

[0146] Accordingly, after the credential is signed by the cryptographic processor in the security module 708, the signed credential is sent to the key manager 724 via the link 726 (block 810). In this way, the information is, in effect, sent over a secured channel (as represented by the corresponding portion of the line 718) even though the actual data path may not be secure.

[0147] The key manager 724 sends the received information to the cryptographic processor 722 for decryption and/or authentication processing as necessary. The key manager 724 then verifies that the received information indicates that the user is authorized to access the network (block 812). In some embodiments the access server 704 may include a wireless proximity device (e.g., an RFID reader) and associated processing to enable the credentials to be easily and directly loaded into the access server when a user presents his or her token to the access server. In other embodiments the information may be acquired using a non-dedicated RFID reader. The acquired information may also be loaded into the access server by other means (e.g., downloaded via a communication medium).

[0148] Since the key manager 724 has received an indication via the cryptographic signature associated with the credential that the token 742 is proximate the access device 702, once the credentials are verified the key manager 724 may be assured that it is safe to provide access to the requested service. As discussed above, providing access to a network may involve sending security associations or keys to the access device 702. These keys may be sent to the access device 702 via the secured channel (cryptographic boundary 718). Accordingly, the cryptographic processor 722 may encrypt the keys before sending them over the link 726 (block 814).

[0149] The access device 702 may be configured so that these keys, etc., are decrypted and maintained within the security boundary of the access device 702 (block 816). For example, the keys may be stored within the integrated circuit 712 (e.g., keys 740). Alternatively, a cryptographic processor in the security module may use a key (e.g., keys 740) to encrypt the received keys before storing them in the data memory 714.

[0150] As represented by block 818, the access device may then use the received keys to gain access to the network as discussed herein. Again, in some embodiments these keys may only be used in the clear within the security boundary of the access device 702.

[0151] Additional details of a proximity authentication device are disclosed, for example in commonly-owned U.S. patent application Ser. No. 10/955,806, filed Sep. 30, 2004, the disclosure of which is hereby incorporated by reference herein.

[0152] FIG. 9 illustrates another embodiment of an access device that provides a secure mechanism for entering credentials. An access device 900 includes a data interface 904 that is located within a security boundary of the access device 900. For example, the data interface 904 may be located on the same integrated circuit 902 as a security module 906. As a result, credentials may be directly entered into the security boundary.

[0153] In addition, the security module 906 may use one or more keys (e.g., keys 908) to encrypt credentials within

the security boundary so that the credentials are not provided in the clear outside of the security boundary. Thus, the security module effectively extends the security boundary using cryptographic techniques. For example, the security boundary may be effectively extend (as represented by dashed lines 916) to an external data memory 914 by encrypting data before it is stored. In addition, the security boundary may effectively extend (as represented by dashed lines 920) through a communication medium to another cryptographic processing system (not shown).

[0154] In the embodiment of FIG. 9, the access device incorporates a wireless interface 910 and an antenna 912 (or another form of a wireless transceiver) to communicate with other wireless devices (e.g., a wireless access point and access server, not shown) via wireless signals 918. In some embodiments the data communication interface 910 for the access device may advantageously be located on the same integrated circuit as, for example, the security module 906. The wireless interface may support, for example, 802.11, Bluetooth and/or other wireless communication standards.

[0155] In some embodiments the access device may forward the input information to, for example, an access server to gain access to a service. The information also may be enrolled with a key manager. Thus, as described above, the key manager may compare information received from an access device with the key manager's database of authorized credentials (e.g., fingerprint data). When a match is received, the key manager may provide the associated key(s) to the requesting access device.

[0156] In some embodiments the access server may include an input device and associated processing to enable the information to be easily and directly loaded into the access server. In other embodiments the information may be acquired using a non-dedicated input device (e.g., a sensor). The acquired information may then be loaded into the access server by other means (e.g., downloaded via a communication medium).

[0157] FIG. 10 illustrates one embodiment of a system 1000 that provides a secure mechanism for a user to enter credentials. A processing system 1002 includes a secure processing system such as a trusted platform module ("TPM") 1004.

[0158] Typically, the trusted platform module may generate and maintain keys for the processing system. For example, a TPM may provide a set of cryptographic capabilities that enable certain computer functions to be securely executed within the TPM environment (e.g., hardware). To this end the TPM may include one or more cryptographic processors that perform cryptographic operations including, for example, encryption, decryption, authentication and key management. Specifications for a TPM are defined by the Trusted Computing Group organization.

[0159] Typically, to enable access to services managed by the TPM, a user must first enroll his or her credentials with the TPM. This may involve, for example, providing a password to the TPM. To this end, the TPM may include an input device (not shown) that incorporates some of the secure input mechanisms and techniques disclosed in the previous discussions and the discussions that follow (e.g., direct connection, RFID, biometric sensor, keyboard, etc.).

[0160] Then, when a user wishes to access the services managed by the TPM, the user must authenticate himself or