What is claimed is:

1. A distributed key management system, comprising

a) a server;

b) a plurality of key-holding devices adapted to communicate with the server; and

c) a key-requesting device adapted to communicate with the server;

wherein each one of the plurality of key-holding devices is adapted to hold a different fragment of a private key; the server adapted to reconstruct the private key based on the fragments received from the plurality of key-holding devices; and the key-requesting device adapted to obtain the private key from the server.

2. The system of claim 1, wherein the server is further adapted to reconstruct the private key based on the fragments received from at least a part of the plurality of key-holding devices.

3. The system of claim 2, wherein the server is adapted to reconstruct the private key using Shamir's Secret Sharing algorithm over Galois Field 256.

4. The system of claim 3, wherein the private key is a random number or is constructed using a random number, and the private key is a byte array with byte value in 0-255 range.

5. The system of claim 1, wherein the key-requesting device is adapted to produce a final key based on the private key received from the server such that the server has no access to the final key.

6. The system of claim 1, wherein the server is configured to conduct an operation related to the private key only when the server has been unlocked using an encryption key held on the plurality of key-holding devices.

7. The system of claim 6, wherein the server is adapted to hold a configuration file which is compulsory for conducting the operation; the configuration file associated with a respective public key for each one of the plurality of key-holding devices; the server adapted to be unlocked using the encryption key held on one of the plurality of key-holding devices and a corresponding public key for the one of the plurality of key-holding devices.

8. The system of claim 6, wherein the server is locked when it has been restarted.

9. The system of claim 6, wherein the operation is:

a) adding a new key-holding device;

b) removing one of the plurality of the key-holding devices;

c) generating a new private key; or

d) approving a request from the key-requesting device.

10. The system of claim 1, wherein the server is configured to recalculate the fragments of the private key when a new key-holding device joins the plurality of key-holding devices, and afterwards distribute the fragments of the private key to the plurality of key-holding devices and the new key-holding device.

11. The system of claim 1, wherein the server is configured to remove one of the plurality of the key-holding devices from being able to communicate with the server when a predetermined number of other key-holding devices authorizes a removal.

12. The system of claim 1, wherein the key-holding devices are portable computing devices.

13. The system of claim 1, wherein the key-holding devices are adapted to encrypt their respective fragments using a biometric authentication.

14. A method for distributively managing keys, comprising the steps of:

a) generating a private key by a server;

b) appointing a plurality of key-holding devices;

c) splitting the private key into a plurality of fragments in accordance with a number of the key-holding devices; and

d) distributing a different one of the fragments to each one of the plurality of key-holding devices.

15. The method of claim 14 wherein the appointing step further comprises registering a first one of the plurality of the key-holding devices using a PIN; and registering the rest of the plurality of the key-holding devices by approval of all or a predefined minimum number of the plurality of the existing key-holding devices.

16. The method of claim 14, further comprises the step of recalculating the key fragments when a new key-holding device joins the plurality of key-holding devices; and afterwards distributing the private key to the plurality of key-holding devices and the new key-holding device.

17. A method for reconstructing a private key from a plurality of key-holding devices, comprising the steps of receiving fragments of the private key from the plurality of key-holding devices by a server; and reconstructing the private key by the server.

18. The method of claim 17, wherein in the reconstructing step mentioned above the server reconstructs the private key based on the fragments received from at least a part of the plurality of key-holding devices.

19. The method of claim 18, further comprises the step of authenticating by a user, on each one of the plurality of key-holding devices, before sending a corresponding fragment to the server.

20. The method of claim 17, further comprises the step of producing a final key by a key–requesting device after it receives the private key from the server, such that the server has no access to the final key.