

a given apparatus or method. Finally, like reference numerals denote like features throughout the specification and figures.

#### DETAILED DESCRIPTION

[0022] The invention is described below, with reference to detailed illustrative embodiments. It will be apparent that the invention may be embodied in a wide variety of forms, some of which may be quite different from those of the disclosed embodiments. Consequently, the specific structural and functional details disclosed herein are merely representative and do not limit the scope of the invention. For example, references to specific structures and processes in the disclosed embodiments should be understood to be but one example of structures and processes that may be used in these or other embodiments in accordance with the teachings provided herein. Accordingly, otherwise restrictive nomenclatures such as “is,” “are,” etc. should be understood to include less restrictive meanings such as “may be,” etc. For convenience, an embodiment of a system constructed or a method practiced according to the invention may be referred to herein simply as an “embodiment.” References to “an” or “one” embodiment in this discussion are not necessarily to the same embodiment, and such references mean at least one.

[0023] FIG. 1 illustrates one embodiment of a secure system 100 constructed in accordance with the invention. A computing system 102 includes a processor 104, a first data memory 106, an instruction control module 108 and one or more cryptographic engine(s) 110. In a typical embodiment the computing system 102 comprises a single integrated circuit (i.e., chip). A second data memory (e.g., an external memory) 112 connects to the computing system 102 via a data bus 114.

[0024] In general, as treated herein the first data memory has some attribute that makes it impossible or undesirable to alter its contents after it has been deployed in the field. Typically, the first data memory is not reprogrammable. For example, it may be a read-only memory (“ROM”). In addition and/or alternatively, the first data memory may have an attribute of being located within an associated computing system (e.g., TPM) and/or on the same integrated circuit as the associated computing system. These or other attributes may make it impossible or undesirable to alter the contents of the memory. For convenience, the terms internal memory, internal ROM, on-chip memory, on-chip ROM and instruction ROM may be used herein to refer to a memory having one or more of these or related attributes.

[0025] In general, as treated herein the second data memory refers to a memory that is reprogrammable. Such a memory also may have a characteristic of being located outside of an associated computing system (e.g., TPM) and/or on a different integrated circuit than the associated computing system. For convenience, the terms external memory, external flash, flash memory, off-chip memory and off-chip flash may be used herein to refer to a memory having one or more of these or related attributes.

[0026] In some embodiments the first data memory (e.g., an instruction memory) 106 stores operating code (e.g., functions) 116 and a function table 118 that may be used to determine where a given function resides in the data memory 106. When the data memory 106 comprises an

internal memory the instruction code 116 and function table 118 may be loaded into the internal memory when the chip is manufactured.

[0027] In some embodiments once the system 100 is deployed in the field (e.g., in a personal computer, a server, etc.), the operating code for the computing system 102 may be upgraded by downloading new operating code (e.g., functions) 120 and a corresponding function table 122 into the second data memory 112. For example, the new operating code 120 may contain one or more new functions and/or modified versions of one or more of the original functions 116. In this case the new function table 122 may specify the locations of the original, unmodified functions 116 and the locations of the new and/or modified functions 120. The instruction control module 108 may be used to assist the processor 104 in efficiently obtaining the appropriate code from a storage location in either the data memory 106 or the data memory 112.

[0028] In some embodiments the cryptographic engine(s) 110 may be used to cryptographically verify and protect the operating code 120 and the function table 122. For example, the cryptographic engine(s) 110 may be used to verify that any new operating code and function tables received by the system 100 are from a trusted source. In some embodiments this may be accomplished by verifying a cryptographic signature over the received code and function table. In addition, the cryptographic engine(s) 110 may be used to encrypt, decrypt and authenticate the operating code 120 and function table 122 that are stored in the data memory 112. By encrypting the information before storing it in the data memory 112 the computing system 102 may prevent unauthorized access to the operating code and function table stored in the data memory 112. In addition, by authenticating information retrieved from the data memory 112, the computing system may verify that any operating code 120 and function table 122 retrieved from the data memory 112 has not been tampered with or replaced by unauthorized persons or programs.

[0029] In some embodiments the trusted source may comprise an external (e.g., remote) secure signing environment 124. The environment 124 may be, for example, a FIPS Level 3 environment such as a hardware security module that provides a secure mechanism to provide data to one or more computing systems 102. This data may include, for example, new code, a function table for the new code, a secure code descriptor (e.g., including keys to be used by the computing system) and other information. The environment 124 may include cryptographic and/or physical mechanisms to protect the data to be sent to the computing system 102 and keys used by the environment 124. For example, the environment 124 may securely maintain a private key 126 that is used sign and/or encrypt the data. A corresponding public key may then be securely loaded into the computing system 102.

[0030] In this way, the computing system 102 may use the public key to verify the authenticity of any received data. For example, the environment 124 may sign new secure code and a new function table using the private key 126 and send the resulting signed data to the computing system via a communication link 128. The computing system may then use the public key to verify that the signed data is from a trusted source.