37216.HEY.P110SG.PC
SG 11202302236Q

Claims

1. An authenticating and reporting system (10) for authenticating a user at and reporting about use of a charging device (40) comprising:
   - at least one database unit comprising:
     - at least one cryptography module (22) configured to sign and encrypt authentication elements (28) and to decrypt charging report elements (48), and
     - at least one transmitting and receiving module (26) configured to transmit encrypted authentication elements (28) and to receive encrypted charging report elements (48);
   - at least one charging device (40) comprising:
     - at least one wireless communication module (44),
     - at least one encrypting and decrypting unit (46),
     - at least one storage module (42), and
     - at least one control module,

     wherein the at least one charging device (40) is configured to decrypt the authentication elements (28), control a charging procedure of a connected chargeable device, provide encrypted charging report elements (48), and store a timestamp parameter of a transmitted encrypted charging report element (48) or a group of transmitted encrypted charging report elements (48); and
   - at least one mobile device (30) configured to transfer the authentication elements (28) from the database unit (20) to the charging device (40) and the charging report elements (48) from the charging device (40) to the database unit (20),

   wherein the database unit (20) is configured such that, once a first authentication element has been provided to a user, a second or further authentication element is provided only in exchange for a charging report element or a bundle of charging report elements relating to the preceding authentication element or elements,
   wherein the authentication elements (28) are single-use tokens, each usable for one charging procedure,
   wherein the single-use authentication elements (28) each contain configuration data of an assigned charging device (40), and wherein the configuration data comprises values that must be set by the charging device (40) in relation to the connected chargeable device of the user before starting the charging procedure,
   wherein the at least one mobile device (30) synchronizes with the database unit (20) at regular intervals whenever mobile network coverage is available, so that the next valid

authentication element is transferred to the at least one mobile device (30) whenever possible, in order to ensure that the user possesses the single-use authentication element (28) for the designated charging device (40) even if no mobile connection is available at the location of the charging device (40).

2. The authenticating and reporting system (10) according to claim 1, wherein one authentication element (28) comprises

- a charging device identification parameter (52),
- a user identification parameter (52),
- a sequence parameter (56), and
- a confirmation timestamp of a charging report element (58).

3. The authenticating and reporting system (10) according to one of the preceding claims, wherein the charging device (40) is pre-paired to the database unit (20).

4. The authenticating and reporting system (10) according to one of the preceding claims, wherein the cryptography module (22) of the database unit (20) and the encrypting and decrypting unit (46) use public key cryptography.

5. The authenticating and reporting system (10) according to one of the preceding claims, wherein the mobile device (30) comprises an application (32) configured to interoperate with the database unit (20) and the charging device (40).

6. The authenticating and reporting system (10) according to claim 5, wherein the application (32) is further configured to start and stop the charging procedure, monitor the charging procedure and display the charging report element (48).

7. The authenticating and reporting system (10) according to claim 6, wherein the mobile device (30) and/or the application (32) are untrusted.

8. Use of an authenticating and reporting system (10) according to one of claims 1 to 7.