

credentials assigned for access to another network. Referring to FIG. 5, the devices 514 and 516 may be used to connect to an enterprise LAN at the user's office. In this case, the second set of credentials may be provided to the office network 534 via the WAN 502 and other routing mechanisms 532. Once the appropriate keys are exchanged, an enterprise virtual private network ("VPN") or other form of connection may be established between the access device and the office network 534. Again, this network may be entirely separate and cryptographically secured from any other network connections for that user or any other user of the system.

[0104] Blocks 624-628 illustrate that the network may be continued to be automatically built as other users provide his or her credentials to multiple access devices in the system. As represented by block 624, user B may provide his or her credential to another access device (referred to for convenience as "access device 3"). The access device 3 sends the credential to the access server and, after the access server verifies that the credential has been enrolled, the access server sends associated key(s) to the access device 3 (block 626). Access device 3 may then use the key(s) associated with user B to connect to the network (block 628).

[0105] The system described above may provide several advantages as compared to conventional systems. Traditional networks may only provide device level authentication that is achieved by manually configuring the head end and all devices that may connect to the network. For example, the router may be configured by an administrator physically connected to a LAN port of the router. Here, the administrator may enter in the keys for the router and identify each of the devices that may connect to the router. In addition, the administrator may manually configure each device in the network with the necessary key to enable the device to connect to that specific router.

[0106] In contrast, a network constructed using the teachings described herein may be automatically built by binding components (e.g., access devices) together as a user authenticates himself or herself to these components. This is facilitated, for example, by the ability to securely authenticate at the system level. For example, the proximity of the user may be verified as well as the ability of a security module to protect keys (e.g., using appropriate hardware).

[0107] A variety of secure techniques may be used to authenticate a user to a device. For example, a credential may be provided via a direct connection into an input device, credentials may be injected into a security boundary of a device via RFID signals or a sensor may be physically located within a security boundary of a device.

[0108] Here, the network may be built using digital certificates based on public/private keys pairs. This process may be initiated by using a private key that is protected on each component and may provide a secure environment where the components may dynamically change the keys.

[0109] In addition, each user does not need access to the keys that identify that user since the user does not need to pre-configure each device with the appropriate key. Instead the user may only present information such as a credential to obtain access to the network via a given device.

[0110] Moreover, a system may be configured to provide multiple networks. Each of these networks may include a

given set of components that are defined for different users and/or for different permission levels for a given user. These networks may be secured from one another by using cryptographic techniques to authenticate access to each network and secure the data flowing through each network.

[0111] Referring now to FIGS. 7-10, several embodiments of mechanisms for providing credentials to a device will be discussed. In general, the following description describes providing credentials to an access device. However, these mechanisms also may be used to provide credentials to an access server or some other component in a system.

[0112] FIG. 7 illustrates one embodiment of a system 700 where selected services may be provided to a user via a computing device when a wireless token assigned to a user is proximate to the input device. An input device 716 includes components that may be used to determine whether a wireless token (e.g., an RFID token) 742 assigned to a user or users is proximate to the input device 716. For example, a wireless proximity reader (e.g., an RFID reader 728) may be configured to receive signals 744 (e.g., RF signals) from the wireless proximity token 742. The signals 744 may include information that uniquely identifies the wireless proximity token 742. For example, this information may include one or more credentials (e.g., a password) that may be used to access a secured service through an access server 704.

[0113] The determination of proximity between the token 742 and the reader 728 may be established using a variety of mechanisms depending on the application. In some embodiments, the token will not generate signals until it is within a given distance of the reader. This may be accomplished, for example, by using a relatively passive token that intercepts signals transmitted by the reader and transmits signals in response to the received signals. Different distances between the token 742 and the reader 728 may be defined as indicative of proximity depending on the requirements of the application and, in some cases, characteristics of the operating environment.

[0114] RF interfaces (e.g., Bluetooth interfaces) 736 and 706 and associated antennas 734 and 732 may then be used to send the credentials from the input device 716 to the access device 702 via RF signals 730. The RF interfaces also may be used for other communications between the input device 716 and the access device 702.

[0115] An access device 702 such as a computer may request access to a service from the access server 704 by sending a request over a communication link 726. Depending upon the particular application, the communication link 726 may comprise, for example, electric wires, optical cables or air. Thus, the access device 702 may support wired or wireless communications with the access server 704.

[0116] Typically, access to the service will be initiated by the user's interaction with the access device 702. For example, the user may use a keyboard or pointing device (e.g., a computer mouse) to access the service. In conjunction with this the user may be required to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric sensor to verify the authenticity of the user. In this way, access to a service may be withheld until the user provides adequate credentials including, for example, what the user knows (e.g., a password), what the user possesses (e.g., a token) and who the user is (e.g., a physical or biometric characteristic).