

## CLAIMS

1. A method for providing a digital signature, the method comprising the steps of:

- 5       – providing a private signature key being distributed among two or more nodes of a cold wallet, each node of the cold wallet thereby being in the possession of one or more shares of the private signature key, and none of the nodes of the cold wallet being in the possession of all shares of the private signature key,
- 10       – each node of the cold wallet generating a pre-signature, based on its share(s) of the private signature key, and transmitting the pre-signature to one of two or more pre-signature nodes, in such a manner that each pre-signature node receives a pre-signature from only one of the nodes of the cold wallet,
- 15       – a signing application requesting a signature and transmitting a message to be signed to each of the pre-signature nodes,
- in response to receiving the request for a signature and the message to be signed, each pre-signature node generating a partial signature, based on its pre-signature and on the message to be signed,
- each pre-signature node transmitting its partial signature to the signing application, and
- the signing application computing a digital signature from the partial signatures.

20   2. A method according to claim 1, further comprising the step of each of the pre-signature nodes deleting the pre-signature after the step of generating a partial signature and before the step of transmitting the partial signature.

3. A method according to claim 1 or 2, wherein the step of each node of the cold wallet transmitting the pre-signature to one of the pre-signature nodes is performed using a one-way communication channel.

25   4. A method according to any of the preceding claims, wherein the step of providing a private signature key is performed by the nodes of the cold wallet generating the private signature key by means of a multi-party computation protocol.

5. A method according to any of the preceding claims, wherein each node of the cold wallet generates the pre-signature as part of a batch comprising two or more pre-signatures.
6. A method according to any of the preceding claims, wherein at least the steps of providing a private signature key, generating pre-signatures and transmitting the pre-signatures to the pre-signature nodes are performed as pre-processing steps prior to the step of the signing application requesting a signature.
7. A method according to any of claims 1-5, wherein the step of each node of the cold wallet generating a pre-signature, based on its share(s) of the private signature key, and transmitting the pre-signature to one of two or more pre-signature nodes is initiated by the pre-signature nodes in response to receipt of a request for a signature from the signing application.
8. A method according to any of the preceding claims, wherein the step of each pre-signature node generating a partial signature is performed without internal communication among the pre-signature nodes.
9. A method according to any of the preceding claims, further comprising the step of authorizing the request for a signature from the signing application.
10. A method according to any of the preceding claims, wherein the nodes of the cold wallet fulfil a threshold condition,  $t$ , and the pre-signature nodes fulfil a threshold condition,  $t'$ , where  $t' \geq t$ .
11. A method according to any of the preceding claims, further comprising the steps of:
- at least some of the nodes of the cold wallet generating one or more additional pre-signature shares, encrypting the additional pre-signature share(s), and transmitting the encrypted additional pre-signature share(s) to one or more of the pre-signature nodes along with the pre-signatures, and
  - each pre-signature node which has received an encrypted additional pre-signature share transmitting the encrypted additional pre-signature share to the signing application along with the partial signature,

wherein the step of the signing application computing a digital signature comprises the steps of:

- the signing application decrypting the received encrypted additional pre-signature share(s),
- the signing application generating an additional pre-signature, based on the decrypted additional pre-signature share(s), and generating an additional partial signature based on the additional pre-signature and on the message to be signed, and
- the signing application computing the digital signature from the partial signatures received from the pre-signature nodes and the generated additional partial signature.

12. A method according to claim 11, wherein the step of generating one or more additional pre-signature shares is performed by each of the nodes of the cold wallet generating an additional pre-signature share and encrypting the additional pre-signature share.

13. A method according to claim 11, wherein the step of generating one or more additional pre-signature shares is performed by at least two of the nodes of the cold wallet applying a multi-party computation protocol.

14. A method according to any of claims 11-13, wherein the additional pre-signature shares are encrypted and decrypted by means of symmetric encryption keys shared between the respective nodes of the cold wallet and the signing application.

15. A system for providing a digital signature, the system comprising:

- a cold wallet comprising two or more nodes having a private signature key distributed among the nodes, each node of the cold wallet thereby being in the possession of one or more shares of the private signature key, and none of the nodes of the cold wallet being in the possession of all shares of the private signature key, the nodes of the cold wallet being configured to generate a pre-signature, based on its share(s) of the private signature key, and to transmit the pre-signature to a pre-signature node,
- a pre-signature wallet comprising two or more pre-signature nodes, the pre-signature nodes being configured to receive pre-signatures from the nodes of the cold wallet in such a manner that each pre-signature node receives a pre-signature from only one of the nodes of the cold wallet, to generate a partial signature, based on its pre-signature and a message to be signed, and to transmit its partial signature to a signing application, and

- a signing application configured to transmit a request for a signature and a message to be signed to the pre-signature nodes, to receive partial signatures from the pre-signature nodes, and to compute a digital signature from the partial signatures.

16. A system according to claim 15, wherein data transmission to the cold wallet is  
5 prevented.