CLAIMS

1. A method of reconstructing a secret by a first key unit, the method comprising:

receiving a first encrypted slice from a second key unit and a second encrypted slice from a third key unit;

sending fingerprints of the first encrypted slice and the second encrypted slice to a group authority;

in response to a validation of the fingerprints by the group authority, receiving group authority keys from the group authority;

decrypting, by the first key unit, the first encrypted slice and the second encrypted slice using the group authority keys, , wherein the first encrypted slice and the second encrypted slice are decrypted using different group authority keys;

reconstructing the secret based on the first decrypted slice and the second decrypted slice;

slicing, by the first key unit, the reconstructed secret into a first new slice and a second new slice; and

encrypting, by the first key unit, the first new slice and the second new slice with new group authority keys from the group authority, wherein a different new group authority key is used to encrypt the first new slice and the second new slice.

2. The method of claim 1, further comprising:

generating a first fingerprint of the encrypted first slice and a second fingerprint of the encrypted second slice; and

wherein the sending the fingerprints of the first encrypted slice and the second encrypted slice comprises: sending the first fingerprint and the second fingerprint to the group authority, wherein the receiving the group authority keys is in response to the group authority validating the first fingerprint and the second fingerprint.

3. The method of claim 1, further comprising:

transmitting the encrypted first new slice to the second key unit; and

transmitting the encrypted second new slice to the third key unit.

4. The method of claim 3, further comprising receiving one or more new group authority keys from the group authority, wherein the encrypting the first new slice and the second new slice is performed using the one or more new group authority keys.

5. The method of claim 3, further comprising:

generating a first new fingerprint of the encrypted first new slice;

generating a second new fingerprint of the encrypted second slice; and

transmitting the first new fingerprint and the second new fingerprint to the group authority.

6. The method of claim 3, further comprising:
receiving a third encrypted slice from the second key unit;
receiving a fourth encrypted slice from the third key unit; and
storing the third encrypted slice and the fourth encrypted slice in a slice storage.

7. The method of claim 6, further comprising:
determining that the third key unit has failed;
receiving a request from the group authority to transmit the fourth encrypted slice to a fourth key unit; and
transmitting the fourth encrypted slice to the fourth key unit.

8. The method of claim 1, further comprising:
encrypting the reconstructed secret;
storing the reconstructed secret in a secret access control unit;
receiving request from a user, the request including a user key;
decrypting the reconstructed secret using the user key; and
responding to the request using the reconstructed secret.

9. The method of claim 1, wherein the secret is a storage encryption key.

10. The method of claim 1, wherein the group authority is a certificate authority.

11. A system, comprising:
a memory; and
a central processing unit (CPU) coupled to the memory, the CPU configured to execute instructions to:
determine that a key unit storing a secret has failed, the key unit included in a group;
identify, responsive to the determining, a replacement key unit;
transmit, responsive to the identifying, a signal to the group, the signal indicating that the replacement key unit is to reconstruct the secret;
receive fingerprints of encrypted key slices from the replacement key unit;
validate the received fingerprints, the validating including comparing the received fingerprints to stored fingerprints stored in a fingerprint storage;
responsive to the validation, transmit stored group authority keys to the replacement key unit, wherein the stored group authority keys decrypt the encrypted key slices and reconstruct the secret;
generate new group authority keys; and

transmit the new group authority keys to the replacement key unit, wherein the new group authority keys are used to encrypt new key slices generated from slicing the reconstructed secret, and wherein a different new group authority key is used to encrypt each new key slice.

12. The system of claim 11, wherein the CPU is further configured to:
add the replacement key unit to the group; and
validate an identity of the replacement key unit.

13. The system of claim 12, wherein the CPU is further configured to:

receive new fingerprints from the replacement key unit; and
store the new fingerprints in a fingerprint store.

14. The system of claim 11, wherein the system is a certificate authority.

15. The system of claim 11, wherein the secret is a storage encryption key.

16. A computer program product, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a computer to cause the computer to:
obtain, at a first key unit, a first secret;
receive , at the first key unit, group authority keys from a group authority;
generate, by the first key unit and based on the received group authority keys, a plurality of encrypted slices of the first secret, wherein each of the plurality of encrypted slices are encrypted with a different group authority key from the received group authority keys;
transmit, by the first key unit, the plurality of encrypted slices to a plurality of other key units, the plurality of other key units comprising a second key unit, wherein each of the other key units stores an encrypted slice from the plurality of encrypted slices;
receive, at the first key unit, a first encrypted slice from the second key unit, wherein the first encrypted slice corresponds to a second secret, and wherein the first encrypted slice is encrypted with a first group authority key;
transmit the first encrypted slice to a replacement key unit, wherein the first encrypted slice is used to reconstruct the second secret; and
receive, at the first key unit, a replacement encrypted slice from the replacement key unit, wherein the replacement encrypted slice is encrypted with a new group authority key, and wherein the replacement encrypted slice corresponds to a reconstructed second secret.

17. The computer program product of claim 16, wherein the instructions further cause the computer to:

generate one or more fingerprints based on the plurality of encrypted slices, wherein the one or more fingerprints protect access to the one or more group authority keys; and

transmit the one or more fingerprints to the group authority.

18. The computer program product of claim 16, wherein the generating the plurality of encrypted slices includes:

slicing the secret into a plurality of slices; and

encrypting, using the group authority keys, the plurality of slices.

19. The computer program product of claim 16,

wherein the instructions further cause the computer to generate, based on the encrypted slices and an error correcting code, a second plurality of slices; and

transmit the second plurality of slices to a plurality of key units.

20. The computer program product of claim 16, wherein the instructions further cause the computer to:

receive , at the first key unit , a second encrypted slice from a third key unit;

store the first encrypted slice and the second encrypted slice; and

receive a request from the group authority to transmit the first encrypted slice to the replacement key unit.

21. The computer program product of claim 16, wherein the instructions further cause the computer to:

replace the first encrypted slice with the replacement encrypted slice.

22. The computer program product of claim 21, wherein the instructions further cause the computer to:

receive one or more new group authority keys from the group authority;

generate, based on the one or more group authority keys, one or more new encrypted slices of the secret; and

transmit at least one of the one or more new encrypted slices to the replacement key unit.

23. The system of claim 13, wherein storing the new fingerprints in the fingerprint store comprises overwriting the stored fingerprints with the new fingerprints.

24. The computer program product of claim 16, wherein none of the plurality of encrypted slices are stored by the first key unit.