

herself to the TPM. This may involve, for example, providing the original password to the TPM. To this end, the processing system **1002** may include an input device **1006** that is connected to the TPM via a link **1008**.

[**0161**] In some embodiments, the link may be routed directly from the input device to the TPM to ensure that data may be securely sent over the link. For example, data from this link may not be routed using software routines such as operating system calls. In addition, data from the link may not be stored in data memory that is accessible by other components in the system. For example, the data may not be sent through a software stack and may not be stored in a data memory that is accessed via an internal bus such as a PCI bus. Consequently, input information may be passed to the TPM without being compromised by viruses, hackers, etc., that may have compromised the system. In some embodiments an additional degree of protection may be provided by physically embedding or attaching the input device **1006** within/to the processing system.

[**0162**] Through the use of physical and cryptographic techniques the TPM securely uses and maintains sensitive information such as these credentials within its security boundary. After verifying the credentials (e.g., comparing the received credentials with previously enrolled credentials) within the security boundary, the TPM **1004** may provide the requested access or may facilitate acquiring access to a service from another processing entity.

[**0163**] In some embodiments a user may authenticate himself or herself to the TPM to use keys stored within the security boundary of the TPM. For example, the system of **FIG. 10** may be used to access encrypted data (e.g., an encrypted password) stored in a local data memory (e.g., file storage **1012**). In this case, the TPM **1004** may store cryptographic information (e.g., keys, security associations, etc.) that enables the TPM to decrypt encrypted data. In a typical case, once the user is authenticated, the TPM will use the key within its security boundary, then provide the results to the user. For example, the TPM may return decrypted data (e.g., media content) or signed data to the user. In this way, the keys may be used without exposing the keys in the clear outside the security boundary of the TPM.

[**0164**] In the event there is insufficient storage for the keys in the TPM, the TPM may encrypt the keys and send them to an external data storage component (e.g., file storage **1012**). Thus, even if the encrypted data files in the file storage **1012** may be accessed by other components in the system the security of the encrypted data may be maintained because the keys are encrypted. In other words, sensitive information is only used in the clear within the security boundary of the TPM.

[**0165**] In some embodiments the TPM **1004** may control access to one or more data networks **1022** that are accessed via a network interface **1010**. Here, the TPM **1002** may provide network authentication credentials (e.g., a certificate) to a service provider (e.g., an access point, not shown) connected to a network to authenticate it to the service provider. These network authentication credentials may be securely stored in a data memory (not shown) in the TPM **1004** or stored in encrypted form in the file storage **1012**.

[**0166**] The network interface **1010** may be used to connect to wired and/or wireless network(s). As discussed herein,

cryptographic techniques may be used to ensure the security of data transferred between the TPM **1004** and other devices connected to the network. Accordingly, a network connection may be used, for example, to communicate with a key manager to obtain key information (e.g., security associations) and authorization for key usage.

[**0167**] Input device **1014** depicts another embodiment of an input device that may be used to securely provide information (e.g., credentials) to the processing system. The input device **1014** includes a security module **1018** and keys **1020** implemented within a security boundary to provide cryptographic functionality. For example, the security module may be used to encrypt/sign information (e.g., credentials) entered into the input device. In this way, this information may be securely sent (as represented by dashed line **1016**) to the TPM **1004**.

[**0168**] The security module **1018** and the trusted platform module **1004** may include components and perform operations as discussed herein to provide strong authentication and establish a secure channel. For example, a public key and associated certificate may be published for the security module **1018** to enable the TPM to verify the authenticity and the security of the input device using techniques as discussed herein. As a result, a secure channel **1016** may be established between these components such that the security boundary of the TPM may, in effect, be extended to include the input device **1014** and the secure channel.

[**0169**] Since information sent between the components may be secured in this manner, the input device **1014** does not need to be securely connected to the processing system. Thus, the input device **1014** may be advantageously used in applications where the input device is remote from the processing system **1002** and connected to the processing via, for example, a wired or wireless interface such as a network. In addition, the input device may be advantageously used in applications where the input device may be connected to the TPM via an insecure link (e.g., a USB link in a computer).

[**0170**] In some embodiments, the input mechanism (e.g., a key pad, a sensor, etc.) on the input device **1014** may be connected in a secure manner to the security module **1018**. For example, the input mechanism may be located on the same integrated circuit as the security module. In addition, these components may be implemented within a physically protected enclosure. Accordingly, the security boundary of the input device **1014** may include the input mechanism, the security module **1018** and external memory (not shown) that the security module uses to store encrypted information. As a result, the input device **1014** may provide a highly secure mechanism for a user to provide credentials to the TPM **1004**.

[**0171**] Referring now to **FIGS. 11-14** selected components and operations of several embodiments of security modules will be discussed in more detail. In some embodiments a security module may provide key protection and management (e.g., enforcing proper usage of keys) required for multiple levels of key material.

[**0172**] In addition, a security module may provide cryptographic processing such as encryption, decryption, authentication, verification and signing for a device that uses cryptographic services (e.g., an access device) in which the security module is installed. For example, a security module