What is claimed is:

1. A distributed key management system, comprising

a) a server;

b) a plurality of key-holding computing devices adapted to communicate with the server, wherein each one of the plurality of key-holding computing devices is adapted to hold a different fragment of a private key; and

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

in response to the request for the private key, the server adapted to reconstruct the private key based on the fragments of the private key received from the plurality of key-holding computing devices,

wherein the server is configured to recalculate the private key based on the fragments of the private key when a new key-holding computing device joins the plurality of key-holding computing devices, and afterwards distribute the fragments of the private key to the plurality of key-holding computing devices and the new key-holding computing device and wherein the server is configured to remove one of the plurality of the key-holding computing devices from being able to communicate with the server when a predetermined number of other key-holding computing devices authorizes a removal;

the key-requesting computing device adapted to obtain the private key from the server, wherein the key-requesting computing 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; and

the server is configured to conduct an operation related to the private key only when the server has been unlocked by any one of the plurality of key-holding computing devices using a same encryption key held on all of the plurality of key-holding computing devices, wherein the server is able to read a configuration file which is compulsory for conducting the operation only when server is unlocked.

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 computing 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 plurality of key-holding computing devices are smartphones belonging to different users.

6. The system of claim 1, wherein the server is locked when it has been restarted.

7. The system of claim 1, wherein the operation is:

a) adding a new key-holding computing device;

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

c) generating a new private key; or

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

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

9. The system of claim 1, wherein the server is adapted to hold the configuration file which is associated with a respective public key for each one of the plurality of key-holding computing devices; the server being unable to read the configuration file unless it is unlocked using the encryption key by any one of the plurality of key-holding computing devices using the encryption key held on all of the plurality of key-holding computing devices.

10. 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 computing devices, wherein the appointing comprises registering a first one of the plurality of the key-holding computing devices using a PIN and registering rest of the plurality of the key-holding computing devices by approval of all or a predefined minimum number of plurality of existing key-holding computing devices;

c) splitting the private key into a plurality of fragments in accordance with a number of the key-holding computing devices and recalculating the privet key based on the plurality of fragments when a new key-holding computing device joins the plurality of key-holding computing devices and afterwards distributing the private key to the plurality of key-holding computing devices and the new key-holding computing device and wherein the server is configured to remove one of the plurality of the key-holding computing devices from being able to communicate with the server when a predetermined number of other key-holding computing devices authorizes a removal; and

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

the server is configured to conduct an operation related to the private key only when the server has been unlocked by any one of the plurality of key-holding computing devices using a same encryption key held on all of the plurality of key-holding computing devices; wherein the server is able to read a configuration file which is compulsory for conducting the operation only when server is unlocked.

11. The method of claim 10, wherein the server is adapted to hold the configuration file which is associated with a respective public key for each one of the plurality of key-holding computing devices;

the server being unable to read the configuration file unless it is unlocked using the encryption key by any one of the plurality of key-holding computing devices using the encryption key held on all of the plurality of key-holding computing devices.