

Claims:

1. Set (s) of two or more dongles (a,b,c) for providing a digital signature (S_i),

wherein each dongle (a,b,c) holds a secret key (K_i),

wherein each dongle (a,b,c) is configured to receive a message (M), to compute (28,36) a digital signature (S_i) of the received message (M) using the secret key (K_i), and to transmit the computed digital signature (S_i),

characterised in that at least one of the dongles (a) is configured to, before computing (28) the digital signature (S_a), verify (26) the presence of at least one other dongle (b,c) belonging to the set (s), and to compute (28) the digital signature (S_a) only within a limited timeframe from a successful verification of the presence of one or more other dongles (b,c).

2. Set (s) according to claim 1, wherein the at least one of the dongles (a) is configured to verify the presence of at least one other dongle (b,c) belonging to the set (s) by requiring a zero-knowledge proof.

3. Set (s) according to one of the preceding claims, characterised in that the at least one of the dongles (a) stores a lower limit of the number of other dongles (b,c), the presence of which must be proven, before computing (28) the digital signature (S_a).

4. Set (s) according to one of the preceding claims, characterised in that the at least one dongle (a) is configured to measure the time required for verifying the presence of the at least one other dongle (b,c) belonging to the set (s) and to compute (28) the digital signature (S_a) only upon successful verification of the presence of one or more other dongles (b,c) within a predefined timeframe for each of the one or more other dongles (b,c).

5. Set (s) according to one of the preceding claims, characterised in that the dongles (a,b,c) are configured to establish direct wireless connections (4,5) between each other for verification of presence, wherein the at least one dongle (a) is configured to measure the signal strength of the wireless

connection (4) to the at least one other dongle (b) belonging to the set (s) and to compute (28) the digital signature (S_a) only if the signal strength exceeds a predefined minimum signal strength and/or a distance measure derived from the signal strength is below a predefined maximum distance for each of the one or more other dongles (b).

6. Set (s) according to one of the preceding claims, characterised in that at least one of the dongles (c) is configured to verify the presence of a mobile terminal (T_c) before confirming its own presence to any other dongle (a,b).

7. Set (s) according to claim 6, characterised in that the mobile terminal (T_c) is configured to confirm its presence only within a limited timeframe after authentication of a user of the mobile terminal (T_c), preferably a biometric authentication.

8. Method for providing a digital signature (S_i) with a dongle (a) belonging to a set (s) according to one of claims 1 to 7, wherein the dongle (a) holds a secret key (K_a), the method comprising the following steps:

- receiving a message (M) to be signed;
- verifying (26) the presence of at least one other dongle (b,c) belonging to the set (s);
- if the verification is successful, computing (28) within a limited timeframe from the successful verification a digital signature (S_a) of the message (M) using the secret key (K_a); and
- transmitting the computed digital signature (S_a).

9. Method according to claim 8, wherein the step of verifying (26) the presence of at least one other dongle (b,c) belonging to the set (s) is characterised by requiring a zero-knowledge proof, including:

- sending a request for providing the zero-knowledge proof to the at least one other dongle (b,c),
 - receiving a zero-knowledge proof from the at least one other dongle (b,c), and
 - verifying (26) the received zero-knowledge proof,
- wherein the presence of the at least one other dongle (b,c) is verified if the verification of the received zero-knowledge proof is successful.

10. Method according to one of claims 8 or 9, characterised by: during verifying (26) the presence of at least one other dongle (b,c) belonging to the set (s), measuring the time required for verifying (26) the presence, and, before computing (28) a signature (S_a) of the received message (M), requiring that the time required is within a predefined timeframe for each of the one or more other dongles (b,c).

11. Method according to one of claims 8 to 10, characterised by: measuring the signal strength of a wireless connection (4,5) to the at least one other dongle (b,c) belonging to the set (s), and, before computing (28) a signature (S_a) of the received message (M), requiring that the measured signal strength exceeds a predefined minimum signal strength and/or a distance measure derived from the measured signal strength is below a predefined maximum distance for each of the one or more other dongles (b,c).

12. Method according to one of claims 8 to 11, characterised by: before computing a signature of the received message or providing a zero-knowledge proof, verifying (56) the presence of a mobile terminal (T_c) connected to the dongle (c).

13. The method according to claim 12, characterised by: verifying (56) the presence of the mobile terminal (T_c) comprises authenticating a user of the mobile terminal (T_c), preferably using at least partially biometric credentials.