CLAIMS

1. A computer-implemented method for creating a master seed using location data, the computer-implemented method comprising:

creating a signing request message using a location-based hardware security module (HSM) located at a location;

transmitting the signing request message to a location authority with coordinates of the location attached;

receiving a response from the location authority authorizing the signing request message based on the coordinates and providing a signature; and

creating the master seed based on the signature, and further comprising:

receiving a recovery mnemonic sentence to regenerate the master seed;

creating signing request messages using the location-based HSM at the location;

transmitting the signing request messages to the location authority with the coordinates of the location attached;

receiving a second response from the location authority authorizing the signing request messages and providing a second signature;

verifying a checksum derived from the mnemonic sentence with a second checksum derived from the second signature; and

creating the master seed based on the mnemonic sentence and the second signature and the verification of the checksum.

2. The computer-implemented method of claim 1, wherein creating the signing request message comprises:

acquiring location data of the location-based HSM;

determining the location data is located at a predetermined location, wherein the predetermined location is an undisclosed location known only by an operator of the location-based HSM;

extracting longitudinal and latitudinal values from the location data;

generating a random number using a random number generator; and

creating the signing request message using the random number and attaching the longitudinal and latitudinal values.

3. The computer-implemented method of claim 2, wherein the random number generator generates the random number using a current time of the location-based HSM.

4. any of the The computer-implemented method of any of the preceding claims, wherein the signing request messages include location data around the location.

5. The computer-implemented method of any preceding claim, wherein the location is within an authorization zone of the location authority.

6. The computer-implemented method of any of claims 1 to 4, wherein the location authority is physically located at a geographically assured location.

7. A computer program product for creating a master seed using location data, the computer program product comprising:

a computer readable storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method according to any of claims 1 to 6.

8. A computer program stored on a computer readable medium and loadable into the internal memory of a digital computer, comprising software code portions, when said program is run on a computer, for performing the method of any of claims 1 to 6.

9. A location-based hardware security module (HSM) for generating a master seed using location data, the location-based HSM comprising:

a pseudo-random number generator (PRNG) configured to generate a random number;

a global positioning system (GPS) module configured to determine a location of the location-based HSM;

an encryption module configured to generate a signing request message, wherein the signing request message includes the random number and the location;

a communication device configured to transmit the signing request message to a location authority for authorization, the communication device further configured to receive a signature from the location authority upon authorization of the signing request message; and

wherein the encryption module is further configured to generate the master seed based on the signature;

and by the HSM further operable for:

receiving a recovery mnemonic sentence to regenerate the master seed;

creating signing request messages using the location-based HSM at the location;

transmitting the signing request messages to the location authority with the coordinates of the location attached;

receiving a second response from the location authority authorizing the signing request messages and providing a second signature;

verifying a checksum derived from the mnemonic sentence with a second checksum derived from the second signature; and

creating the master seed based on the mnemonic sentence and the second signature and the verification of the checksum.

10. The location-based HSM of claim 9, wherein the PRNG generates the random number using a current time as entropy.

11. The location-based HSM of claim 9, wherein the location is a longitudinal and latitudinal coordinate of the location-based HSM that is within an authorization zone of the location authority.

12. The location-based HSM of claim 9, wherein the encryption module is further configured to recreate the master seed based on a mnemonic sentence.

13. The location-based HSM of claim 9, wherein the communication device is further configured to transmit the signing request message to multiple location authorities in order to receive the signature.

14. The location-based HSM of claim 9, wherein the location authority is a facility located at a fixed location.