Patent Claims

1. A method for operating a system (1) for controlling access to an access-restricted area (8) in a building or a compound, wherein the system (1) comprises a transmitter and receiver unit (14) for the radio communication with mobile electronic devices (6) carried along by users (2), a storage unit (26, 28), a processing unit (20) and a code processing unit (16, 22), and wherein the method comprises the steps of:

receiving a first identifier (Ki) of a first mobile electronic device (6) of a first user (2) by means of the transmitter and receiver unit (14) when the first mobile electronic device (6) is located in a public area (10), from which the first user (2) can request access to the access-restricted area (8);

storing the received first identifier (Ki) in the storage unit (26, 28), wherein a first dataset (DSi) is created for the first identifier (Ki) and assigned to the first user (2) present in the public area (10), wherein a plurality of datasets can be stored in the storage unit (26, 28), and wherein each dataset is assigned to a user (2) present in the public area (10);

storing a first password (Ci) in the first dataset (DSi) such that the first password (Ci) is assigned to the first identifier (Ki);

determining if the first identifier (Ki) is assigned to a user profile in a database (34) by means of the processor unit (20) in order to authenticate the first user (2) as having access authorization in the event of such an assignment;

acquiring a password (Cd) presented by the first user (2) by means of the code processing unit (16, 22) when the first user (2) requests access to the access-restricted area (8); and

determining if the acquired password (Cd) matches the first password (Ci) stored in the first dataset (DSi) of the storage unit (26, 28) by means of the processor unit (20), wherein the first user (2) is recognized as an access-requesting user (2) in the event of a match.

2. The method according to claim 1, furthermore comprising the step of generating a result signal, which initiates a building action if the acquired password (Cd) matches the first password (Ci).

3. The method according to claim 2, furthermore comprising the step of reading the user profile of the first user (2), which is stored in the database (34), in order to determine a user-specific building action.

4. The method according to claim 3, wherein the user-specific building action comprises unlocking a building door, to which the first user (2) has access authorization, or registering a destination call to a destination floor defined for the first user (2) or a combination of unlocking a building door and registering a destination call.

5. The method according to one of claims 2-4, furthermore comprising the step of generating a control signal as a function of the result signal in order to release a barrier (18, 36) such that the user (2) can enter the access-restricted area (8).

6. The method according to one of the preceding claims, wherein the code processing unit (16, 22) comprises an optical reader for acquiring the acquired password (Cd) from a screen of the mobile electronic device (6), on which the acquired password (Cd) is displayed in machine-readable form.

7. The method according to claim 6, wherein the displayed password is a numeric code, an alphanumeric code, a barcode, a QR code or a color code.

8. The method according to one of claims 1-5, wherein the code processing unit (16, 22) is designed for acquiring the acquired password (Cd) from the first mobile electronic device (6), on which the acquired password (Cd) is displayed or stored.

9. The method according to one of the preceding claims, wherein the radio link between the transmitter and receiver unit (14) and a mobile electronic device (6) of a user (2) is realized in accordance with a Bluetooth standard or a WLAN/WiFi standard, and wherein the transmitter and receiver unit (14) receives the first identifier (Ki) via the radio link when the mobile electronic device (6) is located in the radio range of the transmitter and receiver unit (14).

10. The method according to one of the preceding claims, wherein the first identifier (Ki) is generated by application-specific software, which is active on the mobile device (6), and wherein the first identifier (Ki) is time-invariant.

11. The method according to one of claims 1-10, wherein the first identifier (Ki) comprises a device identification number or a telephone number assigned to a mobile device (6).

12. The method according to one of the preceding claims, wherein the first identifier (Ki) and the first password (Ci) are received by the transmitter and receiver unit (14) when the first mobile

electronic device (6) is located in the public area (10) and transmits the first identifier (Ki) and the first password (Ci).

13. The method according to one of the preceding claims, wherein a dataset (DSi) is stored in the storage unit (26, 28) for each mobile electronic device (6) of a user (2), which transmits the first identifier (Ki) and the first password (Ci), when a plurality of mobile electronic devices (6) are located in the public area (10).

14. A system (1) for controlling access to an access-restricted area (8) in a building or a compound, wherein the system (1) comprises:

a transmitter and receiver unit (14) for the radio communication with a first mobile electronic device (6) carried along by a first user (2), wherein said transmitter and receiver unit is designed for receiving a first identifier (Ki) of the first mobile electronic device (6) when the first mobile electronic device (6) is located in a public area (10), from which the first user (2) can request access to the access-restricted area (8);

a storage unit (26, 28) that is designed for creating a first dataset (DSi), which is assigned to the first user (2) present in the public area (10), for the first identifier (Ki) and for storing a first password (Ci) in the first dataset (DSi) such that the first password (Ci) is assigned to the first identifier (Ki), wherein a plurality of datasets can be stored in the storage unit (26, 28);

a code processing unit (16, 22) that is designed for acquiring a password (Cd) presented by the first user (2) when the first user (2) requests access to the access-restricted area (8); and

a processor unit (20) that is designed for

- determining if the first identifier (Ki) is assigned to a user profile in a database (34),
- authenticating the first user (2) as having access authorization if the first identifier (Ki) is assigned to a user profile in the database (34), and
- determining if the acquired password (Cd) matches with the first password (Ci) stored in the first dataset (DSi) of the storage unit (26, 28), wherein the first user (2) is recognized as an access-requesting user (2) in the event of a match.

15. The system (1) according to claim 14, wherein the processor unit (20) is furthermore designed for generating a result signal, which initiates a building action in the event of a match.