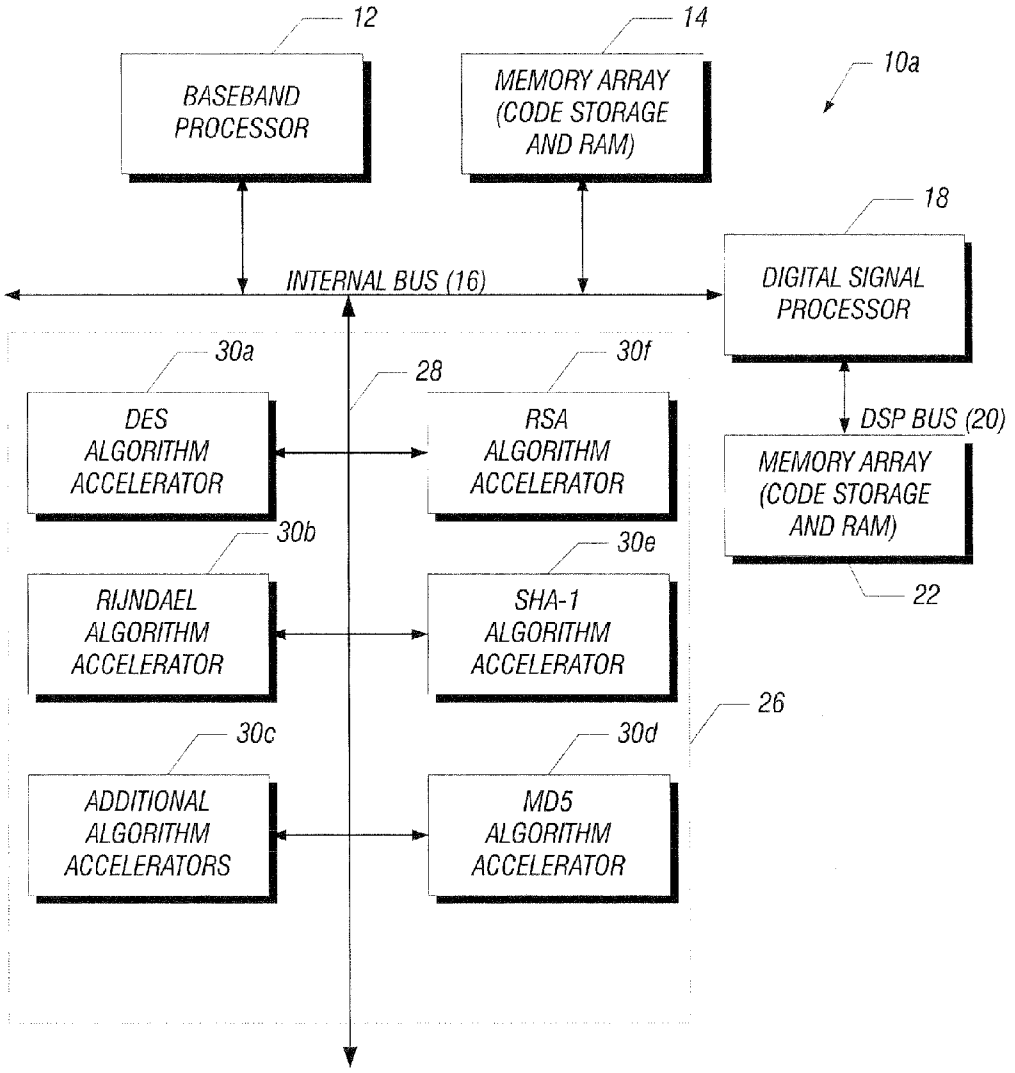

12
BASEBAND PROCESSOR
14
MEMORY ARRAY (CODE STORAGE AND RAM)
10a
18
DIGITAL SIGNAL PROCESSOR
INTERNAL BUS (16)
DSP BUS (20)
MEMORY ARRAY (CODE STORAGE AND RAM)
22
28
30a
DES ALGORITHM ACCELERATOR
30f
RSA ALGORITHM ACCELERATOR
30b
RIJNDAEL ALGORITHM ACCELERATOR
30e
SHA-1 ALGORITHM ACCELERATOR
26
30c
ADDITIONAL ALGORITHM ACCELERATORS
30d
MD5 ALGORITHM ACCELERATOR

FIG. 3

SECURITY PROTOCOLS FOR PROCESSOR-BASED SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 13/021,880 filed on Feb. 7, 2011, which is a continuation of U.S. patent application Ser. No. 10/105,201, filed on Mar. 25, 2002 which issued as U.S. Pat. No. 7,900,054.

BACKGROUND

[0002] This invention relates generally to processor-based systems and, in particular embodiments, to processor-based systems capable of implementing wireless communications.

[0003] Wireless communications may be implemented by cellular telephones as well as networked devices that use wireless protocols. A processor-based system then communicates with other systems using an appropriate wireless protocol.

[0004] A number of security procedures may be implemented to enable secure communications between two stations. In addition, it may be necessary to authenticate a given communicator to insure that the communicator is authorized to use the network such as a wireless telephone system.

[0005] Conventionally, security may be implemented through a dedicated module or plug-in card that includes its own separate processor-based system including a processor and memory. Conventionally called subscriber identity modules (SIMs), these processor-based systems function relatively independently of the system in which they are embedded. They provide access to secure data such as a subscriber's identity. This data control is enforced by an onboard processor.

[0006] The use of a removable SIM is a relatively high cost approach. The dedicated SIM adds significantly to the cost of the electronic system that it serves to protect.

[0007] Software techniques may also be used to provide security in electronic devices. Software only security solutions are subject to compromise from coding errors, viruses, and hacker attacks.

[0008] Thus, purely hardware approaches may be subject to some deficiencies in terms of cost and purely software approaches may be subject to deficiencies in terms of effectiveness.

[0009] Thus, there is a need for better ways to implement security protocols in processor-based systems, and in particular, those systems utilized for wireless communications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** is a schematic depiction of one embodiment of the present invention;

[0011] FIG. **2** is a flow chart for one embodiment of the present invention; and

[0012] FIG. **3** is a schematic depiction of another embodiment of the present invention.

DETAILED DESCRIPTION

[0013] Referring to FIG. **1**, a processor-based system **10** may be implemented, in one embodiment, as a wireless communication device. Two examples of such wireless communication devices include cellular telephones and networked devices, which communicate by a radio frequency signal.

[0014] An internal bus **16** couples a baseband processor **12** to a memory array **14**. A digital signal processor **18** is also coupled to the bus **16** in one embodiment. In one embodiment, the digital signal processor **18** may include its own memory array **22** coupled to the processor **18** via a bus **20**.

[0015] In one embodiment, a subscriber identity module is not utilized and instead, the security functions normally implemented through a subscriber identity module may be embedded within an application processor **25**. Thus, a single integrated circuit may accomplish an application processing function and a subscriber identity module (SIM) function.

[0016] In general, an application processor **25** handles applications not directly involved in baseband operations. The application processor **25** may have embedded storage **24** that may include a virtual SIM **24***a* that may be a range of addresses dedicated to the SIM functions. In some embodiments, other components such as the baseband processor **12** may be integrated with the application processor **25**. Thus, in some embodiments, the virtual subscriber identity module **24** includes an access-restricted, dedicated range of addresses in a memory space **24**.

[0017] In some cases, the virtual SIM **24***a* may store software that implements user authentication, digital signatures, and the security protocols for mobile commerce transactions as well as implementing the SIM functions. In some cases, dedicated hardware or a control logic may be used with the virtual SIM **24***a* and in other cases, the application processor **25** may control the virtual SIM **24***a*.

[0018] By integrating the virtual SIM **24** with the application processor **25**, the ability to hack or corrupt the SIM functions may be reduced. In addition, the overall system **10** may be made in smaller sizes and have reduced power consumption in some embodiments.

[0019] In some cases, the memory **24** may be formed of a nonvolatile memory such as flash memory. In other cases, a volatile memory such as random access memory may be used together with a battery. In any case, the virtual SIM **24***a* address range within the memory **24** is physically integrated with the application processor **25**. In such case, the application processor **25** may service the virtual SIM **24***a* as it does the rest of the memory **24**. Access to the virtual SIM **24***a* may be controlled so that only certain applications can access the address range represented by the virtual SIM **24***a*.

[0020] Referring to FIG. **2**, the virtual SIM software **50** implements the virtual subscriber identity module functions. In short, the software **50** identifies particular instructions as bearing on particular addresses. If those addresses correspond to the space dedicated for security protocols, special privileges may be granted. In all other cases, access to security protocols may be precluded.

[0021] When an instruction is received as indicated at block **52**, it is checked as indicated in diamond **54** to see if it relates to addresses in the dedicated virtual SIM space **25**. If so, access may be granted for the instruction to various cryptographic features as indicated in block **56**. Otherwise access privileges are not provided.

[0022] In some cases, the access to the security privileges may be implemented by providing an appropriate code word to the instruction. In other cases, the instruction may be allowed to access various hardware and software features of the system **10** to implement cryptographic functions.

[0023] Thus, in some embodiments, both secure and non-secure processes may utilize the same processing hardware, such as the baseband processor **12** and digital signal proces-

sor **18**. If, in some embodiments, the virtual SIM implementation is not wholly software based it may not require dedicated hardware and as a result may be a more cost effective solution.

[0024] Referring to FIG. **3**, another processor-based system **10***a* may include a baseband processor **12**, a memory array **14**, an internal bus **16**, a digital signal processor **18**, a digital signal processor bus **20**, and a memory array **22** in some embodiments. Coupled to the internal bus **16** is an array of hardware cryptographic accelerators **26**. For example, a Data Encryption Standard (DES) algorithm accelerator **30***a* (See National Bureau of Standards NBS FIPS PUB 46, "Data Encryption Standard", National Bureau of Standards, U.S. Dept. of Commerce, January 1977), an Advanced Encryption Standard (AES) (See J. Daemen, V. Rigmen, "The Block Cipher Rijndael," Smart Card Research and Applications, LNCS 1820, J. -J. Quisquater and B. Schneier, Eds., Springer-Verlag, 2000, pp. 286-296) or Rijndael algorithm accelerator **30***b*, a RSA algorithm accelerator **30***f* (See R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" Communications of the ACM, v. 21, n. 2, February 1978, pp. 120-6.), a Securing Hash Algorithm, (SHA-1) accelerator **30***e* (See National Bureau of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard" U.S. Department of Commerce, May 1994), a Message Digest 5 (MD5) algorithm accelerator **30***d* (See R. L. Rivest, "The MD5 Message Digest Algorithm", RFC 1320, April 1992) may be included as well as additional algorithm accelerators **30***c*. Thus, the array **26** may include a wide variety of hardware based security algorithm accelerators including one way hash function (SHA-land MD5). The system may use the virtual subscriber identity module **25** described with respect to the previous embodiments as well.

[0025] Because each accelerator **30** in the array **26** is dedicated to a special purpose, its performance for a particular standard may be optimized. The control of each accelerator in the array **26** may be controlled by one of the processors **12** or **18**. In some embodiments, the array **26** may be integrated on a single integrated circuit.

[0026] Using symmetric, asymmetric, hashing and privacy algorithms, a variety of security protocols can be serviced by the array **26** of accelerators **30**.

[0027] While the present invention has been described with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of this present invention.

What is claimed is:

1. An apparatus comprising:

a processor, said processor to execute first and second code sequences, said processor including a storage having a virtual memory space and said processor adapted to detect instructions directed to addresses associated with said virtual memory space, to identify which of said first and second code sequences issued said instructions to an address associated with said virtual memory space and to allow the first code sequence that issued instructions to said address but not the second code sequence that did not issue instructions to said address, access to a resource; and

a memory coupled to said processor.

2. The apparatus of claim **1** wherein said apparatus detects instructions directed to said memory space by comparing the addresses of said instructions to the addresses corresponding to said virtual memory space.

3. The apparatus of claim **1** wherein said apparatus only allows instructions directed to said memory space to access cryptographic functions.

4. The apparatus of claim **1** wherein said resource including a plurality of cryptographic accelerators each for different cryptographic techniques.

5. The apparatus of claim **4** including a data encryption standard algorithm accelerator.

6. The apparatus of claim **5** including a Rijndael algorithm accelerator.

7. The apparatus of claim **5** including at least three different hardware cryptographic algorithm accelerators..

8. The apparatus of claim **7** including an integrated circuit including all of said cryptographic accelerators.

9. The apparatus of claim **1** wherein said resource to implement a security protocol to accomplish a subscriber identity module function.

10. The apparatus of claim **1** wherein said apparatus is a cellular telephone.

11. The apparatus of claim **1** wherein said processor is an application processor and said code sequences are applications.

12. The apparatus of claim **11** wherein said apparatus is a cellular telephone.

13. The apparatus of claim **12** including a die containing said application processor wherein said function is implemented on said die.

14. The apparatus of claim **12** wherein said function and said processor are on the same die.

15. The apparatus of claim **12** wherein said function is integrated with an application processor.

16. The apparatus of claim **12** wherein the function is integrated as a portion of the application processor.

17. A method comprising:

integrating a processor with a storage having a virtual memory space associated with a particular address;

detecting instructions directed to said address associated with said virtual memory space;

detecting whether a first or a second code sequence is directing instructions to access said address; and

granting access to the first code sequence that directed instructions to said address access to a resource and denying access to the second code sequence that did not direct instructions to said address.

18. The method of claim **17** including assigning an address range to said virtual memory space.

19. The method of claim **17** including detecting instructions directed to said memory space by comparing the addresses of said instructions to the addresses corresponding to said virtual memory space.

20. The method of claim **17** including allowing only instructions addressed to said memory space to access a resource including cryptographic functions.

21. The method of claim **20** including providing separate cryptographic accelerators for a plurality of cryptographic techniques.

22. The method of claim **21** including providing a data encryption standard algorithm accelerator.

23. The method of claim **22** including providing a Rijndael algorithm accelerator.

24. The method of claim **21** including providing at least three different hardware cryptographic algorithm accelerators.

25. The method of claim **24** including providing said cryptographic accelerators on the same integrated circuit.

26. The method of claim **17** including using said virtual memory space to implement a subscriber identity module function.

* * * * *