Claims

Claim 1. A method for signing a request data using a Group-shared Private Key (GPK), comprising:

S201 transmitting, by an initiating Key Shard Holder (KSH), a signing request and a request data, to a Communication Coordination Application (CCA); wherein the signing request comprises a first hash of the request data and a GPK shard of the initiating KSH;

S202 creating, by the CCA, a signing session to invite the plurality of KSHs to join the signing session as participating KSHs; wherein the CCA is operable to transmit the request data to the plurality of KSHs for the plurality of KSHs to decide whether to become the participating KSHs;

S203 transmitting, by each of the participating KSHs, an approval message to the CCA, wherein the approval message comprises a second hash of the request data and a GPK shard of the each of the participating KSHs;

S204 forwarding, by the CCA, the signing request and a plurality of the approval messages to a Trusted Execution Environment (TEE), wherein the TEE comprises a TEE program;

S205 authenticating, by the TEE program, the request data based on the first hash of the request data and a plurality of the second hashes of the request data;

S206 regenerating, by the TEE program, the GPK based on the GPK shards from the signing request and the plurality of the approval messages;

S207 signing, by the TEE program, the request data with the GPK to obtain a signed request data; and

S208 transmitting, from the TEE, the signed request data to the CCA.

Claim 2. The method according to Claim 1, wherein the TEE is arranged to be data communication with a Key Management Service (KMS).

Claim 3. The method according to Claim 2, wherein, the signing request is operable

(i) to be encrypted by a KMS public key in S201, and
(ii) to be decrypted by a KMS private key in S205.

Claim 4. The method according to Claim 2, wherein, the approval message is operable

(i) to be encrypted by a Key Management Service (KMS) public key in S203, and
(ii) to be decrypted by a KMS private key in S205.

Claim 5. The method according to Claim 1, wherein the request data comprises digital asset transaction data or an operation command.

Claim 6. The method according to Claim 1, wherein the TEE is secured with hardware-based memory encryption.

Claim 7. The method according to Claim 1, wherein, the CCA is operable to initiate the step of S204 if total number of the GPK shards received by the CCA is sufficient for regenerating the GPK.

Claim 8. The method according to Claim 1, wherein, the KSH is operable to transmit a rejection message to the CCA if the KSH decides not to approval the request data.

Claim 9. The method according to Claim 1, wherein the GPK shard is assembled from a second number of Secondary GPK Shards (SGS); wherein SGS is obtained from further slicing of the GPK shard, and the second number is:

(i) larger than or equal to two; and
(ii) smaller than or equal to total number of SGS generated.