

[0014] In one aspect the invention relates to authenticating a user to access a service provided by or accessible via an access device (e.g., a computing device). For example, the user may access data stored on the access device or on a remote computing device. The user also may access applications running on the access device or on remote servers. In addition the user may gain access to a data network via the access device.

[0015] In one aspect of the invention, credentials for gaining access to the service are provided to an input device that is proximate the access device. Cryptographic techniques may then be used to authenticate and/or protect the credentials.

[0016] In some embodiments, a secure communication mechanism may be established between the input device and the access device for transmission of the credentials. For example, a user may initially provide the credentials to the input device in a secure manner. In some embodiments this may include entering the credentials into a security boundary in the input device. A cryptographic processing component in the input device may then cryptographically encrypt and/or sign the credentials within the security boundary. Here, the authenticity of the signing/encrypting may be verified to the access device by a published digital certificate. The input device then provides the signed/encrypted credentials to the access device.

[0017] The access device may then provide the credentials to a service provider to gain access to a service. In some embodiments, a secure communication mechanism may be established between the access device and the service provider. For example, a cryptographic processing component in the access device may cryptographically encrypt and/or sign the credentials within a security boundary. Here, the authenticity of the signing/encrypting may be verified to third parties (e.g., a service provider) by a published digital certificate. The access device then provides the signed/encrypted credentials to a service provider.

[0018] The service provider may validate that the credentials originate from a specific access device. For example, a cryptographic processor in the service provider may use the access device's public key to cause the access device to prove that it has the corresponding private key. In addition, since the service provider has access to a certificate for the public key, assurance may be provided that the access device has a mechanism for protecting keys and that the private key of the access device was not exposed outside of the security boundary. Consequently, a high level of assurance that the credentials came from a specific and/or trusted access device that is currently being used by an authorized user (as authenticated by the cryptographic processing in the input device) may be provided to the service provider.

[0019] In some embodiments authentication may be used to verify that a user is in the proximity of the access device. For example, an authorized user may be provided access to a service only when a wireless token assigned to the user is in the proximity of the input device which in turn is in relative proximity to the access device through which access to the secured service is obtained. In this way, a reasonable assumption may be made that the authorized user is in fact using a specific access device to request the service.

[0020] In some embodiments an input sensor is implemented within a security boundary on the input device. In

this way, the credential may be passed via the input sensor directly to the security boundary of the input device then passed securely to the access device. As a result, the credentials may be passed to the access device without being routed via software messages or applications. As a result, the credentials may not be intercepted by a hacker or computer virus that may have compromised the software executing on the access device.

[0021] In some embodiments the input device comprises a proximity authentication system such as an RFID system. For example, a user's credentials may be stored on an RFID token and the input device may include an RFID reader. In this case, the RFID reader reads the credentials when the RFID token is proximate the input device.

[0022] In some embodiments the input device may comprise a biometric sensor such as a fingerprint reader. In this case, the credentials may include biometric information (e.g., a scan of a fingerprint).

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] These and other features, aspects and advantages of the present invention will be more fully understood when considered with respect to the following detailed description, appended claims and accompanying drawings, wherein:

[0024] **FIG. 1** is a simplified block diagram of one embodiment of an authentication system constructed in accordance with the invention;

[0025] **FIG. 2** is a flow chart of one embodiment of authentication operations that may be performed in accordance with the invention;

[0026] **FIG. 3** is a simplified block diagram of one embodiment of a user authentication system constructed in accordance with the invention;

[0027] **FIG. 4** is a flow chart of one embodiment of user authentication operations that may be performed in accordance with the invention;

[0028] **FIG. 5** is a simplified block diagram of one embodiment of a user authentication system constructed in accordance with the invention;

[0029] **FIG. 6** is a flow chart of one embodiment of user authentication operations that may be performed in accordance with the invention;

[0030] **FIG. 7** is a simplified block diagram of one embodiment of a proximity-based authentication system constructed in accordance with the invention;

[0031] **FIG. 8** is a flow chart of one embodiment of proximity-based authentication operations that may be performed in accordance with the invention;

[0032] **FIG. 9** is a simplified block diagram of one embodiment of an access device constructed in accordance with the invention;

[0033] **FIG. 10** is a simplified block diagram of one embodiment of a processing system constructed in accordance with the invention;

[0034] **FIG. 11** is a simplified block diagram of one embodiment of a security module constructed in accordance with the invention;