

[0117] The input device 716 and the access device 702 may incorporate security mechanisms to ensure that the credentials provided by a user may be secured when the credentials are maintained within and sent from these devices. For example, the input device may provide a security boundary within which any sensitive information (e.g., credentials received from the token and keys received from the access device) may be used and maintained in a secure manner. In addition, the access device may provide a security boundary to protect any sensitive information (e.g., keys and credentials)

[0118] To this end, these devices may include security modules 708 and 746 that provide cryptographic processing to, for example, sign and/or encrypt the credentials. In some embodiments information may only pass between the reader 728 and the security module 746 via a connection within a common integrated circuit. Thus, the input device may be configured so that the credentials never leave the integrated circuit in the clear.

[0119] In addition, the access device 702 may be in secure communication with the access server 704. For example, a cryptographically secured communication channel 718 may be established between the security module 708 and the access server 704. In this case, the security module 708 may process (e.g., encrypt/sign) the credentials before sending them to the access server 704. Accordingly, the security modules may provide strong authentication that the credentials are from a specific token 742 that is proximate that particular input device 716 that, in turn, is relatively proximate a specific access device 702.

[0120] After the access server 704 has received authenticated credentials from the access device 702, the access server may provide access to the requested service. As used herein the term service may include, for example, access to data and/or a data processing service. Thus, a service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such as security associations and keys, access a web page, access a data network or access a processing application.

[0121] As used herein the term data may include any information that may be accessed by a computing device including, for example, data files, passwords and cryptographic security associations including keys.

[0122] As used herein the term access may include, for example, acquiring, using, invoking, etc. Thus, data may be accessed by providing a copy of the data to the access device. Data also may be accessed by enabling the access device to manipulate or use the data. As an example of the latter, once a user has been authorized to access a service a trusted platform module may use keys to perform operations for the user. For a data network, access may include, for example, sending and/or receiving data over the network. For a processing application access may include, for example, invoking, interacting with or using the application or loading the application onto the access device.

[0123] An access server may comprise hardware and/or software that facilitate providing a service. For example, an access server may consist of a processing system that processes requests for service, verifies whether the requester is authorized to access the service and provides or facilitates the requested access.

[0124] In practice, an access server may be located local or remote with respect to the entity requesting service (e.g., access device 702). For example, a local trusted platform module may control access to passwords in a computing system. In addition, a remote wireless access point may control a computing system's access to a data network connected to the access point.

[0125] An access device may comprise hardware and/or software that facilitate access to a service. For example, an access device may comprise a computing system such as, without limitation, a personal computer, a server, a cellular phone, a personal data assistant ("PDA"), etc.

[0126] For convenience, FIG. 7 only depicts one token, input device, access device and access server. It should be understood, however, that a system may include any number of these components. For example, a user may use a token to access one or more services via one or more access devices. Thus, an access device may access services from multiple access servers. Also, multiple access devices may access the services provided by a given access server.

[0127] Authorization to access a service may depend on the specific token and access device being used. For example, a user may be assigned one token to access certain services through certain access devices. In addition, the user may be assigned another token to access other services through the same or other access devices. Also, multiple sets of information (e.g., credentials) may be included on a single token to enable a user to access different services or to enable multiple users to share a token.

[0128] A wireless proximity reader and token may be implemented using one or more of a wide variety of wireless proximity techniques. For example, the proximity reader and the token may support, without limitation, one or more of RFID, ISO 14443 and ISO 15693.

[0129] Tokens may be implemented in various physical forms depending upon the needs of the respective applications. For example, a token may be in a form that is easy to carry, similar to a plastic credit card, a "smart card" or a building access card. Also, a token may take the form of a tag or a label that may be attached to another article.

[0130] Examples of tokens may include, without limitation, smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc. In some embodiments, the token includes circuitry used in a typical smart card. For example, the token may store an encrypted password that may be sent to an authentication system.

[0131] Referring now to FIG. 8 additional details of operations and configurations in a proximity-based authentication system will be described. As represented by block 802, a security boundary is provided within the input device 716 and the access device 702 to, for example, secure the process of gaining access to a service, including securing the authentication process and information used during the authentication process. This security boundary may be established, for example, using hardware and/or cryptographic techniques.

[0132] Hardware techniques for providing a security boundary may include, for example, placing components within a single integrated circuit. As shown in FIG. 7 an RF