US 20120238206A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2012/0238206 A1**

(43) **Pub. Date: Sep. 20, 2012**

Singh et al.

(54) **COMMUNICATIONS DEVICE PROVIDING NEAR FIELD COMMUNICATION (NFC) SECURE ELEMENT DISABLING FEATURES RELATED METHODS**

(75) Inventors: **Ravi Singh**, Toronto (CA); **Neil Patrick Adams**, Kitchener (CA); **Kristof Takacs**, Waterloo (CA); **Shivangi Anantrupa Gandhi**, Brampton (CA)

(73) Assignee: **Research In Motion Limited**, Waterloo (CA)

(21) Appl. No.: **13/157,685**

(22) Filed: **Jun. 10, 2011**

Related U.S. Application Data

(60) Provisional application No. 61/452,511, filed on Mar. 14, 2011.

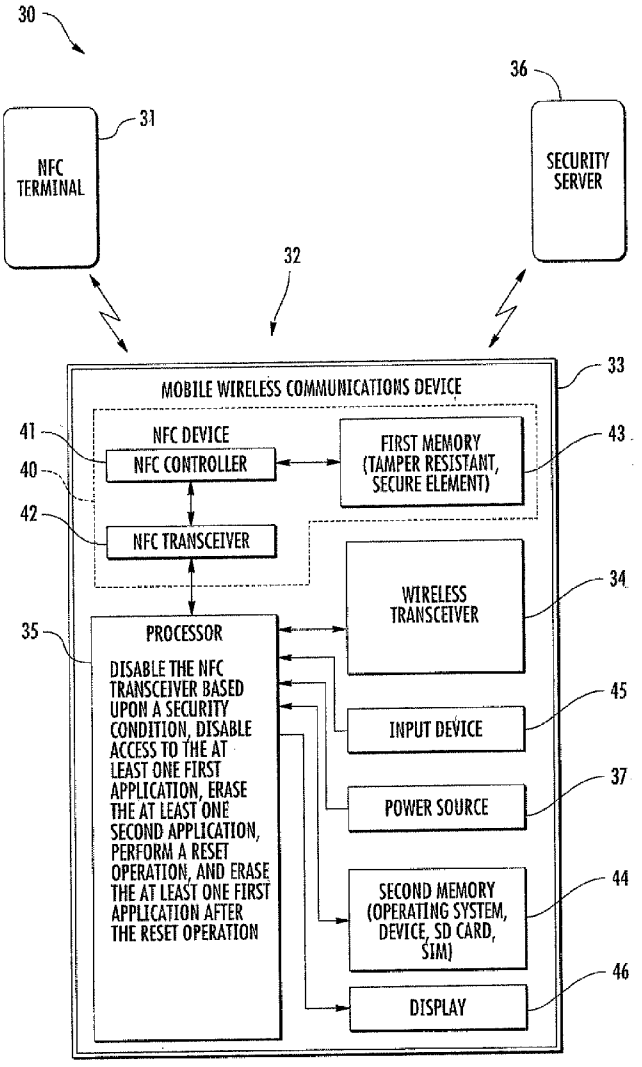
Publication Classification

(51) **Int. Cl.**
H04B 5/00 (2006.01)

(52) **U.S. Cl.** **455/41.1**

(57) **ABSTRACT**

A communications device may include a near field communication (NFC) device, at least one memory configured to store secure application data to be communicated via the NFC device and a secure element (SE) application programming interface (API) associated with the secure application data, and a processor coupled with the NFC device and the at least one memory. The processor may be configured to disable the SE API to prevent access to the secure application data based upon a security condition, and enable the SE API to allow access to the secure application data based upon a security restore event.



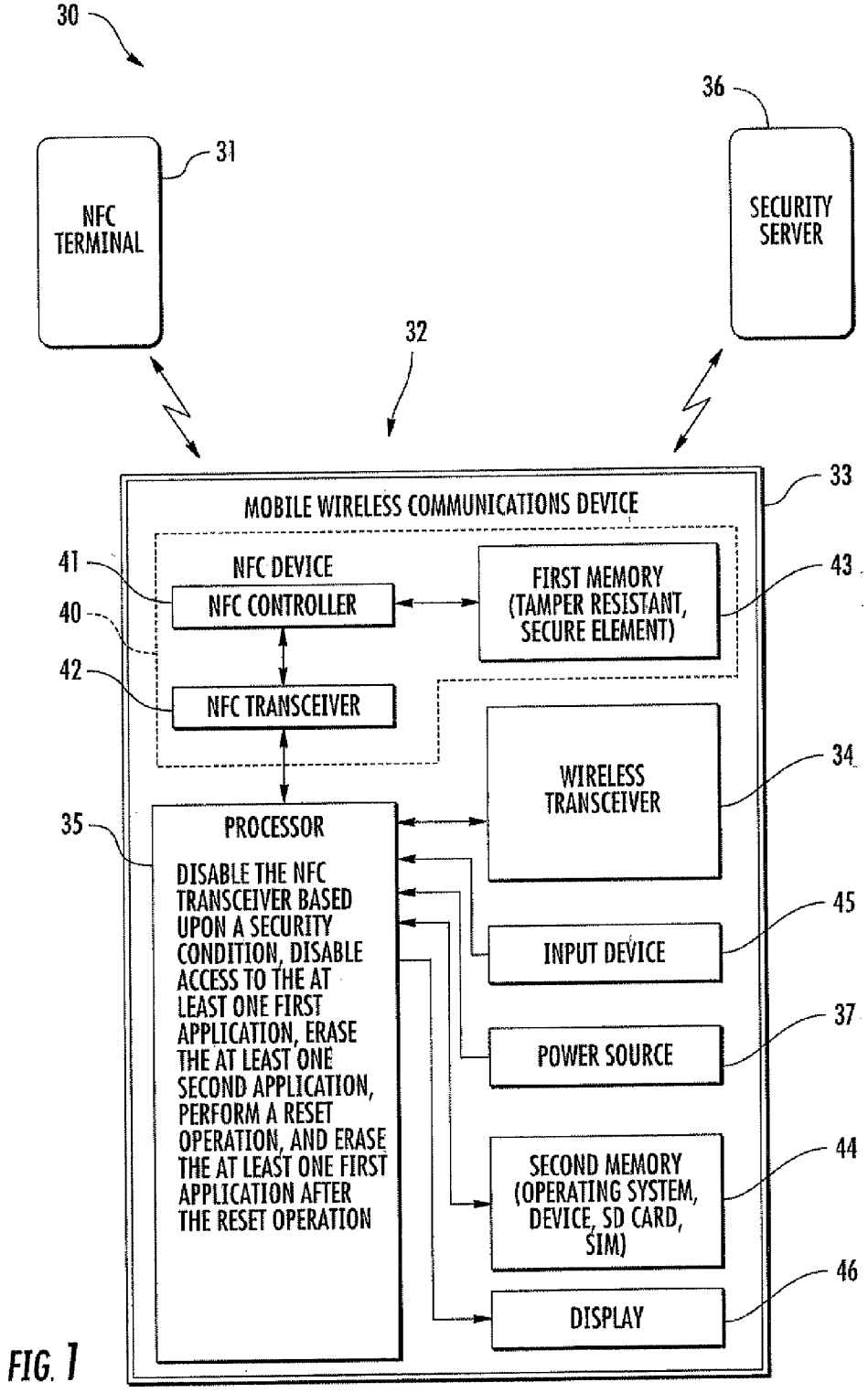

30
36
31
NFC TERMINAL
SECURITY SERVER
32
33
MOBILE WIRELESS COMMUNICATIONS DEVICE
41
NFC DEVICE
NFC CONTROLLER
FIRST MEMORY (TAMPER RESISTANT, SECURE ELEMENT)
43
40
42
NFC TRANSCEIVER
WIRELESS TRANSCEIVER
34
35
PROCESSOR
DISABLE THE NFC TRANSCEIVER BASED UPON A SECURITY CONDITION, DISABLE ACCESS TO THE AT LEAST ONE FIRST APPLICATION, ERASE THE AT LEAST ONE SECOND APPLICATION, PERFORM A RESET OPERATION, AND ERASE THE AT LEAST ONE FIRST APPLICATION AFTER THE RESET OPERATION
45
INPUT DEVICE
37
POWER SOURCE
SECOND MEMORY (OPERATING SYSTEM, DEVICE, SD CARD, SIM)
44
46
DISPLAY

FIG. 1

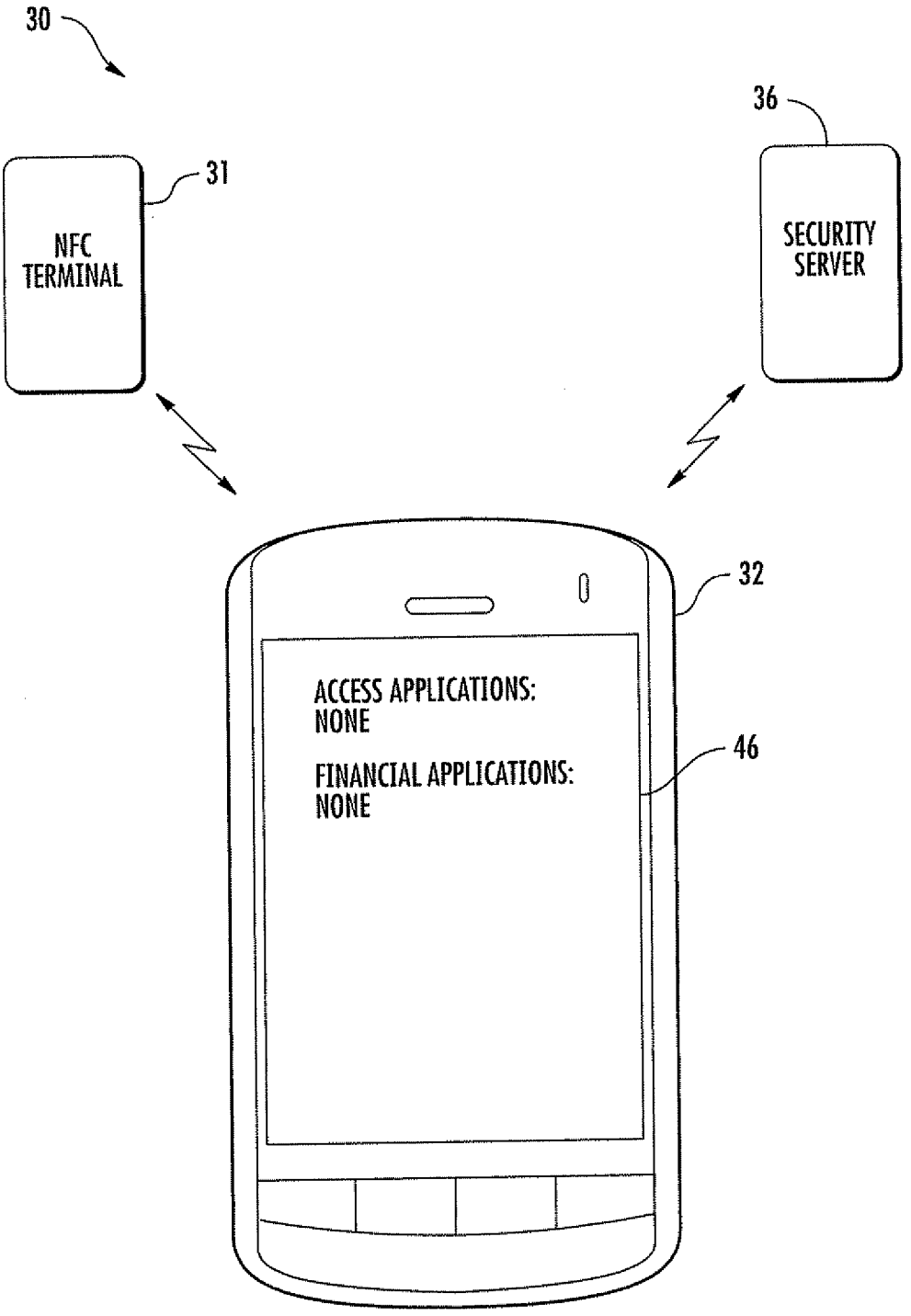

30
31
NFC TERMINAL
36
SECURITY SERVER
32
ACCESS APPLICATIONS: NONE
FINANCIAL APPLICATIONS: NONE
46

FIG. 2

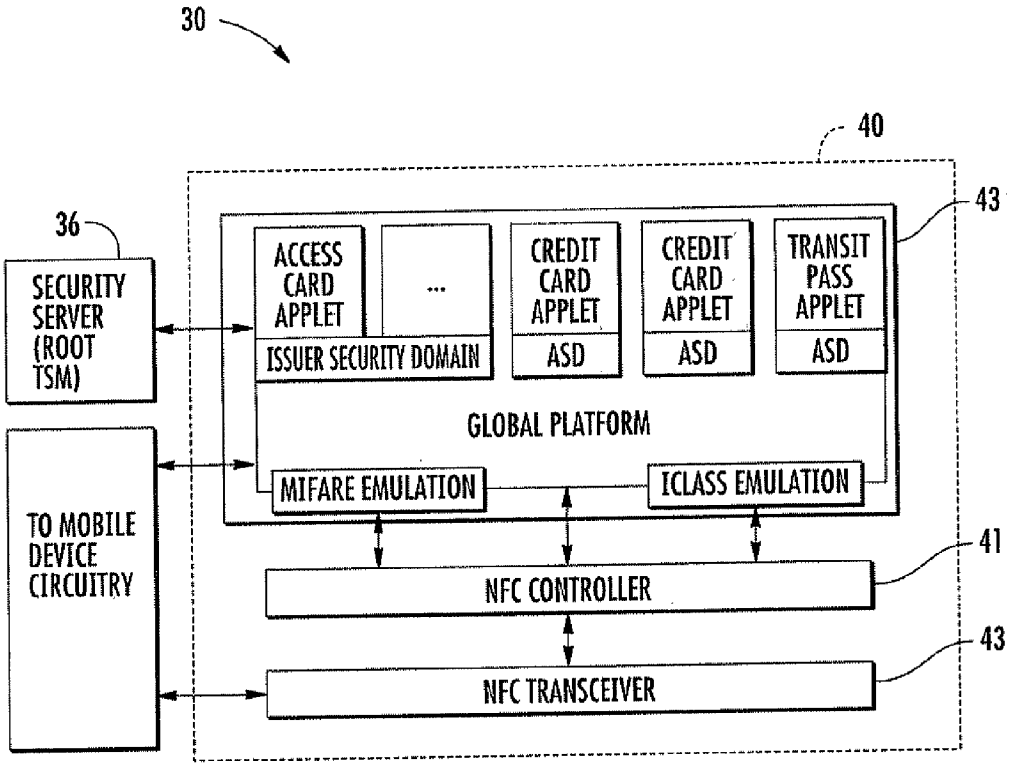

30
40
36
SECURITY SERVER (ROOT TSM)
TO MOBILE DEVICE CIRCUITRY
ACCESS CARD APPLET
...
ISSUER SECURITY DOMAIN
CREDIT CARD APPLET
ASD
CREDIT CARD APPLET
ASD
TRANSIT PASS APPLET
ASD
43
GLOBAL PLATFORM
MIFARE EMULATION
ICLASS EMULATION
41
NFC CONTROLLER
43
NFC TRANSCEIVER

FIG. 3

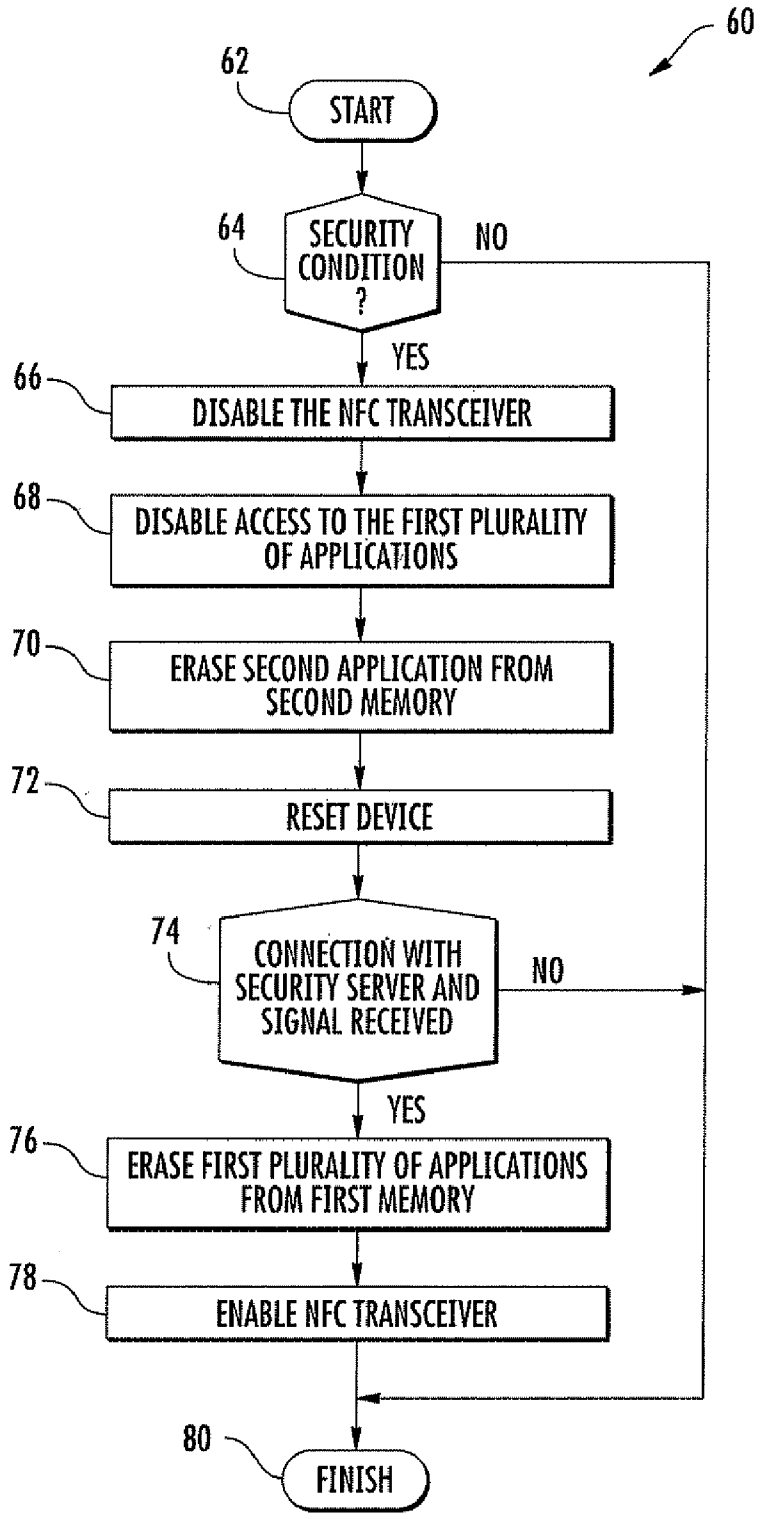

60
62
START
64
SECURITY CONDITION ?
NO
YES
66
DISABLE THE NFC TRANSCEIVER
68
DISABLE ACCESS TO THE FIRST PLURALITY OF APPLICATIONS
70
ERASE SECOND APPLICATION FROM SECOND MEMORY
72
RESET DEVICE
74
CONNECTION WITH SECURITY SERVER AND SIGNAL RECEIVED
NO
YES
76
ERASE FIRST PLURALITY OF APPLICATIONS FROM FIRST MEMORY
78
ENABLE NFC TRANSCEIVER
80
FINISH

FIG. 4

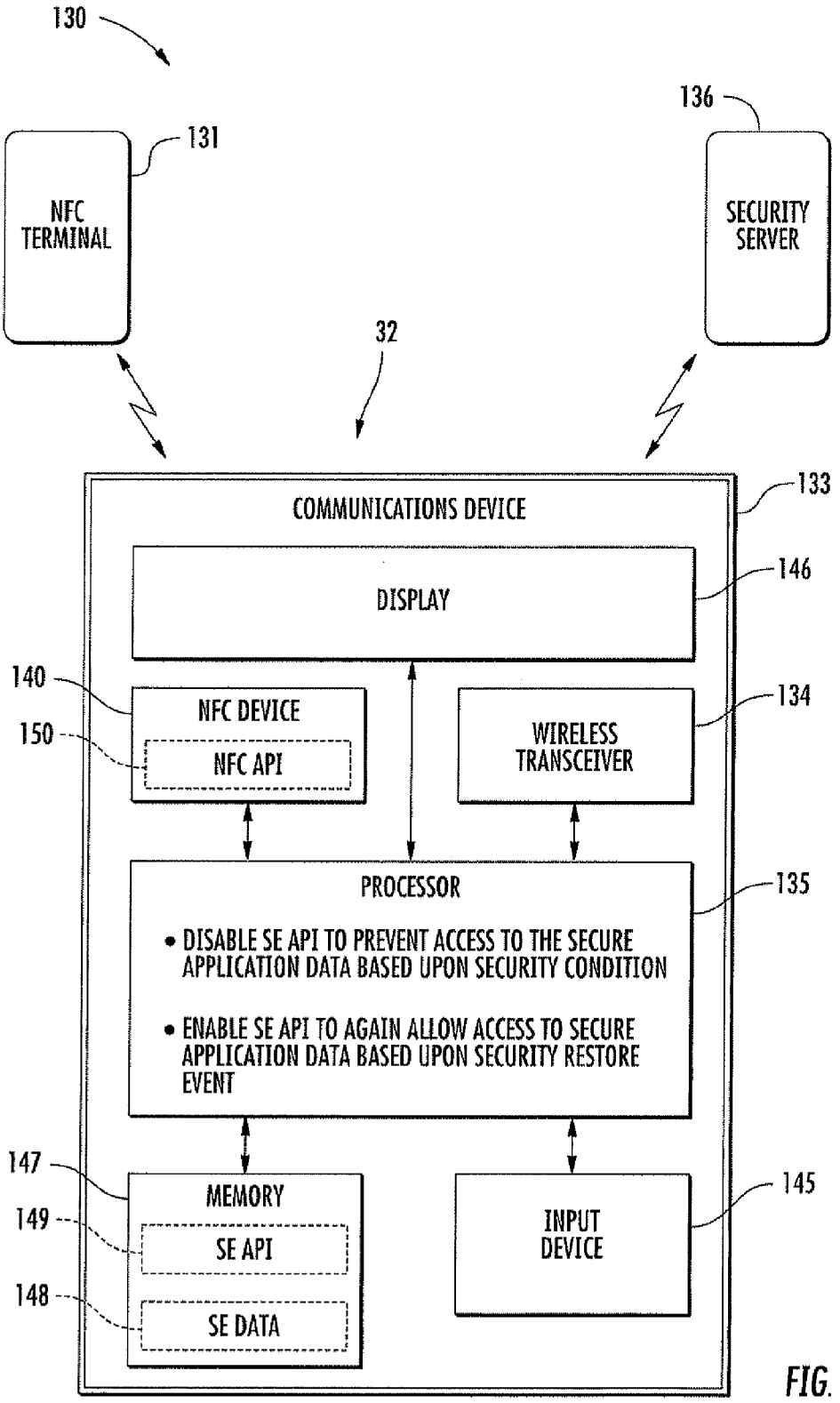

130
131
NFC TERMINAL
136
SECURITY SERVER
32
133
COMMUNICATIONS DEVICE
146
DISPLAY
140
NFC DEVICE
150
NFC API
134
WIRELESS TRANSCEIVER
135
PROCESSOR
• DISABLE SE API TO PREVENT ACCESS TO THE SECURE APPLICATION DATA BASED UPON SECURITY CONDITION
• ENABLE SE API TO AGAIN ALLOW ACCESS TO SECURE APPLICATION DATA BASED UPON SECURITY RESTORE EVENT
147
MEMORY
149
SE API
148
SE DATA
145
INPUT DEVICE

FIG. 5

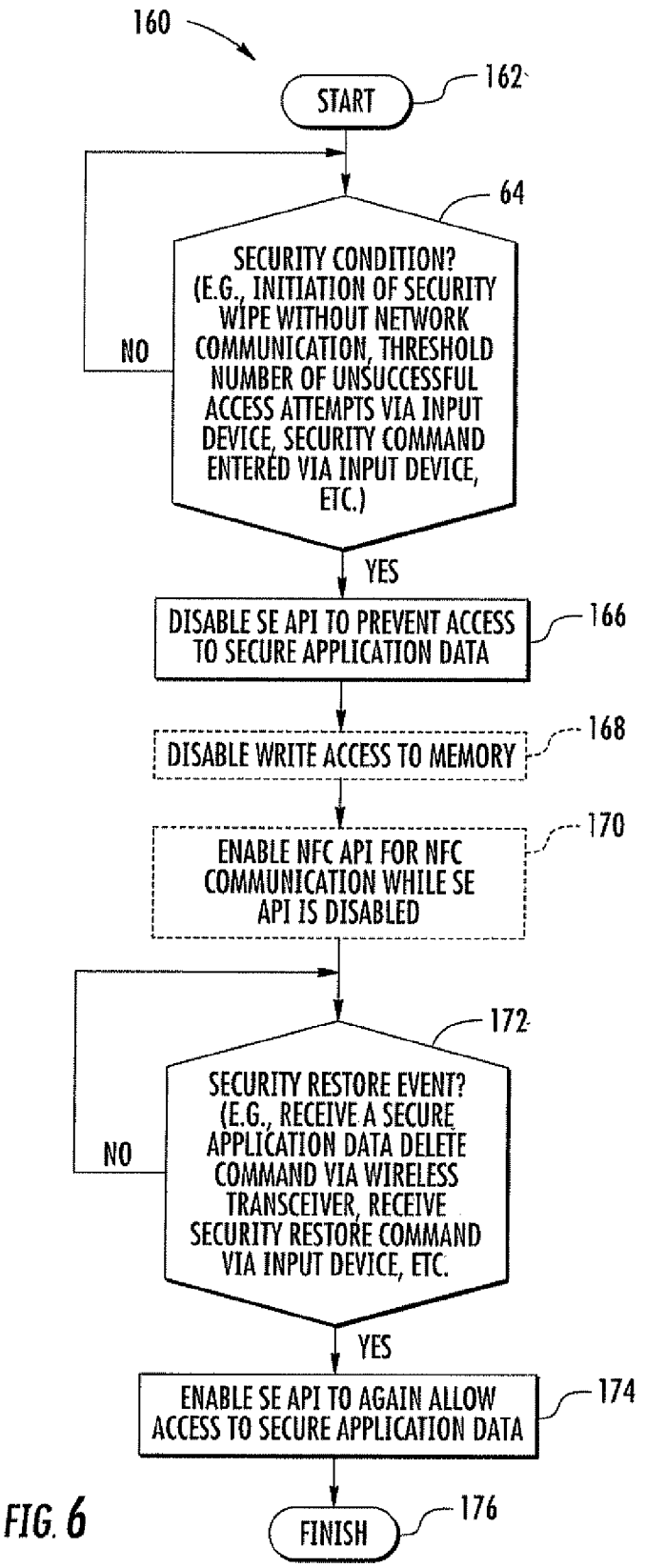

160
START
162
64
SECURITY CONDITION? (E.G., INITIATION OF SECURITY WIPE WITHOUT NETWORK COMMUNICATION, THRESHOLD NUMBER OF UNSUCCESSFUL ACCESS ATTEMPTS VIA INPUT DEVICE, SECURITY COMMAND ENTERED VIA INPUT DEVICE, ETC.)
NO
YES
DISABLE SE API TO PREVENT ACCESS TO SECURE APPLICATION DATA
166
DISABLE WRITE ACCESS TO MEMORY
168
ENABLE NFC API FOR NFC COMMUNICATION WHILE SE API IS DISABLED
170
172
SECURITY RESTORE EVENT? (E.G., RECEIVE A SECURE APPLICATION DATA DELETE COMMAND VIA WIRELESS TRANSCEIVER, RECEIVE SECURITY RESTORE COMMAND VIA INPUT DEVICE, ETC.
NO
YES
ENABLE SE API TO AGAIN ALLOW ACCESS TO SECURE APPLICATION DATA
174
FINISH
176

FIG. 6

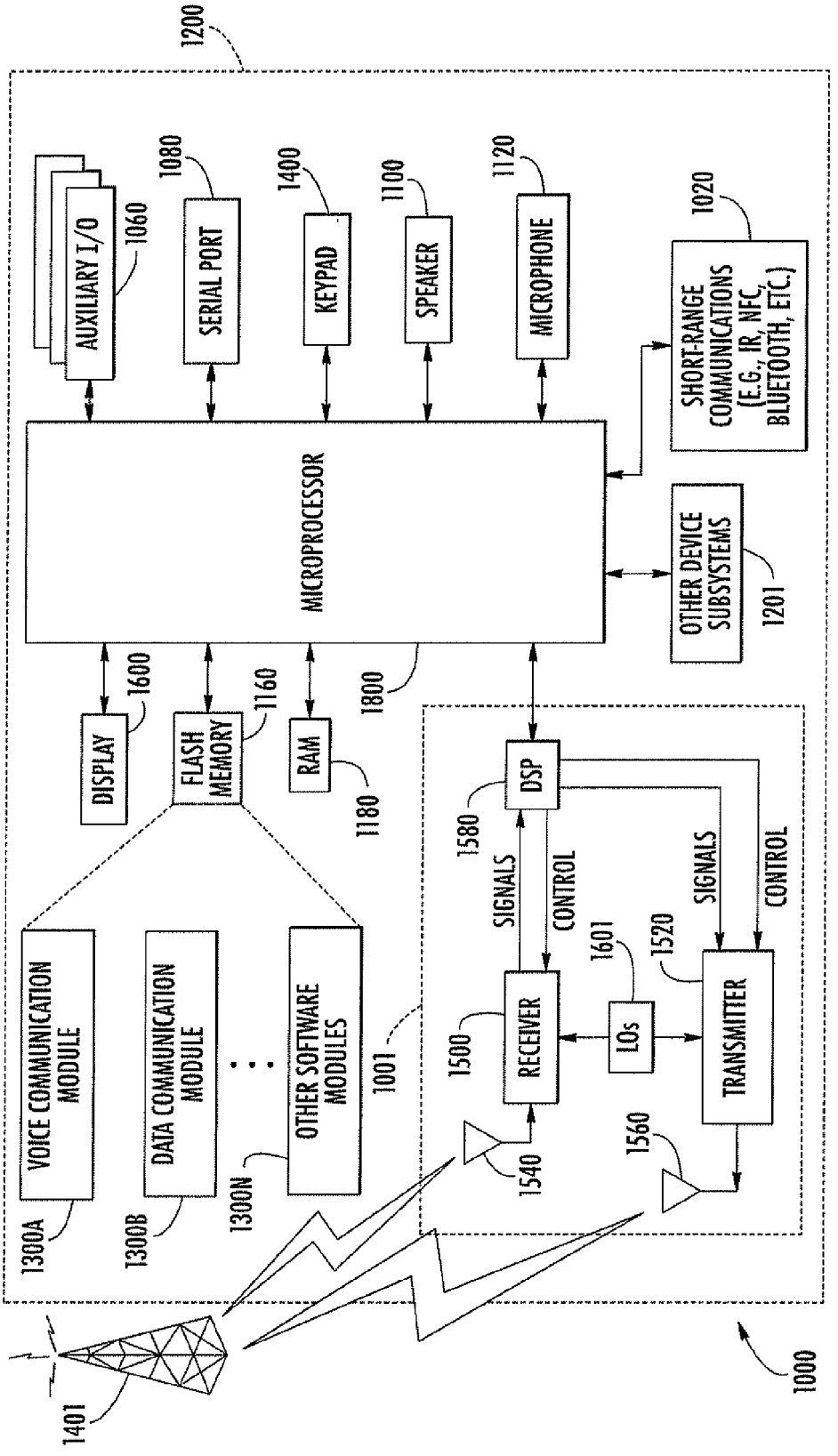

1200
AUXILIARY I/O
1060
SERIAL PORT
1080
KEYPAD
1400
SPEAKER
1100
MICROPHONE
1120
SHORT-RANGE COMMUNICATIONS (E.G., IR, NFC, BLUETOOTH, ETC.)
1020
MICROPROCESSOR
OTHER DEVICE SUBSYSTEMS
1201
1800
DISPLAY
1600
FLASH MEMORY
1160
RAM
1180
VOICE COMMUNICATION MODULE
1300A
DATA COMMUNICATION MODULE
1300B
OTHER SOFTWARE MODULES
1300N
1001
DSP
1580
SIGNALS
CONTROL
RECEIVER
1500
LOs
1601
TRANSMITTER
1520
1540
1560
1401
1000

FIG. 7

COMMUNICATIONS DEVICE PROVIDING NEAR FIELD COMMUNICATION (NFC) SECURE ELEMENT DISABLING FEATURES RELATED METHODS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of provisional application no. 61/452,511, filed Mar. 14, 2011, which is hereby incorporated herein in its entirety by reference.

TECHNICAL FIELD

[0002] This application relates to the field of communications, and more particularly, to wireless communications systems and related methods.

BACKGROUND

[0003] Mobile communication systems continue to grow in popularity and have become an integral part of both personal and business communications. Various mobile devices now incorporate Personal Digital Assistant (PDA) features such as calendars, address books, task lists, calculators, memo and writing programs, media players, games, etc. These multi-function devices usually allow electronic mail (email) messages to be sent and received wirelessly, as well as access the internet via a cellular network and/or a wireless local area network (WLAN), for example.

[0004] Some mobile devices incorporate contactless card technology and/or near field communication (NFC) chips. NFC technology is commonly used for contactless short-range communications based on radio frequency identification (RFID) standards, using magnetic field induction to enable communication between electronic devices, including mobile wireless communications devices. This short-range high frequency wireless communications technology exchanges data between devices over a short distance, such as only a few centimeters.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. **1** is a schematic block diagram of a communications system in accordance with an example embodiment.

[0006] FIG. **2** is a schematic diagram of the communications system of FIG. **1** showing the display of the mobile device.

[0007] FIG. **3** is a more detailed schematic diagram of the communications system of FIG. **1**.

[0008] FIG. **4** is a flow diagram illustrating example method aspects associated with the systems of FIGS. **1-3**.

[0009] FIG. **5** is a schematic block diagram of a communications system in accordance with another example embodiment.

[0010] FIG. **6** is a flow diagram illustrating example method aspects associated with the system of FIG. **5**.

[0011] FIG. **7** is a schematic block diagram illustrating example mobile wireless communications device components that may be used with the devices of FIGS. **1-3** and **5**.

DETAILED DESCRIPTION

[0012] The present description is made with reference to the accompanying drawings, in which embodiments are shown. However, many different embodiments may be used, and thus the description should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete. Like numbers refer to like elements throughout.

[0013] Generally speaking, a communications device is provided herein which may include a near field communication (NFC) device, at least one memory configured to store secure application data to be communicated via the NFC device and a secure element (SE) application programming interface (API) associated with the secure application data, and a processor coupled with the NFC device and with the at least one memory. The processor may be configured to disable the SE API to prevent access to the secure application data based upon a security condition, and enable the SE API to allow access to the secure application data based upon a security restore event. Accordingly, the processor may advantageously prevent access to the secure application data without having to wait for a trusted service manager (TSM) to authorize deletion of the secure application data, for example.

[0014] More particularly, the communications device may further include a wireless transceiver coupled with the processor, and the security condition may comprise initiation of a wipe while the wireless transceiver is not in communication with a wireless communications network. In accordance with other examples, the communications device may further include an input device coupled with the processor, and the security condition may comprise a threshold number of unsuccessful device authentication attempts via the input device, or a security command entered via the input device. Also by way of example, the security restore event may comprise receiving a secure application data delete command via the wireless transceiver, or receiving a security restore command via the input device.

[0015] The NFC device may also have an NFC API associated therewith. As such, the processor may be further configured to enable the NFC API for NFC communication while the SE API is disabled. Additionally, the processor may be further configured to prevent write access to the memory based upon the occurrence of the security condition.

[0016] A related communications system may include a NFC terminal and a communications device, such as the one described briefly above. A related method for operating a communications device, such as the one described briefly above, may include disabling the SE API to prevent access to the secure application data based upon a security condition, and enabling the SE API to allow access to the secure application data based upon a security restore event.

[0017] A related non-transitory computer-readable medium is for a communications device such as the one described briefly above. The non-transitory computer-readable medium may have computer-executable instructions for causing the communications device to perform steps comprising disabling the SE API to prevent access to the secure application data based upon a security condition, and enabling the SE API to allow access to the secure application data based upon a security restore event.

[0018] Referring initially to FIGS. **1-2**, a communications system **30** illustratively includes a near field communication (NEC) terminal **31** associated with an object, and a mobile wireless communications device **32** (also referred to as a "mobile device" herein). Example mobile wireless communications devices may include portable or personal media players (e.g., music or MP3 players, video players, electronic

book readers, etc.), portable gaming devices, portable or mobile telephones, smartphones, tablet computers, digital cameras, etc.

[0019] The mobile device **32** illustratively includes a portable housing **33** and a wireless transceiver **34** carried by the portable housing **33**. The wireless transceiver **34** may comprise a cellular transceiver or other type of wireless communications transceiver, and may communicate any combination of voice and data, such as, for example, email. The wireless transceiver **34** may communicate with a security server **36** that may provide one or more of remote instructions and provisioning operations to the mobile device **32**.

[0020] The mobile device **32** includes a display **46** carried by the portable housing **33**. The display **46** may comprise a liquid crystal display (LCD), for example, and may be configured to display information relating to data or voice communications. The display **46** may be in the form of an active display that includes a backlight, for example. The display **46** may display email information, contact information, or call information. The display **46** may be another type of display, for example, a passive display, and may display other information.

[0021] The mobile device **32** also includes an input device **45**. The input device **45** may be a keypad, touch-screen display, or other input device, for example.

[0022] The mobile device **32** also includes a processor **35** that is carried by the portable housing **33** and coupled with the wireless transceiver circuitry **34**, the input device **45**, and the display **46**. The processor **35** may be implemented using hardware (e.g., memory, etc.) and software components, i.e., computer-readable instructions for causing the mobile device **32** to perform the various functions or operations described herein.

[0023] The mobile device **32** also includes an NFC device **40** carried by the portable housing and coupled with the processor **35**. The NFC device **40** includes a NFC controller **41** and a NFC transceiver **42** coupled with the NFC controller **41**. The NFC controller **41** and the NFC transceiver **42** advantageously cooperate to perform at least one NFC communication function. For example, the NFC device **40** may communicate with the NFC terminal **31** based upon proximity thereto using NFC communication. The NFC terminal **31** may be a NFC tag, a NFC-enabled mobile device, a smart poster, etc.

[0024] By way of background, NFC is a short-range wireless communications technology in which NFC-enabled devices are "swiped," "bumped" or otherwise moved in close proximity to communicate. In one non-limiting example implementation, NFC may operate at 13.56 MHz and with an effective range of several centimeters, typically 4 cm or less, but other suitable versions of near-field communication which may have different operating frequencies, effective ranges, etc., for example, may also be used.

[0025] The NFC device **40** also includes a first memory **43** coupled to the NFC controller **41**. More particularly, the first memory **43** may be embedded within the NFC device hardware or within the NFC integrated circuit (IC). The first memory **43** may be tamper resistant, for example. In other words, the first memory **43** may comprise a secure element. The first memory **43** or secure element, may store applications relating to NFC communications, or contactless applications for communicating with the NFC terminal **31**. For example, the applications may include financial payment applications, secure access system applications, loyalty card applications, and other applications, and may be encrypted. In some example embodiments, the first memory **43** may store only one application.

[0026] The mobile device **32** also includes a second memory **44**. The second memory **44** may comprise the device memory, for example. In other words, the second memory **44** may include operating system files, applications, and other device data. In some example embodiments, the second memory **44** may be part of the universal integrated circuit card (UICC), for example. The second memory **44** may also be removable, and may be a secure-digital (SD) card or a subscriber identity module (SIM) card, for example. The second memory **44** may comprise another type of memory, for example a flash memory. While first and second memories **43**, **44** are described herein, more than two memories may be used. In other words, applications, or secure elements, may be stored in or spread over various memory devices. It should also be noted that a secure element may be implemented in a dedicated or secure area of a common memory, for example. In addition, multiple secure elements may be used.

[0027] The processor **35** may be configured to disable the NFC transceiver **42** based upon a security condition. A security condition may occur when a user of the device **32** cannot be authenticated, for example, as a result of the device **32** receiving too many incorrect password entries via the input device **45**. Alternatively, the security condition may occur when the device **32** receives, via the input device **45**, a command to perform operations associated with a security condition. This may occur, for example, in the context of a user who will no longer be using the device **32** and is preparing to give away the device **32** to another user or trade in the device **32** for a new device, for example. These operations may be collectively referred to as a "wipe". Still further, a security condition may occur when the device **32** receives a remote command, e.g., a remote wipe command, indicating a security condition, for example, from a system administrator. This may occur, for example, in the context of a lost or stolen or otherwise compromised device. However, a user-initiated wipe may also occur when the mobile device **32** is not in communication with a network, i.e., it is out of coverage (e.g., wireless coverage, data coverage, radio coverage, etc., for example.

[0028] If a security condition is detected, the processor **35** may be configured to disable access to the applications on the first memory **43**, e.g., secure payment applications. Disabling is performed since the mobile device **32** typically does not have unlimited read/write access to the first memory **43** since the first memory does not inherently "trust" the mobile device **32**. That is, secure data or applications stored on the first memory **43** typically may not be modified except by a trusted third party source, as will be discussed further below. Thus, the security server **36** is able to initiate a wipe of the first memory **43** based upon communication therewith, as will be described in further detail below. That is, the ability for a mobile device application to interact with an application on a secure element may be disabled via the baseband interface. Another example approach is to use a mobile device application to disable the ability of an application on the secure element to communicate via the NFC transceiver **42**.

[0029] After disabling access to the applications on the first memory **43**, the processor **35** is configured to erase the contents, or second application from the second memory **44**, or device memory. In other words, the mobile device **32** is wiped.

[0030] The processor **35** performs a reset operation after successfully erasing the applications from the second memory **44**. In other words, the reset operation may be based upon a successful wipe. The reset operation may be performed by selectively disabling a power source **37** carried by the housing **33** and coupled to the processor **35**. In other words, the reset operation may comprise a power down/power up cycle of the mobile device **32**. The power source **37** may comprise a battery cell, for example. In some example embodiments, a reset operation may not be performed.

[0031] The processor **35** is also configured to erase the applications from the first memory **43** after the reset operation. The processor **35** may erase the applications based upon a command received from the security server **36** via the wireless transceiver **34** after the reset operation. The processor **35**, after the applications are deleted or wiped from the first memory **44**, is configured to enable access to the NFC transceiver.

[0032] In some example embodiments, the contents, or second application from the second memory **44**, may not be erased based upon a security condition. Based upon a security condition, the application on the first memory **43** may be erased while selectively maintaining the second application on the second memory **44**. In other words, the processor **35** may be configured to erase the application from the first memory **43** without performing the steps of erasing the second application and resetting.

[0033] Referring now to FIG. **3**, in one advantageous example embodiment, the first memory **43** may comprise an embedded secure element (eSE). An eSE comprises an integrated circuit (IC) that manages and includes credentials (e.g., credentials associated with various credit cards, bank cards, gift cards, access cards, transit passes, etc.) that have been provisioned to the mobile device **32**. In an example embodiment, the eSE **43** may run based upon a GlobalPlatform card specification and be compatible with a Java Card Platform Specification, for example. The eSE **43** may run or be compatible with other or additional platforms.

[0034] Within the eSE **43**, GlobalPlatform is responsible for managing the lifecycle of other applets, and for providing them with security services (e.g., allowing application security domains to be created). Security domains maintain a lifecycle state for each applet (e.g., active, locked, etc.), manage the keys for authenticated access to an applet, and serve as an endpoint when a secure channel is established between a security server **36**, i.e., trusted service manager (TSM) and an applet. The security server **36** or TSM is typically responsible for provisioning and managing the applets within its security domain on the first memory **43**.

[0035] RF readers, and more particularly, NFC readers, for example, the NFC terminal **31** may communicate with the applets that are installed on the eSE **43** via the NFC controller **41** and NFC transceiver **43**. A reader, or NFC terminal **31** first selects an applet by its applet identifier (AID), GlobalPlatform checks for the existence of the applet in question (and verifies that the applet is in the correct lifecycle state), and then further application protocol data units (APDUs) sent by the reader are routed to the applet by GlobalPlatform. Generally, the RF readers, for example, the NFC terminal **31**, do not open secure channels to the security domains, and any authentication that occurs with the NFC terminal is the responsibility of the specific applet that gets selected.

[0036] The TSM **36** may open a secure channel to the issuer security domain (ISD) via the mobile device **32**, by authenticating itself using the appropriate ISD keys. An ISD is considered the security endpoint that communicates with the root TSM and allow for installation of applets and management of application security domains (ASDs). To the mobile device **32**, this secure channel is entirely opaque. The TSM **36** may then manage applets (e.g., install and delete them, change their lifecycle states) and manage the application security domains on the eSE **43**. After establishing a secure channel with a security domain, the TSM **36** can then send APDUs to the applets that belong to that security domain. The applet can determine that it is communicating with its TSM **36** over a secure channel, and can thus allow access to privileged or "administrative" commands.

[0037] The eSE **43** typically does not "trust" the mobile device **32** to the same degree as the TSM **36**, since GlobalPlatform may not intend for a mobile device to have access to the keys that are needed to open a secure channel. However, an applet can determine that it is communicating over the baseband interface and thus allow access to commands that would not otherwise be available. The baseband interface generally refers to an interface for communications between the processor **35** and the eSE **43**, or first memory, (via the NFC controller **41**). This may include commands that are sent from the wireless transceiver **34**, for example, that are then sent to the eSE **43** across the baseband interface.

[0038] For example, a credit card applet may allow the baseband interface to place it in a "visible" or "hidden" state, while allowing access to the necessary commands for a typical financial transaction over the NFC transceiver **42** or RF interface. It should be noted that due to this restriction, the mobile device **32** may not "wipe" the eSE **43** in a conventional sense. Based on the interfaces and application programming interfaces (APIs) provided by GlobalPlatform, there is typically no way for the mobile device **32** to delete an applet or, for that matter, even to enumerate the applets that are installed/instantiated on the eSE **43**.

[0039] Based on the restrictions described earlier, it may be increasingly difficult for the mobile device **32** to directly delete applets from the eSE **43**. However, it may be unacceptable for a mobile device to delay a wipe until such time that the TSM **36** could be contacted to wipe the eSE **43**, especially given that an attacker might remove the mobile device SIM, or any other persistent memory device, i.e., the second memory **44**, to ensure it does not have coverage.

[0040] In the present embodiments, the processor **35** takes steps to ensure data and access to the eSE **43** is prevented when the mobile device wipe is triggered (effectively resembling a wipe of the eSE **43** to the end user) and will result in the eSE being wiped at the next possible opportunity, i.e., whenever the mobile device **32** has coverage and is able to contact the TSM **36**.

[0041] The eSE **43** may include applets or other code to perform the wipe process. More particularly, the eSE **43** may include one or more emulation layers, for example, the MIFARE and iClass emulation layers. The emulation layers may not be directly linked to applets or other code on the eSE **43**, for example. The applet generally includes security keys for writing to its corresponding emulation layer, for example, for the MIFARE emulation class, this would be K_MIFARE, which is derived from K_A and K_B for a specific block of MIFARE memory. Each of the wipe applets may be installed and instantiated by the TSM **36**. The applets may be visible over the baseband interface, and it may respond to a specific

APDU that may trigger it to wipe its corresponding emulation layer using the security keys, for example.

[0042] The ISD lifecycle state can be moved to card lock, effectively disabling access to all applets on the eSE **43** by an applet provided that it is granted the card lock privilege. Thus, a wipe applet can be installed and instantiated by the TSM **36** to the ISD and given card lock privileges. The applet may be only visible over the baseband interface, and may respond to a specific APDU that triggers it to move the ISD lifecycle state to card lock. Additional code may be used so that certain portions, for example, internal code, can communicate with this applet.

[0043] In a normal operating state, the user uses the mobile device **32** normally for voice and/or data communications. For example, if the user uses a wallet application and the TSM **36** has installed anything to their mobile device's eSE **43**, the TSM installs and instantiates the "wipe applet" to the ISD, and asserts a persistent flag indicating the eSE **43** is in use. If, at some point, the eSE **43** is provisioned with an emulation layer credential, for example, the corresponding emulation layer wipe applet would be installed and instantiated at this time. For example, if the eSE **43** is provisioned with a MIFARE credential, then the MIFARE wipe applet would be installed and instantiated at this time.

[0044] In a first step, the wipe is triggered. As noted above, the mobile device wipe may be triggered in multiple ways, for example, receipt of too many incorrect password entries via the input device **45** in an attempt to gain access to the mobile device **32**, receipt of a local wipe command, e.g., comprising a "wipe" option on the mobile device, or a remote wipe command may be sent. In the remote wipe case, an acknowledgement may be sent, for example. It is worthwhile noting that the wipe may not be delayed if this acknowledgement is not sent.

[0045] In a second step, access to the processing interface for communicating with the eSE **43** and the transceiver **42** is prevented or restricted. If a persistent flag indicating the eSE **43** has been personalized, the mobile device wipe code may assert a persistent flag indicating the eSE **43** has been locked. Each of the above-noted persistent flags may be set or cleared. The eSE primary interface APIs and the NFC transceiver APIs check the value of a persistent flag indicating that the eSE **43** has been locked when they are called. If it is asserted, the eSE primary interface APIs typically should ignore any call not coming from an internal or trusted module, and the NFC transceiver APIs should disable all access to the card emulation mode.

[0046] In a third step, each emulation layer is wiped. The wipe APDU is sent to the corresponding wipe applet over the baseband interface. The applet wipes personalization data in the emulation layer. More particularly, for example, the wipe APDU may wipe the personalization data in the iClass and MIFARE emulation layers.

[0047] In a fourth step, the eSE **43**/ISD is moved to a card locked state. The wipe APDU is sent to the wipe applet over the baseband interface. The applet moves the ISD state to card locked, effectively denying access to applets and security domains on the eSE **43**. It should be noted that this step should take place after the third step, since otherwise communication may not be possible with the applets that wipe the emulation layers in those steps. After this step, although the eSE **43** still includes personalized applets, these applets are no longer accessible to anyone but the TSM **36**. From the end user's perspective, the eSE **43** is "wiped".

[0048] In a fifth step, the mobile device **32** is wiped. The mobile device **32** is wiped by operating system (OS) code, for example.

[0049] In a sixth step, the mobile device **32** restarts. The mobile device **32** restarts after the wipe is successful.

[0050] In a seventh step, an eSE proxy (not shown) signals the TSM **36**. The eSE proxy starts up and detects that the ISD is in a card locked state (by attempting to select the ISD over the baseband interface, or by checking the persistent flag indicating the eSE **43** has been locked. It then waits for a data connection and signals the TSM **36** that the eSE **43** needs to be wiped.

[0051] In an eighth step, the eSE **43** is wiped. The TSM **36** deletes all applets from the eSE **43**. It should be noted that in some embodiments, selective access to the eSE **43** may be provided over the baseband interface. For example, an application from a mobile device manufacturer may be allowed to access the eSE **43** for the purposes of wiping the eSE, while access from third party applications may be restricted.

[0052] In a ninth step, access to eSE primary interface APIs and the NFC transceiver **42** are restored. Once the TSM **36** is satisfied that all applets have been deleted from the eSE **43**, it signals the eSE proxy that a persistent flag indicating the eSE **43** has been locked. At this stage, eSE primary interface APIs are unlocked to third parties, and the NFC transceiver **42** is permitted to enter card emulation mode again. The eSE **43**, at this point, has been reset to a factory state. It should be noted that in different embodiments steps other steps may be performed, or some steps may be performed in different orders.

[0053] Referring now to the flowchart **60** of FIG. **4**, related method aspects are now described. Beginning at Block **62**, the processor **35** determines whether a security condition has been initiated (Block **64**). For example, the securing condition may comprise a wipe, or entering a wrong password a given number of times (which may also trigger a wipe in some embodiments). If a security condition is determined, the processor **35** disables the NFC transceiver **42** (Block **66**). The processor **35** then disables access to the first plurality of applications on the first memory **43** (Block **68**). At Block **70**, the processor **35** erases the second application from the second memory **44**. A reset operation is performed by the processor **35** (Block **72**). At Block **74**, the security server **36** sends a signal to the processor **35** via the wireless transceiver **34** once a connection is established therewith. At Block **76** the processor **35** erases the first plurality of applications from the first memory **43** if the signal from the security server **36** is received. The NFC transceiver **42** at Block **78** is re-enabled after the first plurality of applications is erased. The method ends at Block **80**.

[0054] Turning now to FIG. **5**, a related communications system **130** illustratively includes an NFC terminal **131**, a communications device **132** (e.g., a mobile wireless communication device), and a security server **136**, which are similar to those described above. In particular, in the present example the communications device **132** illustratively includes a housing **133** carrying a wireless transceiver **134**, a NFC device **140**, an input device(s) **145**, a display **146**, one or more memories **147**, and a processor **135**. The wireless transceiver **134**, NFC device **140**, input device **145**, display **146**, and memory **147** are illustratively coupled with the processor **135**, and these components are similar to the counterpart components described above except as otherwise described below.

[0055] The NFC device **140** has one or more NFC APIs **150** associated therewith. Moreover, the memory **147** may be part of the NFC device **140** in some embodiments, it may be a separate memory (e.g., SD card, SIM card, etc.), or both types of memories may be used, as noted above. In the present example, the memory **147** illustratively includes secure element (SE) application data **148** to be communicated via the NFC device **140** (e.g., a secure applet, account information, etc.), and an SE API **149** associated with the secure application data. As noted above, the API controls access to the SE application data **148** stored in the memory **147**.

[0056] As also noted above, SEs are where NFC applets such as payment (e.g., credit or debit card, etc.), transit, physical access control, and other secure applications are stored. In conjunction with the NFC device **140**, the SE will allow the mobile device **132** to act as a payment or access card, for example. Typically, installation and removal or deletion of applications from an SE may only be performed by a third party entity that holds the master keys (i.e., issuer security domain keys) to authenticate with the SE. The third party entity (e.g., TSM) may open a cryptographically secure channel to the secure element (e.g., using a proxy application running on the mobile device **132** to access the SE). For example, when a credit card applet is to be installed on the SE of the mobile device **132**, the TSM, after receiving the appropriate instructions from the given bank, will open a secure channel to a secure element and install the appropriate credit card applet. Subsequently, if the credit card applet is to be removed or deleted, the TSM will remove it.

[0057] Such TSM operations require a communications link between the proxy and the TSM (typically an over-the-air connection in the case of a mobile wireless communications device, as described above). Again, this may create a problem in that if the user wants to wipe the mobile device **132** before giving it away or disposing of it, etc., the user may not have coverage, either because of being out of wireless communications range, account cancellation, SIM card removal, etc. Without coverage, the TSM will not be able to issue the appropriate delete commands, so even after a security wiping of the mobile device **132**, the memory **147** will still retain all of the SE application data **148**. Thus, for example, a credit card may still be used after the mobile device **132** is wiped and handed off to another user.

[0058] With further reference to the flow diagram **160** of FIG. **6**, beginning at Block **162**, the processor **135** is configured to disable the SE API **149** to prevent access to the SE application data **148** based upon a security condition such as a device wipe, at Blocks **164**, **166**. In particular, the disabling may occur despite the wireless transceiver **134** not being in communication with the security server **136** (e.g., TSM) via a wireless communications network. Another security condition that may trigger disabling of the SE API **149** may include a threshold number of unsuccessful access attempts to access the mobile device **132** via the input device **145** (e.g., incorrectly entered passwords, etc.), as noted above.

[0059] Still another security condition that may trigger disabling of the SE API **149** is a security command entered via the input device **145**. For example, in some instances a user may desire to temporarily disable the SE application data **148** so that the mobile device **132** may be loaned to another user without allowing the other user to access the SE data, but not completely wipe the mobile device. In such cases, a security command (e.g., selection of a security option from an on-screen menu, etc.) may be used to temporarily cause the processor **135** to disable the SE API **149** so that the SE application data **148** may not be accessed.

[0060] In some embodiments, write access to the memory **147** may optionally be selectively disabled while the SE API is disabled, at Block **168**. That is, the processor **135** may prevent any further SE data from being written to or installed on the memory **147** by TSMs until the security condition has been resolved, as will be discussed further below. However, in the interim, the processor **135** may optionally enable (or continue to allow) the NFC API **150** to perform NFC communication while the SE API **149** remains disabled for other NFC applications that do not require access to the SE data **148**, at Block **147**.

[0061] The processor **135** may enable the SE API **149** to again allow access to the SE data **148** based upon a security restore event, at Blocks **172**, **174**, which concludes the illustrated method (Block **176**). Accordingly, the processor **135** may advantageously prevent access to the SE data **148** without having to wait for a TSM to authorize deletion of the secure application data, for example. By way of example, the security restore event may include receiving a secure application data delete command via the wireless transceiver **134**, such as a delete command from the TSM that issued the SE data **148**. In the case of a user that temporarily disables the SE API **149** as described above, the security restore event may comprise providing a secure password, biometric, etc., to restore NFC communication for the SE API.

[0062] Accordingly, the processor **135** is advantageously able to disable or suspend the SE API **149** and the ability for the NFC device **140** to route NFC traffic to the SE API if a security condition occurs. Thus, after the mobile device **132** is wiped, etc., even though SE data **148** remains in the memory **147**, the processor **135** prevents NFC device **140** traffic from being routed to or from the SE API **149**. As such, the SE data **148** may not be accessed by the NFC terminal **131** (e.g., an external point-of-sale terminal) for the purposes of performing a payment or other secure transaction.

[0063] Moreover, the processor **135** may, for example, only allow NFC device **140** traffic to resume routing to the SE API **149** after a delete command has been successfully received from the TSM and injected to delete the SE application data **148**, etc. This way, it may be assured that the SE data **148** has been deleted before allowing a next user, for example, to activate NFC device **140** communication routing to the memory **147**. In some example embodiments, the processor **135** may also lock baseband access to the SE data **148** (e.g. through JSR-177) unless the baseband access is being used to issue a delete command. Once the delete command has been issued, baseband access may be reinstated.

[0064] This example approach provides several advantages. For example, the mobile device **132** may be wiped at any time, regardless of whether it has coverage or whether there is a SIM inserted, without having to wait for a TSM to issue delete commands to the secure element to ensure SE data **148** protection. Then, before the SE API **149** or SE data **148** may effectively be used again, the processor **135** will enforce receipt of a cryptographically protected delete command from the TSM (in the case of a device wipe security condition) or appropriate security credentials before allowing the SE API **149** to be used again, such as through the NFC device **140** or the wireless transceiver **134**.

[0065] A related non-transitory computer-readable medium example embodiment may have computer-executable instructions for causing the communications device **132**

to perform steps including disabling the SE. API **149** to prevent access to the SE data **148** based upon a security condition, and enabling the SE API to again allow access to the SE data based upon a security restore event, as described further above. The non-transitory computer-readable medium may perform additional steps described above as well.

[0066] Example components of a mobile wireless communications device **1000** that may be used in accordance with the above-described embodiments are further described below with reference to FIG. **7**. The device **1000** illustratively includes a housing **1200**, a keyboard or keypad **1400** and an output device **1600**. The output device shown is a display **1600**, which may comprise a full graphic LCD. Other types of output devices may alternatively be utilized. A processing device **1800** is contained within the housing **1200** and is coupled between the keypad **1400** and the display **1600**. The processing device **1800** controls the operation of the display **1600**, as well as the overall operation of the mobile device **1000**, in response to actuation of keys on the keypad **1400**.

[0067] The housing **1200** may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keypad may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

[0068] In addition to the processing device **1800**, other parts of the mobile device **1000** are shown schematically in FIG. **7**. These include a communications subsystem **1001**; a short-range communications subsystem **1020**; the keypad **1400** and the display **1600**, along with other input/output devices **1060**, **1080**, **1100** and **1120**; as well as memory devices **1160**, **1180** and various other device subsystems **1201**. The mobile device **1000** may comprise a two-way RF communications device having data and, optionally, voice communications capabilities. In addition, the mobile device **1000** may have the capability to communicate with other computer systems via the Internet.

[0069] Operating system software executed by the processing device **1800** is stored in a persistent store, such as the flash memory **1160**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the random access memory (RAM) **1180**. Communications signals received by the mobile device may also be stored in the RAM **1180**.

[0070] The processing device **1800**, in addition to its operating system functions, enables execution of software applications **1300**A-**1300**N on the device **1000**. A predetermined set of applications that control basic device operations, such as data and voice communications **1300**A and **1300**B, may be installed on the device **1000** during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM may be capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application may also be capable of sending and receiving data items via a wireless network **1401**. The PIM data items may be seamlessly integrated, synchronized and updated via the wireless network **1401** with corresponding data items stored or associated with a host computer system.

[0071] Communication functions, including data and voice communications, are performed through the communications subsystem **1001**, and possibly through the short-range communications subsystem. The communications subsystem **1001** includes a receiver **1500**, a transmitter **1520**, and one or more antennas **1540** and **1560**. In addition, the communications subsystem **1001** also includes a processing module, such as a digital signal processor (DSP) **1580**, and local oscillators (LOs) **1601**. The specific design and implementation of the communications subsystem **1001** is dependent upon the communications network in which the mobile device **1000** is intended to operate. For example, a mobile device **1000** may include a communications subsystem **1001** designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communications networks, and also designed to operate with any of a variety of voice communications networks, such as AMPS, TDMA, CDMA, WCDMA, PCS, GSM, EDGE, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device **1000**. The mobile device **1000** may also be compliant with other communications standards such as 3GSM, 3GPP, UMTS, 4G, etc.

[0072] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore typically involves use of a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0073] When required network registration or activation procedures have been completed, the mobile device **1000** may send and receive communications signals over the communication network **1401**. Signals received from the communications network **1401** by the antenna **1540** are routed to the receiver **1500**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP **1580** to perform more complex communications functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network **1401** are processed (e.g. modulated and encoded) by the DSP **1580** and are then provided to the transmitter **1520** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **1401** (or networks) via the antenna **1560**.

[0074] In addition to processing communications signals, the DSP **1580** provides for control of the receiver **1500** and the transmitter **1520**. For example, gains applied to communications signals in the receiver **1500** and transmitter **1520** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **1580**.

[0075] In a data communications mode, a received signal, such as a text message or web page download, is processed by the communications subsystem **1001** and is input to the processing device **1800**. The received signal is then further processed by the processing device **1800** for an output to the display **1600**, or alternatively to some other auxiliary I/O device **1060**. A device may also be used to compose data items, such as e-mail messages, using the keypad **1400** and/or some other auxiliary I/O device **1060**, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communications network **1401** via the communications subsystem **1001**.

[0076] In a voice communications mode, overall operation of the device is substantially similar to the data communications mode, except that received signals are output to a speaker **1100**, and signals for transmission are generated by a microphone **1120**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device **1000**. In addition, the display **1600** may also be utilized in voice communications mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[0077] The short-range communications subsystem enables communication between the mobile device **1000** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, a Bluetooth™ communications module to provide for communication with similarly-enabled systems and devices, or a near field communications (NFC) sensor for communicating with a NFC device or NFC tag via NFC communications.

[0078] Many modifications and other embodiments will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that various modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A communications device comprising:
a near field communication (NFC) device;
at least one memory configured to store secure application data to be communicated via said NFC device and a secure element (SE) application programming interface (API) associated with the secure application data; and
a processor coupled with said NFC device and with said at least one memory, the processor being configured to
disable the SE API to prevent access to the secure application data based upon a security condition, and
enable the SE API to allow access to the secure application data based upon a security restore event.

2. The communications device of claim **1** further comprising a wireless transceiver coupled with said processor; and wherein the security condition comprises initiation of a wipe while said wireless transceiver is not in communication with a wireless communications network.

3. The communications device of claim **1** further comprising an input device coupled with said processor; and
wherein the security condition comprises a threshold number of unsuccessful device authentication attempts via said input device.

4. The communications device of claim **1** further comprising an input device coupled to said processor; and wherein the security condition comprises a security command entered via said input device.

5. The communications device of claim **1** further comprising a wireless transceiver coupled with said processor; and wherein the security restore event comprises receiving a secure application data delete command via said wireless transceiver.

6. The communications device of claim **1** further comprising an input device coupled with said processor; and wherein the security restore event comprises receiving a security restore command via said input device.

7. The communications device of claim **1** wherein said NFC device has an NFC API associated therewith; and wherein said processor is further configured to enable said NFC API for NFC communication while the SE API is disabled.

8. The communications device of claim **1** wherein said processor is further configured to disable write access to said memory based upon the occurrence of the security condition.

9. A communications system comprising:
a near field communication (NFC) terminal; and
a communications device configured to communicate with said NFC terminal, the communications device comprising
a NFC device,
at least one memory configured to store secure application data to be communicated via said NFC device to said NFC terminal and a secure element (SE) application programming interface (API) associated with the secure application data, and
a processor coupled with said NFC device and with said at least one memory, the processor being configured to
disable the SE API to prevent access to the secure application data based upon a security condition, and
enable the SE API to allow access to the secure application data based upon a security restore event.

10. The communications system of claim **9** wherein said communications device further comprises a wireless transceiver coupled with said processor; and wherein the security condition comprises initiation of a wipe while said wireless transceiver is not in communication with a wireless communications network.

11. The communications system of claim **9** wherein said communications device further comprises an input device coupled with said processor; and wherein the security condition comprises a threshold number of unsuccessful device authentication attempts via said input device.

12. The communications system of claim **9** wherein said communications device further comprises an input device coupled to said processor; and wherein the security condition comprises a security command entered via said input device.

13. The communications system of claim **9** wherein said communications device further comprises a wireless transceiver coupled with said processor; and wherein the security restore event comprises receiving a secure application data delete command via said wireless transceiver.

14. The communications system of claim **9** wherein said communications device further comprises an input device coupled with said processor; and wherein the security restore event comprises receiving a security restore command via said input device.

15. A method for operating a communications device comprising a near field communication (NFC) device and at least one memory configured to store secure application data to be communicated via the NFC device and a secure element (SE) application programming interface (API) associated with the secure application data, the method comprising:
disabling the SE API to prevent access to the secure application data based upon a security condition; and
enabling the SE API to allow access to the secure application data based upon a security restore event.

16. The method of claim **15** wherein the communications device further comprises a wireless transceiver coupled with the processor; and wherein the security condition comprises initiation of a wipe while the wireless transceiver is not in communication with a wireless communications network.

17. The method of claim **15** wherein the communications device further comprises an input device; and wherein the security condition comprises a threshold number of unsuccessful device authentication attempts via the input device.

18. The method of claim **15** wherein the communications device further comprises an input device; and wherein the security condition comprises a security command entered via the input device.

19. The method of claim **15** wherein the communications device further comprises a wireless transceiver coupled with the processor; and wherein the security restore event comprises receiving a secure application data delete command via the wireless transceiver.

20. A non-transitory computer-readable medium for a communications device comprising a near field communication (NFC) device and at least one memory configured to store secure application data to be communicated via the NFC device and a secure element (SE) application programming interface (API) associated with the secure application data, the non-transitory computer-readable medium having computer-executable instructions for causing the communications device to perform steps comprising:

disabling the SE API to prevent access to the secure application data based upon a security condition; and

enabling the SE API to allow access to the secure application data based upon a security restore event.

21. The non-transitory computer-readable medium of claim **20** wherein the communications device further comprises a wireless transceiver; and wherein the security condition comprises initiation of a wipe while the wireless transceiver is not in communication with a wireless communications network.

22. The non-transitory computer-readable medium of claim **20** wherein the communications device further comprises an input device; and wherein the security condition comprises a threshold number of unsuccessful device authentication attempts via the input device.

23. The non-transitory computer-readable medium of claim **20** wherein the communications device further comprises an input device; and wherein the security condition comprises a security command entered via the input device.

24. The non-transitory computer-readable medium of claim **20** wherein the communications device further comprises a wireless transceiver; and wherein the security restore event comprises receiving a secure application data delete command via the wireless transceiver.

* * * * *