

[0232] Moreover, as this module only performs symmetric cryptographic processing on data from a data streaming interface, some or all of the dedicated cryptographic processors shown in **FIG. 11** (e.g., the public key processing and 3DES) may not be needed. For example, the module only performs the asymmetric key operations once after it boots up. In addition, the stateless module does not need to verify the authenticity of the recipient of the data. Accordingly, the remaining cryptographic processing operations may be performed by the master controller **1306**. In this case, the application code for cryptographic algorithms (e.g., DH, DSA, 3DES, AES) may be stored in a ROM **1308**.

[0233] The embodiment shown in **FIG. 13** may secure an incoming data stream (DI) by signing it using the SHA-1 algorithm. Accordingly, a separate processing block **1304** may be provided for this operation. The signed output of this processing **30** block provides a data stream (DO) that is sent to the recipient device via a data interface **1302**. In an embodiment that also encrypts the data stream, a dedicated processing block (not shown) may be provided to implement, for example, a symmetric encryption algorithm.

[0234] Referring now to **FIG. 14**, an example of operations that may be performed by one embodiment of a stateless secure link module will be discussed. As represented by blocks **1402-1408**, a stateless secure link module generates a public-private key pair, stores the private (e.g., identity) key in nonvolatile memory within the security boundary, exports the public key and establishes a secure communication channel with, for example, a key manager.

[0235] As represented by block **1410** the key manager may send symmetric keys to the stateless secure link module via the secure communication channel. For example, the key manager may send symmetric keys that are used to encrypt and/or sign data that the stateless secure link module receives from an input device. The cryptographic processors may then decrypt these keys (block **1412**) and store the decrypted keys (block **1414**) within the security boundary associated with the stateless secure link module.

[0236] As represented by block **1416**, the stateless module may receive data to be encrypted from an input component. As discussed above the input component may be, for example, a biometric sensor, a sensor for a camera, etc., or any other device that needs data to be authenticated or securely transmitted to another (e.g., remote) device (e.g., the recipient device).

[0237] As represented by blocks **1418**, the stateless module uses the symmetric keys within the security boundary to encrypt the data. Then, as represented by block **1420**, the stateless module sends the encrypted data to the remote device.

[0238] In some embodiments the symmetric key may be injected into the stateless module during manufacture (e.g., during chip test). In this case, all or a portion of the external interface **1312**, the RNG **1316** and the asymmetric key processing circuitry may not be needed. Accordingly, in some embodiments a stateless module may simply include a relatively small master controller for injecting the symmetric key and perform other basic operations, a nonvolatile memory, a data buffer memory, a cryptographic processor for the symmetric key operations and optionally, assurance logic.

[0239] Additional details of security modules are disclosed, for example, in commonly-owned U.S. patent application Ser. No. 10/_____, filed Jun. 21, 2005, entitled STATELESS HARDWARE SECURITY MODULE, Attorney Docket No. 53028/SDB/B600, the disclosure of which is hereby incorporated by reference herein.

[0240] It should be appreciated that the various components and features described herein may be incorporated in a system independently of the other components and features. For example, a system incorporating the teachings herein may include various combinations of these components and features. Thus, not all of the components and features described herein may be employed in every such system.

[0241] Different embodiments of the invention may include a variety of hardware and software processing components. In some embodiments of the invention, hardware components such as controllers, state machines and/or logic are used in a system constructed in accordance with the invention. In some embodiments code such as software or firmware executing on one or more processing devices may be used to implement one or more of the described operations.

[0242] Such components may be implemented on one or more integrated circuits. For example, in some embodiments several of these components may be combined within a single integrated circuit. In some embodiments some of the components may be implemented as a single integrated circuit. In some embodiments some components may be implemented as several integrated circuits.

[0243] The components and functions described herein may be connected/coupled in many different ways. The manner in which this is done may depend, in part, on whether the components are separated from the other components. In some embodiments some of the connections represented by the lead lines in the drawings may be in an integrated circuit, on a circuit board and/or over a backplane to other circuit boards. In some embodiments some of the connections represented by the lead lines in the drawings may comprise a data network, for example, a local network and/or a wide area network (e.g., the Internet).

[0244] The signals discussed herein may take several forms. For example, in some embodiments a signal may be an electrical signal transmitted over a wire, light pulses transmitted through air or over an optical fiber or electromagnetic (e.g., RF or infrared) radiation transmitter transmitted through the air.

[0245] A signal may comprise more than one signal. For example, a signal may consist of a series of signals. Also, a differential signal comprises two complementary signals or some other combination of signals. In addition, a group of signals may be collectively referred to herein as a signal.

[0246] Signals as discussed herein also may take the form of data. For example, in some embodiments an application program may send a signal to another application program. Such a signal may be stored in a data memory.

[0247] The components and functions described herein may be connected/coupled directly or indirectly. Thus, in some embodiments there may or may not be intervening devices (e.g., buffers) between connected/coupled components.