

key provides a mechanism to securely receive, use and maintain keys. Thus, the certificate serves to strongly verify the authenticity of any information provided by an access device that has the corresponding private key.

[0079] In some embodiments, the access device and the access server may use the asymmetric key to negotiate one or more other keys that may be used for cryptographic processing. For example, these other keys may be used to encrypt, decrypt, sign, etc., information sent between these components. In this way, a secure channel (represented by dashed lines 316) may be established between the access device and the access server. That is, each component will have one or more keys that enable it to decrypt encrypted information that it received from the other component. In this way, sensitive information (e.g., keys) may be securely sent over a link 318 that may not otherwise be secure.

[0080] Referring now to block 404, to enable the access server to recognize the credentials assigned to a given user, the credentials are enrolled (e.g., entered into) the access server. This may be accomplished, for example, using a credential enrollment mechanism 320. In some embodiments the credential enrollment mechanism may comprise a keyboard and monitor console for the server. In some embodiments the credential enrollment mechanism 320 may be inside a security boundary associated with and enforced by the key manager 310. For example, the credential enrollment mechanism 320 may comprise a keyboard that is physically attached to the key manager, an RFID reader, a biometric sensor, etc. Additional details of these types of components are discussed below.

[0081] The credential enrollment mechanism 320 provides the credential information to the key manager 310 which may then generate one or more keys associated with that credential. These keys may comprise, for example, SSL or IPsec keys/security associations that may enable the user to log onto a security network. The key manager may then maintain a database that associates each authorized user's credential (e.g., credential A) with key(s) and certificate(s) (e.g., key A) that may be generated for that user.

[0082] The credentials and the associated key(s) may be stored in a secure data memory 322. In some embodiments the data memory 322 may be protected within a physical security boundary of the key manager 310. For example, the database 322 may be located within a secure enclosure and/or within the same integrated circuit as the key manager. In some embodiments the data memory 322 may be located external to the key manager. In this case, however, the key manager may encrypt the keys before they are stored in the data memory.

[0083] Referring to block 406, when a user wishes to access a service via the access device 302, the user presents his or her credentials 308 to the access device. As discussed above, the credentials 308 are provided to the access device via a proximate input device.

[0084] In some embodiments credentials may be provided from the input device to the access device via a direct path into the security boundary of the access device. For example, in the access device 304 credentials 332 may be directly entered (as represented by dashed line 334) into a device located within a security boundary 336. This may be accomplished, for example, using a wireless interface that is physically attached to a component within the security boundary.

[0085] Referring to block 408, the access device 302 sends the credentials 308 to the access server 306 via the secure channel 316 discussed above. For example, a cryptographic processor 328 may use a key obtained from the negotiation with the access server 306 discussed above to encrypt the credentials. Typically, the cryptographic processor(s) 328 sign the credentials using such a key or the private key 314.

[0086] At block 410, cryptographic processor(s) 324 in the access server 306 process the encrypted/signed credentials. Through this cryptographic process, the access server obtains strong authentication that the credentials are from a user that is using a specific access device 302. Moreover, assurances may be made via the certificate that an input device (e.g., keyboard, sensor, RFID components, etc.) through which a user inputs credentials is proximate to that access device.

[0087] The access server 306 then checks the credential database to verify that the credentials are associated with an authorized user. For example, the access server may determine whether the credential matches a credential (e.g., credential A) stored in the data memory 322.

[0088] If so, the access server 306 generates or retrieves the key (e.g., key A) that corresponds to that credential. The access server then sends the key to the access device 302 (block 412). Typically, the cryptographic processor 324 will encrypt the key to protect it during transmission. Here, the cryptographic processor may use a negotiated key or the public key associated with the private key 314 to encrypt key A.

[0089] Once the access device 302 receives encrypted key A, the cryptographic processor 328 decrypts the key and stores decrypted key A 340 within the security boundary 312. Here, the cryptographic processor 328 may use a negotiated key or the private key 314 to decrypt key A. The access device 302 may then use key A 340 to, for example, establish a connection with a network (block 414).

[0090] If desired, the user may then use another access device (e.g., access device 304) to access the network. Again, the user presents his or her credentials (e.g., the same credentials referred to above) to access device 304 via the input device (not shown). Cryptographic processor(s) 342 may then encrypt/sign the credentials and send them to the access server via a secure channel 346 over a link 348 that may not otherwise be secure. Again, an asymmetric identity key 344 may be used to establish the secure channel 346, form the basis of a digital certificate, sign credentials, etc. The access server 306 then verifies the credentials. Here, since the access server has received the same credentials it may assume that the same user has authenticated to the access device 304. Accordingly, the access server sends the same key (e.g., key A) to the access device 304 via the secure channel 346, thereby binding these access devices together. The cryptographic processor 342 decrypts encrypted key A and stores decrypted key A 350 within the security boundary. Access device 304 may then use key A to connect to a network or access another service.

[0091] In addition, more than one set of credentials may be presented to a given access device to access a network. For example, multiple users that are assigned different credentials may share an access device. In addition, the same user may have different credentials that provide access to differ-