

CLAIMS

1. A method of preparing a secured authentication of a physical object or group of physical objects (PO(s)) by a recipient (B, B') thereof, the method comprising:
receiving or generating predicted context data (PCD) representing a predicted future location relating to a designated next recipient (B; B') of the physical object or group of physical objects (PO(s)) and a related future time of presence of the physical object or group of physical objects (PO(s)) at the predicted future location;
receiving or generating random context data (RCD) indicating a random location and a random time;
combining, according to a first predetermined combination scheme, the predicted context data (PCD) and the random context data (RCD) to thereby derive modified context data (MCD) representing a modified random location and a modified random time;
encrypting the modified context data (MCD) to obtain a secured start data package (SSDP) representing the modified context data (MCD);
storing said secured start data package (SSDP), or causing it to be stored, to a first data storage (DS1) being accessible for providing the secured data package (SSDP) for a secured authentication of a physical object or group of physical objects (PO(s));
the method further comprising one of the following processes a) to c):
 - a) detecting by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)), to obtain for each discriminating characteristic (k) respective identification data (IDD_k) representing an identity of said related physical object or group of physical objects (PO(s));applying a second predetermined cryptographic hash function (HF2) to a data set resulting from combining, according to a second predetermined combination scheme (CS2), the one or more respective identification data (IDD_k) obtained from the set of said at least one discriminating characteristic (k) and the random context data (RCD) to obtain an original hash value (Ho); detecting (210) by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)) to obtain for each discriminating characteristic (k) respective identification data (IDD_k) representing an identity of said related physical object or group of physical objects (PO(s)); or

b) applying to each of said identification data (IDD_k) a respective first predetermined cryptographic hash function ($HF_{1,k}$) to obtain a respective initial hash value (Hi_k) related to the respective discriminating characteristic (k); and
applying a second predetermined cryptographic hash function ($HF2$) to a data set
5 (H) resulting from combining, according to a second predetermined combination scheme (CS2), the one or more respective initial hash values (Hi_k) obtained from the set of said at least one discriminating characteristic and the random context data (RCD) to obtain an original hash value (Ho); or

(c) applying a second predetermined cryptographic hash function ($HF2$) to
10 the random context data (RCD) to obtain an original hash value (Ho); and
outputting initialization data (IND) representing said respective original hash value (Ho).

2. The method of claim 1, wherein storing said secured start data package (SSDP) to
15 said first data storage (DS1) involves storing the secured start data package (SSDP) to a blockchain or a blockless distributed ledger (DS1).

3. The method of claim 1, wherein:

Said at least one discriminating characteristics (k) comprises a physical unclonable
20 function, PUF (PUF_k); and
detecting said at least one discriminating characteristic (k) to obtain respective identification data (IDD_k) related thereto comprises:

applying a respective challenge of a respective predetermined challenge-
response authentication scheme to the PUF to trigger a response by the PUF ac-
25 cording to said authentication scheme in reaction to said challenge, and

detecting said respective response and generating respective identification
data (IDD_k) representing said response;

applying a respective first predetermined cryptographic hash function ($HF_{1,k}$) com-
prises applying the respective first predetermined cryptographic hash function
30 ($HF_{1,k}$) to said data representing said response to obtain a respective PUF-related initial hash value (Hi_k); and

outputting initialization data (IND) comprises outputting respective identification da-
ta (IDD_k) related to said discriminating characteristic (k), the identification data
(IDD_k) comprising a representation of said respective PUF-related initial hash val-
35 ue (Hi_k).

4. The method of claim 1, further comprising applying a time and location-invariant information (SN) identifying or being otherwise specifically related to the physical object or group of physical objects (PO(s)), respectively.
- 5 5. The method of claim 1, wherein outputting said initialization data (IND) comprises one or more of the following:
adding a marking representing said initialization data (IND) to said physical object or group of physical objects (PO(s));
store said marking representing said initialization data (IND) or causing it to be
10 stored to a third data storage (DS3) and adding to said physical object or group of physical objects (PO(s)) a representation of a pointer indicating where said initialization data (IND) can be accessed in the third data storage (DS3).
6. The method of claim 1, further comprising:
15 receiving a request for determination of another secured start data package (SSDP) relating to another predicted context data (PCD) representing another predicted future location relating to another designated next recipient (C) of the physical object or group of physical objects (PO(s)) and a related future time of presence of the physical object or group of physical objects (PO(s)) at said another
20 predicted future location.
7. The method of claim 1, further comprising:
signing said obtained original hash value (Ho) with a digital signature pertaining to a supplier (A) of said physical object or group of physical objects (PO(s)) to the respective designated next recipient (B; B'); and
25 including said digital signature in the output respective initialization data (IND) or further initialization data (IND), respectively.
8. The method of claim 1, wherein:
30 the predicted context data (PCD) represents a predicted future location of a designated next recipient (C) of the physical object or group of physical objects (PO(s)) and a related future time of presence of the physical object or group of physical objects (PO(s)) at that predicted future location.
- 35 9. The method of claim 8, further comprising:

determining new initialization data (IND) based on the same random context data (RCD) as said new secured start data package (SSDP) and storing or causing said new initialization data (IND) to be stored.

5 10. A method of authenticating a physical object or group of physical objects (PO(s)), the method comprising:

receiving and decrypting a secured start data package (SSDP) representing encrypted context data (CD) representing a location and a related time to recover said context data (CD);

10 receiving or determining current context data (CCD) representing a current location of the physical object or group of physical objects (PO(s)) and a related current time of presence of the physical object or group of physical objects (PO(s)) at that current location;

15 combining, according to a predetermined combination scheme (CS3), the current context data (CCD) with the decrypted context data (CD) to thereby determine test context data (TCD), wherein the combination scheme (CS3) defines an inverse operation to a combination operation (CS1) previously used to generate the received context data (CD);

20 accessing initialization data (IND) related to said physical object or group of physical objects (PO(s)) to recover from the initialization data (IND) an original hash value (Ho) being represented by the initialization data (IND);

the method further comprising one of the following processes a) to c):

25 a) detecting by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)) to obtain identification data (IDD_k) related to said respective discriminating characteristic (k), this identification data (IDD_k) representing a presumed identity of said related physical object or group of physical objects (PO(s)); and

30 generating a test hash value (Ht) by application of a second predetermined cryptographic hash function (HF2) to a combination (Hc), according to a further predetermined combination scheme (CS2), of the test context data (TCD) and each of said identification data (IDD_k) and a time-invariant and location-invariant information (SN) identifying or being otherwise specifically related to the said physical object or group of physical objects (PO(s)); or

35 b) detecting by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)) to obtain identification data (IDD_k) related to said respective discriminating characteristic

(k), this identification data (IDD_k) representing a presumed identity of said related physical object or group of physical objects (PO(s)), wherein the at least one discriminating characteristic (k) comprises a physical unclonable function, PUF, and wherein detecting said discriminating characteristic to obtain identification data (IDD_k) comprises:

applying a respective challenge of a respective predetermined challenge-response authentication scheme to the PUF to trigger a response according to said authentication scheme in reaction to said challenge: and

detecting a respective response by the PUF in accordance with the respective challenge-response authentication scheme in reaction to the challenge and deriving therefrom said identification data;

applying a respective first predetermined cryptographic hash function ($HF_{1,k}$) to the respective identification data (IDD_k) to obtain a respective initial hash value (Hi_k) related to said discriminating characteristic (k); and

generating a test hash value (Ht) by application of a second predetermined cryptographic hash function ($HF2$) to a combination (Hc), according to a further predetermined combination scheme ($CS2$), of the test context data (TCD) and each of said initial hash values (Hi_k), and a time-invariant and location-invariant information identifying or being otherwise specifically related to the said physical object or group of physical objects;

c) generating a test hash value (Ht) by application of a second predetermined cryptographic hash function ($HF2$) to the test context data (TCD) or to a combination (Hc), according to a further predetermined combination scheme ($CS2$), of the test context data (TCD) and a time-invariant and location-invariant information identifying or being otherwise specifically related to the said physical object or group of physical objects;

wherein for the respective one of the processes a) to c), this second predetermined cryptographic hash function ($HF2$) is equal to a corresponding cryptographic hash function previously used to determine the original hash value (Ho) represented by the initialization data (IND), and wherein said further combination scheme ($CS2$) is equal to a corresponding combination scheme previously used to determine the original hash value (Ho) represented by the initialization data (IND); and the method further comprises:

generating a first reading result ($RR1$) comprising:

- a representation of the test hash value (Ht) and a representation of the original hash value (Ho), or

- a matching output indicating whether or not, according to at least one predetermined matching criterion, the test hash value matches said original hash value and thus indicates authenticity of the physical object or group of physical objects.

5

11. The method of claim 10, wherein obtaining the identification data (IDD_k) comprises: sensor-based detecting of said at least one discriminating characteristics (k) of said physical object or group of physical objects (PO(s));
generating object data representing said at least one discriminating characteristics (k) of said physical object or group of physical objects (PO(s));
communicating said object data to a system for automatic object recognition; and receiving the digitally signed identification data from said system in response to said communicating of said object data.

10

12. The method of claim 10 further comprising a storage process comprising storing the first reading result (RR1), or causing it to be stored, into a block of a blockchain of a first set of one or more blockchains or into one or more nodes of a blockless distributed ledger of a first set of one or more blockless distributed ledgers.

15

13. The method of claim 12, wherein:
detecting of at least one discriminating characteristics of the physical object or group of physical objects (PO(s)) comprises detecting a plurality of different ones of said at least one discriminating characteristics to obtain based thereon for each of said at least one discriminating characteristics (k) respective individual set of identification data (IDD_k) representing the physical object or group of physical objects (PO(s));
generating the test hash value (H_t) is performed for each of the individual sets of identification data (IDD_k) separately such as to obtain for each of the individual sets of identification data (IDD_k) a respective individual test hash value (H_{ik});
generating the first reading result is performed for each of the individual test hash values separately to obtain for each of said at least one discriminating characteristics a respective individual first reading result; and
the storage process comprises storing each of said individual first reading results respectively causing it to be stored into a block of a respective individual dedicated blockchain in said first set of blockchains or into one or more nodes of a respective

20

25

30

35

individual dedicated blockless distributed ledger in said first set of blockless distributed ledgers.

14. The method of claim 10, further comprising determining a new secured start data package (SSDP) for a secured authentication of said physical object or group of physical objects (PO(s)) at a further recipient (C) thereof.

15. The method of claim 14 wherein determining said new secured start data package (SSDP) comprises:

issuing a request (R) for determining such new secured start data package (SSDP) for a secured authentication of said physical object or group of physical objects (PO(s)) at a further recipient (C) thereof to an authorized provider (A) of said new secured start data package (SSDP) and receiving said requested new secured start data package (SSDP) in response to the request.

16. The method of claim 10, further comprising:

receiving and storing data representing the predetermined combination scheme (CS), a time and location-invariant information (SN) identifying or being specifically related to the said physical object or group of physical objects, and metadata (MD(CS(SN))) defining a limited validity period of the combination scheme (CS); receiving a request for the combination scheme (CS) and identity information (SN) identifying or being specifically related to a physical object or group of physical objects (PO(s)) from a requesting authentication system; authenticating the requesting authentication system; and

when the requesting system is successfully authenticated as being authorized and according to previously stored metadata (MD(SN)) corresponding to the received identity information (SN), the related combination scheme (CS(SN)) to which the metadata (MD(SN)) pertains is still valid, outputting data representing that related combination scheme (CS(SN)) over a data channel (T) being secured against interception to the requesting system; or

otherwise, denying the request.

17. A non-transitory, computer-readable medium having stored thereon a computer program comprising instructions, which when executed on one or more processors carries out a method comprising:

receiving and decrypting a secured start data package (SSDP) representing encrypted context data (CD) representing a location and a related time to recover said context data (CD);

receiving or determining current context data (CCD) representing a current location of the physical object or group of physical objects (PO(s)) and a related current time of presence of the physical object or group of physical objects (PO(s)) at that current location;

combining, according to a predetermined combination scheme (CS3), the current context data (CCD) with the decrypted context data (CD) to thereby determine test context data (TCD), wherein the combination scheme (CS3) defines an inverse operation to a combination operation (CS1) previously used to generate the received context data (CD);

accessing initialization data (IND) related to said physical object or group of physical objects (PO(s)) to recover from the initialization data (IND) an original hash value (Ho) being represented by the initialization data (IND);

the method further comprising one of the following processes a) to c):

a) detecting by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)) to obtain identification data (IDD_k) related to said respective discriminating characteristic (k), this identification data (IDD_k) representing a presumed identity of said related physical object or group of physical objects (PO(s)); and

generating a test hash value (Ht) by application of a second predetermined cryptographic hash function (HF2) to a combination (Hc), according to a further predetermined combination scheme (CS2), of the test context data (TCD) and each of said identification data (IDD_k) and a time-invariant and location-invariant information (SN) identifying or being otherwise specifically related to the said physical object or group of physical objects (PO(s)); or

b) detecting by means of one or more sensors at least one discriminating characteristic (k) of said physical object or group of physical objects (PO(s)) to obtain identification data (IDD_k) related to said respective discriminating characteristic (k), this identification data (IDD_k) representing a presumed identity of said related physical object or group of physical objects (PO(s)), wherein the at least one discriminating characteristic (k) comprises a physical unclonable function, PUF, and wherein detecting said discriminating characteristic to obtain identification data (IDD_k) comprises:

applying a respective challenge of a respective predetermined challenge-response authentication scheme to the PUF to trigger a response according to said authenti-

cation scheme in reaction to said challenge;

and

detecting a respective response by the PUF in accordance with the respective challenge-response authentication scheme in reaction to the challenge and deriving therefrom said identification data;

applying a respective first predetermined cryptographic hash function ($HF_{,,k}$) to the respective identification data (IDD_k) to obtain a respective initial hash value (Hi_k) related to said discriminating characteristic (k); and

generating a test hash value (Ht) by application of a second predetermined cryptographic hash function ($HF2$) to a combination (Hc), according to a further predetermined combination scheme ($CS2$), of the test context data (TCD) and each of said initial hash values (Hi_k), and a time-invariant and location-invariant information identifying or being otherwise specifically related to the said physical object or group of physical objects;

c) generating a test hash value (Ht) by application of a second predetermined cryptographic hash function ($HF2$) to the test context data (TCD) or to a combination (Hc), according to a further predetermined combination scheme ($CS2$), of the test context data (TCD) and a time-invariant and location-invariant information identifying or being otherwise specifically related to the said physical object or group of physical objects;

wherein for the respective one of the processes a) to c), this second predetermined cryptographic hash function ($HF2$) is equal to a corresponding cryptographic hash function previously used to determine the original hash value (Ho) represented by the initialization data (IND), and wherein said further combination scheme ($CS2$) is equal to a corresponding combination scheme previously used to determine the original hash value (Ho) represented by the initialization data (IND); and

the method further comprises:

generating a first reading result ($RR1$) comprising:

a representation of the test hash value (Ht) and a representation of the original hash value (Ho), or

a matching output indicating whether or not, according to at least one predetermined matching criterion, the test hash value matches said original hash value and thus indicates authenticity of the physical object or group of physical objects.