We claim:

~~1. A method of accessing data (295) stored on a storage device (270) comprising a communicational connection to a access control device (170) comprising access control information (176), the method comprising the steps of:~~

~~receiving an indication from the storage device (270) that the access control device (270) is communicationally connected to the storage device (270);~~

~~establishing a communicational connection with the access control device (170) through the storage device (270);~~

~~providing, to the access control device (270), identifying information; and~~

~~receiving meaningful responses to data storage related requests after the access control device (270) allows the storage device (270) to do so at least in part because of the provided identifying information.~~

~~2. The method of claim 1, wherein the storage device comprises a hardware cryptographic system and the access control device comprises storage-related cryptographic information; and wherein further the receiving the meaningful responses to the data storage related requests occurs after the access control device provides access to the storage-related cryptographic information to the hardware cryptographic system of the storage device.~~

~~3. The method of claim 1, further comprising the steps of receiving an authentication challenge from the access control device, wherein the providing identifying information to the access control device comprises providing, to the access control device, an authentication response to the authentication challenge.~~

~~4. The method of claim 1, further comprising the steps of:~~

~~receiving, from the access control device, a first information to be provided to an authentication computing device external to the access control device;~~

~~establishing a communicational connection with the authentication computing device;~~

~~providing the first information to the authentication computing device;~~

~~receiving, from the authentication computing device, a second information to be provided to the access control device; and~~

~~providing the second information to the access control device.~~

~~5. The method of claim 4, comprising further comprising the steps of: establishing a communicational connection to a network and receiving, as part of the establishing the communicational connection to the network, a network address of the~~

~~authorization computing device; wherein the establishing the communicational connection with the authentication computing device comprises establishing a network communicational connection with the authentication computing device utilizing the received network address of the authorization computing device.~~

~~6. The method of claim 4, further comprising the steps of implementing a virtual process to act as the authentication computing device; wherein the establishing the communicational connection with the authentication computing device comprises establishing a communicational connection with the virtual process.~~

~~7. One or more computer-readable media having computer-executable instructions for performing the steps of claim 1.~~

~~8. An access control device (170), physically and communicationally separable from a storage device (270), the access control device comprising:~~

~~at least one communicational interface;~~

~~at least one processing unit (171); and~~

~~access control information (176) utilizable by the at least one processing unit (171) to selectively enable the storage device (270) to meaningfully respond to data storage related requests.~~

~~9. The access control device of claim 8, further comprising storage-related cryptographic information utilizable by a hardware cryptographic system of the storage device to decrypt encrypted data stored by the storage device; wherein the access control information is further utilizable by the at least one processing unit to selectively provide the storage-related cryptographic information to the storage device.~~

~~10. The access control device of claim 9, wherein specific ones of the storage-related cryptographic information are utilizable by the hardware cryptographic system to decrypt only portions of the encrypted data of the storage device, the portions corresponding to individual users; wherein the access control information comprises identifications of the individual users; and wherein further the at least one processing unit causes the provision of at least some of the specific ones of the storage-related cryptographic information if the at least one processing unit receives authentication from at least some of the individual users as specified by the access control information.~~

~~11. The access control device of claim 9, further comprising instructions executable by the at least one processing unit to erase the storage-related cryptographic information.~~

~~12. The access control device of claim 8, wherein the access control information comprises one or more identities of one or more entities for which the processing unit is to enable the storage device to meaningfully respond to data storage related requests from the one or more entities.~~

~~13. The access control device of claim 8, wherein the at least one processing unit performs steps comprising:~~

~~receiving identity information and authentication information from an entity;~~

~~comparing the received identity information to the access control information;~~

~~if the received identity information is listed in the access control information, comparing the received authentication information to a corresponding authentication information listed in the access control information; and~~

~~if the received authentication information matches the corresponding authentication information listed in the access control information, instructing the storage device to meaningfully respond to the data storage related requests by performing actions requested by the data storage related requests.~~

~~14. The access control device of claim 8, wherein the access control information comprises access control cryptographic information for establishing a secure communicational tunnel with an authorization computing device external to the access control device.~~

~~15. The access control device of claim 14, wherein the at least one processing unit performs steps comprising:~~

~~utilizing the access control cryptographic information to establish the secure communicational tunnel with the authorization computing device;~~

~~providing, to the authorization computing device, through the secure communicational tunnel, information regarding entities associated with an attempted access of the encrypted data;~~

~~receiving, from the authorization computing device, through the secure communicational tunnel, an indication regarding the enabling of the storage device to meaningfully respond to the data storage related requests; and~~

~~selectively enabling the storage device to meaningfully respond to the data storage related requests in accordance with the indication received from the authorization computing device.~~

1. An access control device comprising:

at least one communicational interface through which communications with a storage device comprising encrypted data are established;

at least one processing unit;

access control information comprising identifications of entities that are to be allowed by the access control device to access, in an unencrypted form, the encrypted data stored on the storage device;

storage-related cryptographic information that can decrypt the encrypted data of the storage device with which communications are established through the at least one communicational interface, wherein the storage-related cryptographic information comprises:

a first storage-related cryptographic information that can decrypt only a first portion of the encrypted data of the storage device; and

a second storage-related cryptographic information that can decrypt only a second portion of the encrypted data of the storage device, the second portion being different from the first portion; and

a computer-readable medium comprising computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to perform steps comprising:

receiving an identification of an accessing entity, from a computing device to which the storage device is communicationally coupled, the accessing entity seeking to access, in the unencrypted form, the encrypted data stored on the storage device;

comparing the received identification of the accessing entity to the access control information;

providing, in a secured manner, the storage-related cryptographic information to the storage device, thereby enabling the storage device to decrypt the encrypted data, if the comparing reveals that the received identification of the accessing entity matches at least one of the identifications of the entities that comprise the access control information;

wherein the access control device is physically separable from both the storage device and the computing device; and

wherein further the computer-executable instructions that cause the provision of the storage related cryptographic information to the storage device comprises computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to:

provide, to the storage device, only the first storage-related cryptographic information if the accessing entity is associated with the first storage-related cryptographic information; and

provide, to the storage device, only the second storage-related cryptographic information if the accessing entity is associated with the second storage-related cryptographic information.

2. The access control device of claim 1, wherein the access control information further comprises authentication information associated with at least some of the entities that are to be allowed by the access control device to access, in the unencrypted form, the encrypted data stored on the storage device;

and wherein further the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to perform further steps comprising:

receiving authentication information from the accessing entity; and

comparing the received authentication information to the access control information.

3. The access control device of claim 1, wherein the access control information further comprises access control cryptographic information for establishing secure communications with an authorization computing device, external to the access control device, from which the access control device receives updated access control information.

4. The access control device of claim 1, wherein the access control information further comprises access control cryptographic information;

and wherein further the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to perform further steps comprising:

utilizing the access control cryptographic information to establish a secure communicational tunnel with an authorization computing device through another computing device;

providing, to the authorization computing device, through the secure communicational tunnel, the received identification of the accessing entity; and

providing, in the secured manner, the storage-related cryptographic information to the storage device, thereby enabling the storage device to decrypt the encrypted data, if information received from the authorization computing device in response to the providing

the received identification of the accessing entity indicates that the accessing entity is to be granted access.

5. The access control device of claim 1, wherein the communicational interface comprises a physical connector that is connectable to a physical receptor that is part of the storage device, such that the established communications with the storage device are direct communications between the storage device and the access control device.

6. The access control device of claim 1, wherein the established communications with the storage device are indirect communications passing through the computing device to which both the access control device and the storage device are independently communicationally coupled.

7. The access control device of claim 6, wherein the computer-executable instructions causing the at least one processing unit to provide the storage-related cryptographic information to the storage device in the secured manner, further comprise computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to protect the storage-related cryptographic information prior to the providing so as to prevent the storage-related cryptographic information from being deciphered by the computing device.

8. The access control device of claim 1, wherein the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to erase at least some of the storage-related cryptographic information.

9. The access control device of claim 8, wherein the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to determine, independently of external instruction, to execute the computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to erase the at least some of the storage-related cryptographic information.

10. The access control device of claim 8, wherein the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to perform steps comprising:

receiving an instruction to delete at least some of the encrypted data stored on the storage device; and

in response to the receiving, erasing the at least some of the storage-related cryptographic information.

11. The access control device of claim 1, wherein the computer-readable medium comprises further computer-executable instructions that, when executed by the at least one processing unit, cause the at least one processing unit to provide, to the computing device, a challenge for authentication information associated with the accessing entity if the identification of the accessing entity is received.