

interface 706, a security module 708 and other processing components 710 may be incorporated into a single integrated circuit 712. Thus, any processes performed or information used or stored within the integrated circuit 712 may not be compromised absent physical access to the integrated circuit 712 and the use of an invasive technique for analyzing the internal operations and data of the integrated circuit 712. For many applications, this form of hardware security boundary may provide an acceptably high level of security.

[0133] Other means may be used to provide a security boundary. For example, one or more integrated circuits (e.g., integrated circuit 712) may be protected by a physical structure using known techniques (e.g., epoxy encapsulation). Also, the access device 702 and/or its internal components may be tamper resistant and/or tamper evident.

[0134] Cryptographic techniques for providing a security boundary may include encrypting any important information that is sent to or from the integrated circuit via non-secure paths in the system. For example, security associations and keys may only appear in the clear within the integrated circuit 712. In the event keys need to be sent out of the integrated circuit 712 (e.g., to be stored in a data memory 714), the keys may first be encrypted.

[0135] Similarly, any important information that is sent between the integrated circuit 712 and the access server 704 may be encrypted. For example, information (e.g., credentials) received from the RFID token 742 may be encrypted before being sent over the link 726.

[0136] In FIG. 7 one cryptographic security boundary is represented by the dashed line 718. The line 718 represents, in part, that encrypted information may be sent between the security module 708, the processing component 710 and the data memory 714. Thus, the information may be sent securely even though the mechanism through which this information is sent (e.g., a data bus 720) may not be secure.

[0137] Encrypted information also may be sent between the integrated circuit 712 and a cryptographic processor 722 in a key manager 724 in the access server 704 via the communication link 726. In this case, the cryptographic processors may perform key exchange and encryption, decryption and/or authentication operations as necessary to send and receive the encrypted information and provide the information in the clear for internal processing.

[0138] In general, the form of protection provided within the system may depend on the requirements of a given application. For example, specifications such as FIPS-140-2 define various levels of security that may be implemented within a system

[0139] The security boundary provided by the integrated circuit 712 and the cryptographic boundary 718 may be used to provide a secure mechanism for authenticating a user to access a service. For example, credentials received from the RFID token 742 may be provided directly into an integrated circuit on the input device 716 via RF signals 744.

[0140] Once the information is in the integrated circuit on the input device 716 it may be protected by the physical boundary of the integrated circuit and by a cryptographic boundary (not shown). For example, provisions may be made to ensure that the information does not appear in the clear outside of the integrated circuit. The information may

then be securely sent to the access device 702 via what may otherwise be an insecure link 730.

[0141] Credentials received from the input device 716 may be provided directly into the integrated circuit 712 via RF signals 730. Once the information is in the integrated circuit it may be protected by the physical boundary of the integrated circuit and by the cryptographic boundary 718. Thus even if rogue software in the system were to gain access to the information outside of the chip 712, the software would not be able to decrypt it without appropriate key information. However, the key information also may be protected within the integrated circuit 712 and the cryptographic boundary 718. That is, the key information may not appear in the clear outside of the security boundary. As a result, the credentials may be securely routed to the access server 704.

[0142] Moreover, via this secured mechanism, the access device 702 may reliably authenticate to the access server 704 that a specific RFID token 742 is proximate the input device 716. First, as discussed above, the credentials may be received in a secure manner. Second, the effective "decision" as to whether the token 742 is adjacent may be made within a security boundary. The security module 708 may then cryptographically sign this information using a secure protocol set up between it and the cryptographic processors 722 of the key manager 724. Via this signature the access server 704 may be assured that a given message came from a specific processing system (e.g., access device 702) and that the message has not been compromised. Accordingly, proximity of the token 742 to the input device 716 may be used as a reliable method of authorizing access to a secured service provided by the service provider.

[0143] Referring again to FIG. 8, an example of operations that may be used to access a service will be described. As represented by block 804, when the RFID token 742 is within an appropriate range of the input device 716, the RFID reader 728 will receive an RFID signal 744 from the RFID token 742. As discussed above, the RFID signal 744 may be received by the input device 716 within a security boundary.

[0144] As represented by block 806, the system 700 may be configured so that any information contained within the broadcast RFID signal may be extracted only within a security boundary. For example, as shown in FIG. 7, the RFID reader 728 that extracts the credentials from the RFID signal 744 may be located within an integrated circuit that includes other functionality to protect the credentials. For example, the integrated circuit may include a security module 746 that encrypts/signs the credential (block 808) to prevent the information from being sent out of the integrated circuit in the clear. Here, the cryptographic processor in the security module 746 may use a private key to encrypt the information. A public key associated with this private key may be published with a certificate from a trusted entity. This certificate serves to verify that the public key is authentic. Cryptographic processing in the access device 702 may then use the public key to verify the signature of information received from the security module 746.

[0145] A similar secure process may then be used to send the information to the access server 704. A complementary process may be used to securely send information in the other direction across the link 726.