

CLAIMS:

1. A system (100) for permitting a communication of at least one set of controlled credentials connected to a presenter from a server to a network endpoint, said system comprising:

at least one network endpoint;

at least one accepting appliance (109) configured to send an accepting appliance communication (104), said accepting appliance communication containing an obtained secret keycode (109a) pertaining to said presenter and a once-off shared keycode (109b), and said accepting appliance comprising an accepting appliance processor, an accepting appliance communication interface, accepting appliance memory, and at least one of an accepting appliance input console and an accepting appliance output console;

at least one presenting appliance (108) configured to send a presenting appliance communication (105), said presenting appliance communication containing an obtained presenter identifier (108a) pertaining to said presenter and a once-off shared keycode (108b), and said presenting appliance comprising a presenting appliance processor, a presenting appliance communication interface, presenting appliance memory, and at least one of a presenting appliance input console and a presenting appliance output console;

at least one server that comprises a server processor, at least one server communications interface, and server memory storing at least one entry (103) pertaining to said at least one set of connected controlled credentials, each entry being affiliated to at least one record (102), the record pertaining to any one presenter and comprising a recorded presenter identifier and a recorded secret keycode bound to the recorded presenter identifier;

wherein said at least one server is configured to:

- a) receive said accepting appliance communication (104);
- b) receive said presenting appliance communication (105);

- c) seek a match of said once-off shared keycode (109b) contained in said accepting appliance communication (104) with said once-off shared keycode (108b) contained in said presenting appliance communication (105);
- d) initiate a search for a target record by linking said obtained secret
5 keycode (109a) contained in said accepting appliance communication (104) with said obtained presenter identifier (108a) contained in said presenting appliance communication (105), both said accepting appliance communication and said presenting appliance communication containing the same once-off shared keycode (108b, 109b);
- 10 e) conduct the search for said target record that comprises a recorded secret keycode that is the same as said obtained secret keycode (109a) contained in said accepting appliance communication (104) and recorded presenter identifier that is the same as said obtained presenter identifier (108a) contained in said presenting appliance communication (105);
- 15 f) identify an entry (103) affiliated with said target record;
- g) permit the retrieval of said at least one set of connected controlled credentials pertaining to said entry (103) and permit the release of said at least one set of connected controlled credentials to said network endpoint (110), said network endpoint being a permitted recipient of a type of said at least one set of
20 connected controlled credentials.

2. The system of claim 1, wherein said at least one server comprises a controlling server (101).

- 25 3. The system of claim 2, wherein the controlling server (101) is further configured to generate said once-off shared keycode, and render it available at the accepting appliance (109).

4. The system of claim 2, wherein said accepting appliance is further configured to generate said once-off shared keycode, receive said obtained secret keycode (109a) from said presenter and transmit said accepting appliance communication to said controlling server (101).

5

5. The system of claim 3, wherein said presenting appliance is further configured to receive said once-off shared keycode from said accepting appliance (109), retrieve said obtained presenter identifier from its memory and transmit said presenting appliance communication (105) to said controlling
10 server (101).

6. The system of any one of the preceding claims, wherein said record comprising said recorded presenter identifier and said recorded secret keycode further comprises an alias associated to the presenter identifier and affiliated to
15 said entry (103) pertaining to said at least one set of connected controlled credentials.

7. The system of any one of the preceding claims, wherein said presenting appliance communication further contains an alias associated to said obtained
20 presenter identifier and affiliated to said entry (103) pertaining to said at least one set of connected controlled credentials, and wherein said search for said target record further utilizes said alias contained in said presenting appliance communication (105) to search for said target record comprising said alias in addition to comprising said obtained presenter identifier (108a) and said
25 obtained secret keycode (109a).

8. The system of any one of the preceding claims, wherein said network endpoint comprises said accepting appliance (109) and is configured as a designated recipient of one or more types of said at least one set of connected
30 controlled credentials.

9. The system of any one of claims 1 to 7, wherein said network endpoint is linked to said accepting appliance and is configured as a designated recipient of one or more types of said at least one set of connected controlled credentials.

5

10. The system of claim 2, wherein said at least one set of connected controlled credentials comprises the entry in said target record (102) on said controlling server (101).

10 11. The system of claim 1, wherein said at least one server comprises a controlling server (101) and a different server than said controlling server, wherein said at least one set of connected controlled credentials comprises an entry on the different server, wherein the entry on the different server is affiliated to said target record on said controlling server (101).

15

12. The system of any one of claims 1 to 11, wherein a validity period is assigned to said accepting appliance communication (104), and wherein step c) further comprises establishing whether said validity period has expired.

20 13. The system of any one of claims 1 to 11, wherein a validity period is assigned to said presenting appliance communication (105), and wherein step c) further comprises establishing whether said validity period has expired.

14. The system of any one of claims 1 to 11, wherein a validity period is
25 assigned to said once-off shared keycode, and wherein step c) further comprises establishing whether said validity period has expired.

15. The system of claim 14, wherein said once-off shared keycode is unique over the duration of said validity period.

16. The system of any one of claims 1 to 15, wherein said accepting appliance communication (104) further contains one or more predetermined auxiliary parameters, and said presenting appliance communication also further
5 comprises said one or more predetermined auxiliary parameters.

17. The system of claim 16, when dependent on any one of claims 2 to 5, wherein said controlling server (101) seeks to match at least one of said predetermined auxiliary parameters from said presenting appliance
10 communication (105) with said corresponding predetermined auxiliary parameter(s) from said accepting appliance communication (104) to provide further at least one of correlation and corroboration.

18. The system of any one of claims 2 to 5, wherein, if said records
15 comprise entries of at least one set of connected controlled credentials on said controlling server (101), steps f) and g) are performed at said controlling server, and communication of said at least one set of connected controlled credentials is performed from said controlling server.

20 19. The system of any one of claims 2 to 5, wherein, if said records comprise entries of at least one set of connected controlled credentials on a different server than said controlling server, steps f) and g) are performed at said different server, and communication of said at least one set of connected controlled credentials is performed using one of said controlling server and said
25 different server.

20. The system of any one of claims 2 to 5, wherein, if no match between said accepting appliance communication (104) and presenting appliance communication (105) is found at said controlling server (101), said controlling

server terminates further configured actions and records a status of the events thereat.

21. The system of any one of claims 2 to 5, wherein, if no target record is found at said controlling server (101), said controlling server terminates further configured actions and records a status of the events thereat.

22. The system of any one of claims 2 to 5, wherein said controlling server (101) is further configured to record a status of the events occurring and to relay said status to at least one of: said accepting appliance (109) and said presenting appliance (108).

23. The system of any one of claims 1 to 22, wherein each network endpoint (110) comprises a network endpoint processor, a network endpoint communication interfaces, network endpoint memory, and at least one of a network endpoint input console and a network endpoint output console.

24. The system of any one of claims 1 to 23, wherein the system is operable over a communications network (106, 107, 111).

20

25. A method to permit a communication of at least one set of controlled credentials connected to a presenter from at least one server to a network endpoint (110), said method comprising the following steps performed by at least one server:

25 (a) Receiving, from an accepting appliance (109), an accepting appliance communication (104), said communication containing an obtained secret keycode (109a) pertaining to said presenter and a once-off shared keycode (109b), and said accepting appliance comprising an accepting appliance processor, an accepting appliance communication interface, accepting appliance

memory, and at least one of an accepting appliance input console and an accepting appliance output console;

(b) Receiving, from a presenting appliance (108), a presenting appliance communication (105), said communication containing an obtained presenter identifier (108a) pertaining to said presenter and a once-off shared keycode (108b), and said presenting appliance comprising a presenting appliance processor, a presenting appliance communication interface, presenting appliance memory, and at least one of a presenting appliance input console and a presenting appliance output console;

(c) Seeking, by at least one server processor, a match of said once-off shared keycode (109b) contained in said accepting appliance communication (104) and said once-off shared keycode (108b) contained in said presenting appliance communication (105);

(d) Initiating, by at least one server processor, a search for a target record by linking said obtained secret keycode (109a) contained in said accepting appliance communication (104) and said obtained presenter identifier (108a) contained in said presenting appliance communication (105), both said accepting appliance communication and said presenting appliance communication containing the same once-off shared keycode (108b, 109b);

(e) Conducting, by at least one server processor, the search for the target record comprising a recorded secret keycode that is the same as said obtained secret keycode (109a) contained in said accepting appliance communication (104) and recorded presenter identifier that is the same as said obtained presenter identifier (108a) contained in said presenting appliance communication (105);

(f) Identifying, by at least one server processor, an entry (103) affiliated with said target record, said entry pertaining to said at least one set of connected controlled credentials; and

(g) Permitting, by at least one server processor, a retrieval of said at least one set of connected controlled credentials pertaining to said entry and permitting a release of said set of connected controlled credentials to said

network endpoint (110), said endpoint being a permitted recipient of said at least one set of connected controlled credentials.

26. The method of claim 25, wherein the target record further comprises an alias associated to said obtained presenter identifier (108a) and affiliated to said entry (103) pertaining to said at least one set of connected controlled credentials, and said presenting appliance communication (105) further contains an alias associated to said obtained presenter identifier (108a) and affiliated to said entry pertaining to said at least one set of connected controlled credentials, and wherein step (e) further comprises matching respective aliases of said record and said presenting appliance communication.

27. The method of claim 25 or 26, wherein said at least one server comprises a controlling server (101) and steps (a) to (g) are performed thereon.

15

28. The method of claim 25 or 26, wherein said at least one server comprises a controlling server (101) and a different server than said controlling server, and wherein said at least one set of connected controlled credentials comprises an entry on said different server to said controlling server (101), said entry being affiliated with said target record, and wherein the step of identifying a credential set is performed at said different server, and wherein steps (e) to (g) are performed at one of said controlling server (101) and said different server.

20

29. The method of any one of claims 25 to 28, further comprising assigning a validity period to at least one of: said accepting appliance communication (104), said presenting appliance communication (105) and said once-off shared keycode, and step (c) further comprises establishing whether said validity period has expired.

25

30. The method of claim 29, wherein said once-off shared keycode is unique over the duration of said validity period.

31. The method of any one of claims 25 to 29, wherein each of said
5 presenting appliance communication (105) and said accepting appliance communication (104) further contains one or more predetermined auxiliary parameters, and wherein step (c) further comprises seeking a match of at least one of said predetermined auxiliary parameters in said presenting appliance communication with at least one of corresponding predetermined auxiliary
10 parameters in said accepting appliance communication.

32. The method of claim 27, wherein, if said records comprise entries of at least one set of connected controlled credentials on said controlling server (101), performing the steps (f) and (g) at said controlling server, and the
15 method further comprises releasing said at least one set of connected controlled credentials from said controlling server.

33. The method of claim 25 or 26, wherein said at least one server comprises a controlling server (101), and, if said records comprise entries of at least one
20 set of connected controlled credentials on a different server to said controlling server (101), performing the steps (f) and (g) at said different server, and the method further comprises releasing said at least one set of connected controlled credentials from one of: said controlling server and said different server.

25 34. The method of claim 27 or 28, wherein, if no match between said accepting appliance communication (104) and presenting appliance communication (105) is found, terminating further configured actions and recording a status of the events at said controlling server (101).

35. The method of claims 27 or 28, wherein, if no target record is found, terminating further configured actions and recording a status of the events at said controlling server (101).
- 5 36. The method of claim 27 or 28, further comprising recording a status of the events at said controlling server (101) and relaying the status to at least one of said accepting appliance (109) and said presenting appliance (108).