

CLAIMS

1. A computer-implemented method of tokenization of a physical object, such as a product, the method comprising:

generating or receiving object identification data based on an inspection of the physical object, the object identification data comprising at least one cryptographic hash value as a collision-resistant virtual representation of the physical object;

generating a non-certified token being assigned to the physical object and representing the object identification data, wherein the non-certified token consists of a data structure defined according to a particular data format carrying further information about the non-certified token and its respective purpose which allows an interoperability between different ecosystems in which the token is used.

2. The method of claim 1, further comprising

communicating a non-certified token validation request data via a token framework to one or more certification systems, the non-certified token validation request data representing information indicating the creation of the non-certified token in relation to the object identification data and a request to have the non-certified token validated;

receiving token certification data representing a certification of the previously non-certified token by at least one of the certification systems; and storing the certification data into:

the non-certified token to convert the non-certified token into a certified token being certified by and with respect to each of the certifications represented by the token certification data, or

a different token being derived from the non-certified token and thereby certifying the different token with respect to each of the certifications represented by the token certification data; and

storing the certified token and/or metadata related to the object identification data in a protected data repository, preferably in a digital wallet.

3. The method of any one of the preceding claims, further comprising:

generating or receiving inspection certification data representing a respective certification of one or more object inspection systems used for generating the object identification data, and/or of one or more inspection participants, each inspection

participant being a device, person or institution related to one or more of the object inspection systems or their operation; and

including the inspection certification data in the non-certified token validation request data before communicating it to the at least one certification system.

4. The method of any one of the preceding claims, further comprising:
 - creating, within the token framework, a utility token based on the non-certified token, the utility token comprising data representing a resource and an action the resource is thereby requested to perform; and
 - wherein communicating the non-certified token validation request data comprises incorporating the request to have the non-certified token validated at least in part in the utility token and communicating the utility token to the certification system.
5. The method of any one of the preceding claims, further comprising:
 - communicating information request data via the token framework to one or more of the certification systems, the information request data representing an identity of a requestor and a certified request of the requestor to receive specified requested data; and
 - receiving in return the requested data via the token framework, if the request is certified by the respective certification system.
6. The method of claim 5, further comprising:
 - storing the received requested data, at least in parts, into one or more distributed ledgers.
7. The method of claim 5 or 6, further comprising:
 - identifying, by means of the token framework, one or more data sources from which the requested data may be retained and communicating the information request data selectively to these one or more data sources.
8. The method of any one of the preceding claims, further comprising:
 - receiving information request data via the token framework, the information request data representing an identity of a requestor and a certified request of the requestor to receive specified requested data; and
 - communicating in return the requested data via the token framework.

9. The method of any one of the preceding claims, wherein at least one of the object identification data, the inspection certification data, the non-certified token validation request data, the token certification data, the information request data, and the requested data is communicated, received or stored, respectively, in the form of data being embodied in a token.
10. A system for tokenization of a physical object, such as a product, the system being configured to perform the method of any one of the preceding claims.
11. A computer program for tokenization of a physical object, such as a product, the computer program comprising instructions which when executed on a processing platform of system of claim 10 cause the system to perform the method of any one of claims 1 to 9.
12. A computer-implemented method of certifying a token including object identification data, the method comprising:
 - receiving or generating and storing reference object identification data relating to a specific physical reference object and comprising at least one cryptographic hash value as a collision-resistant virtual representation of the physical reference object;
 - receiving, from a requesting system via a token framework, non-certified token validation request data representing:
 - object identification data relating to a specific physical object and comprising at least one cryptographic hash value as a collision-resistant virtual representation of the physical object, and
 - information indicating the creation of a non-certified token in relation to the object identification data and a request to have the non-certified token validated;
 - correlating the object identification data with the reference object identification data with respect to a specified matching criterion; and,
 - if according to the matching criterion the object identification data matches the reference object identification data, communicating via a token framework token certification data representing a certification of the previously non-certified token to the requesting system, wherein the non-certified token consists of a data structure defined according to a particular data format carrying further information about the

non-certified token and its respective purpose which allows an interoperability between different ecosystems in which the token is used.

13. A certification system being configured to perform the method of claim 12.
14. A computer program for certifying a token, the computer program comprising instructions which when executed on a processing platform of the certification system of claim 13 cause the certification system to perform the method of claim 12.
15. A computer-implemented method of tokenization of a process, such as an identification process for identifying a physical object, the method comprising:
 - generating or receiving process result data representing a result of an interaction of two or more identified certified physical objects in the course of a specific standardized or certified process, the certified physical objects being certified according to the method of claim 12;
 - generating a utility token being assigned to and including the process result data.
16. The method of claim ~~45~~12, wherein:
 - the utility token is initially generated as a non-certified utility token; and
 - the method further comprises:
 - communicating a non-certified utility token validation request data via a token framework to one or more certification systems, the non-certified utility token validation request data representing information indicating the creation of the non-certified utility token in relation to the process result data and a request to have the non-certified token validated;
 - receiving token certification data representing a certification of the previously non-certified utility token by at least one of the certification systems; and
 - storing the certification data into:
 - the non-certified utility token to convert the non-certified utility token into a certified utility token being certified by and with respect to each of the certifications represented by the token certification data, or
 - a different utility token being derived from the non-certified utility token and thereby certifying the different utility token with respect to each of the certifications represented by the token certification data; and

storing the certified utility token and/or metadata related to the certified process in a protected data repository, preferably in a digital wallet.

17. The method of any claim 15 or 16, further comprising:
 - generating or receiving process participant certification data representing a respective certification of one or more process participants, each process participant being a device, person or institution involved in the performance of the standardized process; and
 - including the process certification data in the non-certified utility token validation request data before communicating it to the at least one certification system.
18. The method of any one of claims 15 to 17, further comprising:
 - communicating information request data via the token framework to one or more of the certification systems, the information request data representing an identity of a requestor and a certified request of the requestor to receive specified requested data; and
 - receiving in return the requested data via the token framework, if the request is certified by the respective certification system.
19. The method of claim 18, further comprising:
 - storing the received requested data, at least in parts, into one or more distributed ledgers.
20. The method of claim 18 or 19, further comprising:
 - identifying, by means of the token framework, one or more data sources from which the requested data may be retained and communicating the information request data selectively to these one or more data sources.
21. The method of any one of claims 15 to 20, further comprising:
 - receiving information request data via the token framework, the information request data representing an identity of a requestor and a certified request of the requestor to receive specified requested data; and
 - communicating in return the requested data via the token framework.

22. The method of any one of claims 15 to 21, wherein at least one of the object identification data, the inspection certification data, the non-certified utility token validation request data, the utility token certification data, the information request data, and the requested data is communicated, received or stored, respectively, in the form of data being embodied in a token.
23. A system for tokenization of a process result, the system being configured to perform the method of any one of claims 15 to 22.
24. A computer program for tokenization of a process result, the computer program comprising instructions which when executed on a processing platform of system of claim 23 cause the system to perform the method of any one of claims 15 to 22.