

[0035] FIG. 12 is a flow chart of one embodiment of operations that may be performed in accordance with the invention;

[0036] FIG. 13 is a simplified block diagram of one embodiment of a security module constructed in accordance with the invention; and

[0037] FIG. 14 is a flow chart of one embodiment of operations that may be performed in accordance with the invention.

[0038] In accordance with common practice the various features illustrated in the drawings may not be drawn to scale. Accordingly, the dimensions of the various features may be arbitrarily expanded or reduced for clarity. In addition, some of the drawings may be simplified for clarity. Thus, the drawings may not depict all of the components of a given apparatus or method. Finally, like reference numerals denote like features throughout the specification and figures.

DETAILED DESCRIPTION

[0039] The invention is described below, with reference to detailed illustrative embodiments. It will be apparent that the invention may be embodied in a wide variety of forms, some of which may be quite different from those of the disclosed embodiments. Consequently, the specific structural and functional details disclosed herein are merely representative and do not limit the scope of the invention.

[0040] In one aspect, the invention relates to systems and methods that provide device and/or user level authentication. For example, various techniques are described for authenticating that a user is using a device. In addition, various techniques are described for authenticating a device to a service such as enabling access to a data network.

[0041] In a conventional data network device level authentication may be used to ensure that only authorized devices are allowed to connect to the network. Here, cryptographic techniques may be employed to authenticate that a device that is attempting to connect to the network is the device it purports to be and is authorized to use the network. For example, a device typically connects to the network via an access point such as a router. Compatible cryptographic keys are thus provided to the router and to authorized devices to enable these devices to perform cryptographic operations that provide the desired authentication. In such a network, a mechanism must be provided for securely distributing keys to all devices that may connect to the network. Traditionally, this has been accomplished by the user or a network administrator manually loading the keys into the devices (e.g., via a keyboard or a software program).

[0042] Such device level authentication may have a number of drawbacks. For example, there may not be any verification as to which user is using the device. Moreover, when multiple users use the same device, there may not be an efficient mechanism to determine which verification information (e.g., cryptographic certificate) should be used to authenticate to the system.

[0043] FIG. 1 illustrates one embodiment of a system 100 constructed in accordance with the invention where one or more users (not shown) may use one or more access devices 102 and 104 to access services (e.g., connect to a data

network) via an access server 106. For example, to access a service a user presents authentication information (e.g., credentials such as a password) to an input device 108. For convenience the term "credential(s)" may be used to refer generally to any type of information that a user may present for authentication purposes.

[0044] The input device 108 may include a security processing component (e.g., a security module 110, a processor with code for cryptographic operations, etc.) that provides cryptographic processing and may incorporate other security mechanisms. For example, the security module 110 may include one or more cryptographic processors that perform cryptographic operations such as encryption, decryption, authentication, verification and signing. Using the security module 110, the input device 108 may authenticate the credentials received from the user. The input device 108 may then securely send the credentials via an interface (e.g., an RF interface 124) to an access device 102 or 104 via signals 118 through a medium (e.g., a wireless medium).

[0045] The access device 102 or 104 includes an interface (e.g., RF interface 126 or 128) for receiving the signals 118. The access device 102 or 104 includes some form of processing (e.g., access processor 130 or 132) for accessing a service. For example, in some embodiments the access processor may comprise a processor for a cell phone or some other form of wireless device.

[0046] The access device 102 or 104 also may include a security processing component (e.g., security module 112 or 114) that provides cryptographic processing and may incorporate other security mechanisms. For example, a security module may include one or more cryptographic processors that perform cryptographic operations such as encryption, decryption, authentication, verification and signing. Using the security module, an access device 102 or 104 may authenticate the credentials received from the input device 108. The access device may then securely send the credentials via an interface (e.g., interface 134 or 136) to the access server 106 via signals 120 over a medium (e.g., a wireless medium).

[0047] The access server 106 includes an interface (e.g., interface 138) for receiving the signals 120. The access server includes some form of processing 140 for providing access to a service. For example, in some embodiments the access processor may comprise a network server for a wired and/or wireless network.

[0048] The access server 106 also may include a security processing component (e.g., security module 116, a key manager, etc.) that provides cryptographic processing and may incorporate other security mechanisms. Here, the security module 116 may process the received credentials to, for example, authenticate and/or decrypt the credentials. The above architecture may thus provide relatively strong authentication to the access server 106 that the credentials have been presented to a trusted input device 108 that is associated with a trusted access device 102 or 104. As a result, the access server 106 may enable the access device 102 or 104 to access the requested service.

[0049] Selected operations of the system 100 will be explained in more detail in conjunction with the flowchart of FIG. 2. As represented by block 202, one or more keys may be generated to enable the input device 108 to securely