

CLAIMS

1. An authentication method comprising a verification process and an authentication process, wherein the verification process and the authentication process are conducted on at least two distinct systems, wherein at least parts of the verification process are conducted on at least one verification device and at least parts of the authentication process are conducted on at least one authentication device, wherein the verification process comprises:

- capturing first biometric data of a person;
- extracting second biometric data from a biometric identification document;
- comparing the first biometric data with corresponding second biometric data from the biometric identification document to obtain a similarity value comparable with a first similarity threshold;
- in response to the similarity value of the first biometric data compared with the corresponding second biometric data exceeding the first similarity threshold:
 - verifying the person's identity;
 - gathering additional data;
 - certifying the first biometric data and the additional data;
 - storing the certified first biometric data and the certified additional data;

wherein the authentication process comprises:

- capturing live biometric data of the person;
- receiving the certified first biometric data of the person;
- comparing the live biometric data with the certified first biometric data; and
- in response to a similarity value of the live biometric data and compared with the certified first biometric data exceeding a second similarity threshold,
- authenticating the person; and

wherein the at least one verification device comprises a self-service terminal, and wherein the verification process, conducted on the self-service terminal, further comprises:

- obtaining an identification number, wherein the identification number is a unique identification number extracted from the biometric identification document;
- in response to the similarity value of the first biometric data compared with the corresponding second biometric data exceeding the first similarity threshold:
 - generating a key using the additional data;

- encrypting the certified first biometric data and the certified additional data with the key generated from the additional data; and
- storing the encrypted certified first biometric data and the encrypted certified additional data with the identification number in a central database; and

wherein, in the authentication process, receiving the certified first biometric data of the person comprises:

- capturing an image of an authentication biometric identification document of the person;
- extracting authentication additional data from the authentication biometric identification document;
- extracting an authentication identification number from the authentication biometric identification document;
- generating a key using the authentication additional data;
- requesting the stored encrypted certified first biometric data from the central database using the authentication identification number; and
- decrypting the encrypted certified first biometric data with the key generated from the authentication additional data.

~~2. The authentication method of claim 1, wherein the verification process further comprises, in response to the similarity value of the first biometric data compared with the second biometric data exceeding the first similarity threshold:~~

- ~~- verifying the person's identity;~~
- ~~- gathering additional data;~~
- ~~- certifying the first biometric data and the additional data; and~~
- ~~- storing the certified first biometric data and the certified additional data.~~

~~3.2.~~ The authentication method of claim ~~21~~, wherein the at least one ~~of the~~ verification devices ~~is~~comprises a mobile device of the person, and wherein, in the verification process, storing the certified first biometric data and the certified additional data comprises storing the certified first biometric data and the certified additional data on the mobile device of the person, and wherein, in the authentication process, receiving the certified first biometric data of the person comprises transferring the certified first biometric data from the mobile device of the person to the authentication device.

4. ~~The authentication method of claim 2 or 3, wherein at least one of the verification devices is a self-service terminal, and wherein the verification process, conducted on the self-service terminal, further comprises:~~

- ~~— obtaining an identification number, wherein the identification number is a unique identification number extracted from the biometric identification document;~~
- ~~— in response to the similarity value of the first biometric data and the corresponding second biometric data from the biometric identification document exceeding the first similarity threshold:~~
 - ~~— generating a key using the additional data;~~
 - ~~— encrypting the certified first biometric data and the certified additional data with the key generated from the additional data; and~~
 - ~~— storing the encrypted certified enrollment biometric and the encrypted certified additional data with the identification number in a central database; and~~

~~wherein, in the authentication process, receiving the first biometric data of the person comprises:~~

- ~~— capturing an image of an authentication biometric identification document of the person;~~
- ~~— extracting authentication additional data from the authentication biometric identification document;~~
- ~~— extracting an authentication identification number from the biometric document;~~
- ~~— generating a key using the authentication additional data;~~
- ~~— requesting the stored encrypted certified first biometric data from the central database using the authentication identification number; and~~
- ~~— decrypting the encrypted certified first biometric data with the key generated from the authentication additional data.~~

5.3. The authentication method of any one of claims 2 to 41, wherein the at least one of the verification devices comprises a mobile device of the person, and wherein, in the verification process conducted on the mobile device, storing the certified first biometric data and the certified additional data comprises storing the certified first biometric data

~~and the certified additional data are stored~~ on the mobile device of the person, and wherein the verification process, conducted on the mobile device, in response to the person announcing their need to being authenticated in the near future, further comprises:

- obtaining an identification number; and
- storing the certified first biometric data and the certified additional data with the identification number in ~~a~~ the central database.

6.4. The authentication method of any one of claims ~~21~~ to ~~53~~, wherein the at least one verification device comprises a private device of the person, wherein the verification process, conducted on the private device, further comprises:

- extracting data specific to the ~~private verification~~ device from the ~~private verification~~ device;
- generating a key using the data extracted from the ~~private verification~~ device;
- encrypting the certified first biometric data and certified additional data with the key generated from the extracted data; and
- storing the encrypted certified first biometric data and the encrypted certified additional data in ~~a~~ the central database;
- in response to the person announcing their need to being authenticated in the near future, requesting consent to use the stored data comprising the encrypted certified first biometric data and the encrypted certified additional data; and
- in response to the consent of the person to use the stored data being noted, decrypting the encrypted certified first biometric data and the encrypted certified additional data with the key generated from the extracted data ~~extracted from the verification device~~.

7.5. The authentication method of claim ~~53~~ or ~~64~~, wherein the authentication process further comprises:

- making a plurality of certified first biometric data items of people to authenticate available from ~~a~~ the central database to an authentication device; and

wherein receiving the certified first biometric data of the person comprises comparing the plurality of certified first biometric data items with the captured live biometric data of the person and selecting, in response to one of the plurality of certified first biometric data

being similar to the live biometric data, the similar certified first biometric data as certified first biometric data of the person.

8.6. The authentication method of any one of claims 4~~1~~ to 7~~5~~, wherein the central database is secured by a hardware security module and/or the data stored in the central database is encrypted.

9.7. The authentication method of any one of claims 1 to 8~~6~~, wherein the first biometric data, the second biometric data from the biometric identification document and the live biometric data comprise biometric facial images, iris scans, fingerprint images, or a combination thereof.

10.8. The authentication method of any one of claims 2~~1~~ to 9~~7~~, wherein the additional data comprises data extracted from the biometric identification document, manually entered data, data retrieved from a third party, or a combination thereof.

11.9. The authentication method of any one of claims 1 to 10~~8~~, wherein the first biometric data, the second biometric data from the biometric identification document and the live biometric data comprise vectorized representations of biometric facial images, iris scans, fingerprint images, or a combination thereof, and wherein the algorithm used for vectorizing the data is predefined by an operator of the authentication device.

12.10. The authentication method of any one of claims 1 to 11~~9~~, wherein capturing the first biometric data and/or capturing the live biometric data comprise taking a photo of at least a part of the person and/or wherein extracting the second biometric data from the biometric identification document comprises capturing the image of ~~a~~the biometric identification document, which comprises taking a photo of the biometric identification document, scanning the biometric identification document or visually inspecting the biometric identification document.

13.11. The authentication method of any one of claims 1 to 12~~10~~, wherein, when a requirement of authentication ends, any received data is deleted.

14.12. The authentication method of any one of claims 1 to 13~~11~~, wherein authenticating the person comprises at least one of granting access to an area, transferring the certified

additional data to the authentication device, decrypting the encrypted certified additional data, or a combination thereof.

~~15~~13. The authentication method of any one of claims 1 to ~~14~~12, wherein the verification process further comprises generating a user account associated with a unique user ID for the person, wherein the user account is secured by a user name and a PIN.

~~16~~14. An automatic authentication system for authenticating a person comprising:

- at least one verification device; and
- at least one authentication device;

wherein the at least one verification device is remote from the at least one authentication device; wherein the at least one verification device and the at least one authentication device are configured to communicate via a network; and wherein the at least one verification device is configured to:

- capture first biometric data of ~~at~~the person;
- extract second biometric data from ~~the~~a biometric identification document; and
- compare the first biometric data with corresponding second biometric data from the biometric identification document to obtain a similarity value comparable with a first similarity threshold;
- in response to the similarity value of the first biometric data compared with the corresponding second biometric data exceeding the first similarity threshold, the at least one verification device is further configured to:
 - verify the person's identity;
 - gather additional data;
 - certify the first biometric data and the additional data;
 - store the certified first biometric data and the certified additional data;
- and

wherein the at least one authentication device is configured to:

- capture live biometric data of the person;
- receive the certified first biometric data of the person;
- compare the live biometric data with the certified first biometric data; and

- in response to a similarity value of the live biometric data and compared with the certified first biometric data exceeding a second similarity threshold, authenticate the person; and

wherein the at least one verification device comprises a self-service terminal, and the self-service terminal is further configured to:

- obtain an identification number, wherein the identification number is a unique identification number extracted from the biometric identification document;
- in response to the similarity value of the first biometric data compared with the corresponding second biometric data exceeding the first similarity threshold:
 - generate a key using the additional data;
 - encrypt the certified first biometric data and the certified additional data with the key generated from the additional data; and
 - store the encrypted certified first biometric data and the encrypted certified additional data with the identification number in a central database; and

wherein, the at least one authentication device is configured to receive the certified first biometric data of the person by:

- capturing an image of an authentication biometric identification document of the person;
- extracting authentication additional data from the authentication biometric identification document;
- extracting an authentication identification number from the authentication biometric identification document;
- generating a key using the authentication additional data;
- requesting the stored encrypted certified first biometric data from the central database using the authentication identification number; and
- decrypting the encrypted certified first biometric data with the key generated from the authentication additional data.

15. The automatic authentication system of claim 14 further comprising a database system, wherein the database system is remote from the at least one verification device and the at least one authentication device; wherein the database system configured to communicate with the at least one verification device and the at least one authentication device via the network; and wherein the database system is configured to:

- receive data from the at least one verification device; and
- make data available to the at least one authentication device.

~~18.16.~~ The automatic authentication system of claim ~~16-14~~ or ~~17-15~~ further configured to
 5 execute the features of the method according to any one of claims 2-1 to 1513.

~~19.17.~~ A computer program comprising program code instructions for executing the features
 of the method according to any one of claims 1 to 1513.

10 18. An authentication method comprising a verification process and an authentication process,
wherein the verification process and the authentication process are conducted on at least
two distinct systems, wherein at least parts of the verification process are conducted on at
least one verification device and at least parts of the authentication process are conducted
on at least one authentication device, wherein the verification process comprises:

- capturing first biometric data of a person;
- extracting second biometric data from a biometric identification document;
- comparing the first biometric data with corresponding second biometric data
from the biometric identification document to obtain a similarity value
comparable with a first similarity threshold;
- in response to the similarity value of the first biometric data compared with the
second biometric data exceeding the first similarity threshold:
 - verifying the person's identity;
 - gathering additional data;
 - certifying the first biometric data and the additional data; and
 - storing the certified first biometric data and the certified additional data;

wherein the authentication process comprises:

- capturing live biometric data of the person;
- receiving the certified first biometric data of the person;
- comparing the live biometric data with the certified first biometric data; and
- in response to a similarity value of the live biometric data compared with the
certified first biometric data exceeding a second similarity threshold,
authenticating the person;

wherein the verification process further comprises:

- extracting data specific to the verification device from the at least one verification device;

- generating a key using the data extracted from the at least one verification device;

5 - encrypting the certified first biometric data and certified additional data with the key generated from the extracted data; and

- storing the encrypted certified first biometric data and the certified additional data in a central database;

10 - in response to the person announcing their need to being authenticated in the near future, requesting consent to use the stored data comprising the encrypted certified first biometric data and the encrypted certified additional data; and

- in response to the consent of the person to use the stored data being noted, decrypting the encrypted certified first biometric data and the encrypted certified additional data with the key generated from the extracted data.

15

19. An automatic authentication system for authenticating a person comprising:

- at least one verification device; and

- at least one authentication device;

20 wherein the at least one verification device is remote from the at least one authentication device; wherein the at least one verification device and the at least one authentication device are configured to communicate via a network; and wherein the at least one verification device is configured to:

- capture first biometric data of a person;

- extract second biometric data from the biometric identification document; and

25 - compare the first biometric data with corresponding second biometric data from the biometric identification document to obtain a similarity value comparable with a first similarity threshold; and

- in response to the similarity value of the first biometric data compared with the corresponding second biometric data exceeding the first similarity threshold, the at least one

30 verification device is further configured to:

- verify the person's identity;

- gather additional data;

- certify the first biometric data and the additional data;

- store the certified first biometric data and the certified additional data;

wherein the at least one authentication device is configured to:

- capture live biometric data of the person;
- receive the certified first biometric data of the person;
- compare the live biometric data with the certified first biometric data; and
- 5 - in response to a similarity value of the live biometric data compared with the certified first biometric data exceeding a second similarity threshold, authenticate the person; and

wherein the at least one verification device is further configured to:

- extract data specific to the verification device from the at least one verification device;
- generate a key using the data extracted from the at least one verification device;
- 10 - encrypt the certified first biometric data and certified additional data with the key generated from the extracted data; and
- store the encrypted certified first biometric data and the certified additional data in a central database;
- in response to the person announcing their need to being authenticated in the near
- 15 future, request consent to use the stored data comprising the encrypted certified first biometric data and the encrypted certified additional data; and
- in response to the consent of the person to use the stored data being noted, decrypt the encrypted certified first biometric data and the encrypted certified additional data with the key generated from the extracted data.