

CLAIMS

1. A method of authenticating an object with an object authentication device, comprising:
 - sensor-based detecting of one or more discriminating characteristics of a physical object or group of physical objects;
 - generating object data representing said one or more discriminating characteristics of said physical object or group of physical objects;
 - communicating said object data to a system;
 - receiving digitally signed identification data from said system in response to said communicating of said object data;
 - reading a marking provided on or in combination with the physical object or group of physical objects, respectively, to obtain therefrom digitally signed identity information;
 - verifying the correctness of each of the digital signature of the identification data and the digital signature of the identity information;
 - comparing the received identification data with the obtained identity information to verify the authenticity of said object or group of objects based on the result of this comparison; and
 - outputting authentication information indicating whether, according to the result of this verification, said physical object or group of physical objects was determined to be authentic.
2. The method of claim 1, wherein said sensor-based detecting of one or more discriminating characteristics of the physical object or group of physical objects comprises detecting at least one discriminating characteristic that is, at least substantially, invariant under variations of the environmental conditions at which said at least one discriminating characteristic is being detected.

3. The method of claim 1, further comprising:
including the original hash value or another object-specific information contained in the identification data into the output authentication information.
4. The method of claim 3, further comprising a storing process, wherein the storing process comprises digitally signing and storing or causing another device to store said original hash value or said other object-specific information in the digitally signed form into a block of a first blockchain or a node of a first blockless distributed ledger.
5. The method of claim 4, wherein in the storage process further comprises:
reading a marking provided on or in connection with the physical object or group of objects to be authenticated
or detecting one or more selected properties of said object or group of objects to obtain supplementary information relating thereto; and
digitally signing and storing or causing another device to store said supplementary information in the digitally signed form into a block of second blockchain being separate from the first blockchain or into a node of a second blockless distributed ledger being separate from the first blockless distributed ledger.
6. The method of claim 1, further comprising one or more of the following:
performing a user authentication and allowing or denying the user to perform an object authentication with said object authentication device based on the result of the user authentication;
communicating the authentication information and/or the identification data, in whole or part, and/or further information derived therefrom, over a communication link to an opposing side;
capturing and sending security-related information over a communication link to an opposing side;

detecting a security event in information contained in a signal received from the opposing side over the communication link.

7. The method claim 1, further comprising sensor-based detecting of one or more of the following as a security event:

- an attempt or actual act of physical intrusion into the object authentication device;

- an attempt or actual act of locally or remotely accessing an internal control functionality of the object authentication device, wherein such access is not available to a user of the object authentication device in the course of its normal operation.

8. The method of claim 1, further comprising performing one or more of the following security measures in reaction to detection of a security event:

- locking the object authentication device such as to limit or prevent its further use;

- self-destroying at least one functional part of the object authentication device or destroying data stored therein in order to prevent its further use or access by a user;
- outputting an error message.

9. A computer program comprising instructions, which when executed on one or more processors of an object authentication device causes the object authentication device to perform the method according to claim 1.

10. A system for automatic object authentication, the system comprising:

- a first device configured to carry out steps comprising:

- receiving object data representing one or more discriminating characteristics of a physical object or group of physical objects;

processing the object data by means of a machine-learning-based object recognition process to obtain discriminating data representing one or more collision resistant virtual representations of the physical object or group of physical objects;

comparing at least one of the discriminating data and an original hash value derived therefrom by application of a pre-determined cryptographic hash function thereto with corresponding reference data stored in one or more data repositories with restricted access;

and if said comparison with the reference data results in a match, outputting digitally signed identification data comprising said hash value;

and a second device configured to carry out steps comprising:

sensor-based detecting of one or more discriminating characteristics of the physical object or group of physical objects;

generating object data representing said one or more discriminating characteristics of said physical object, or group of physical objects;

communicating said object data to the first device;

receiving the digitally signed identification data from said first device in response to said communicating of said object data;

reading a marking provided on or in combination with the physical object or group of physical objects, respectively, to obtain therefrom digitally signed identity information;

verifying the correctness of each of the digital signature of the identification data and the digital signature of the identity information;

comparing, the received identification data with the obtained identity information to verify the authenticity of said object or group of objects based on the result of this comparison;
and outputting authentication information indicating whether, according to the result of this verification, said physical object or group of physical objects was determined to be authentic.