

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 2505161PC00		FOR FURTHER ACTION	See Form PCT/PEA/416
International application No. PCT/EP2015/050354	International filing date (day/month/year) 09.01.2015	Priority date (day/month/year) 10.01.2014	
International Patent Classification (IPC) or national classification and IPC INV. H04L29/06			
Applicant Mainline Patents Holdings Ltd.			
1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36. 2. This REPORT consists of a total of <u>6</u> sheets, including this cover sheet. 3. This report is also accompanied by ANNEXES, comprising: a. ☒ (sent to the applicant and to the International Bureau) a total of <u>37</u> sheets, as follows: ☒ sheets of the description, claims and/or drawings which have been amended and/or sheets containing rectifications authorized by this Authority, unless those sheets were superseded or cancelled, and any accompanying letters (see Rules 46.5, 66.8, 70.16, 91.2, and Section 607 of the Administrative Instructions). ☐ sheets containing rectifications, where the decision was made by this Authority not to take them into account because they were not authorized by or notified to this Authority at the time when this Authority began to draw up this report, and any accompanying letters (Rules 66.4bis, 70.2(e), 70.16 and 91.2). ☐ superseded sheets and any accompanying letters, where this Authority either considers that the superseding sheets contain an amendment that goes beyond the disclosure in the international application as filed, or the superseding sheets were not accompanied by a letter indicating the basis for the amendments in the application as filed, as indicated in item 4 of Box No. I and the Supplemental Box (see Rule 70.16(b)). b. ☐ (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing, in the form of an Annex C/ST.25 text file, as indicated in the Supplemental Box Relating to Sequence Listing (see paragraph 3ter of Annex C of the Administrative Instructions).			
4. This report contains indications relating to the following items: ☒ Box No. I Basis of the report ☐ Box No. II Priority ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability ☐ Box No. IV Lack of unity of invention ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement ☐ Box No. VI Certain documents cited ☐ Box No. VII Certain defects in the international application ☐ Box No. VIII Certain observations on the international application			
Date of submission of the demand 10.11.2015		Date of completion of this report 24.03.2016	
Name and mailing address of the international preliminary examining authority:  European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016		Authorized officer Ruiz Sanchez, J Telephone No. +31 70 340-4717 	

INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY

International application No.
PCT/EP2015/050354

Box No. I Basis of the report

1. With regard to the **language**, this report is based on
- ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of:
 - ☐ international search (under Rules 12.3(a) and 23.1(b))
 - ☐ publication of the international application (under Rule 12.4(a))
 - ☐ international preliminary examination (under Rules 55.2(a) and/or 55.3(a) and (b))
2. With regard to the **elements*** of the international application, this report is based on (*replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report*):

Description, Pages

1-4, 7-11, 14, 15, 19, as originally filed
22-24, 31

3a, 5, 6, 12, 13, filed with the demand for preliminary international examination
16-18, 20, 21, 25-30

Claims, Numbers

1-36 filed in electronic form on 04-02-2016

Drawings, Sheets

1/13-13/13 as originally filed

- ☐ a sequence listing - see Supplemental Box Relating to Sequence Listing.
3. ☐ The amendments have resulted in the cancellation of:
- ☐ the description, pages
 - ☐ the claims, Nos.
 - ☐ the drawings, sheets/figs
 - ☐ the sequence listing (*specify*):
4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since either they are considered to go beyond the disclosure as filed, or they were not accompanied by a letter indicating the basis for the amendments in the application as filed, as indicated in the Supplemental Box (Rules 70.2(c) and (c-bis)):
- ☐ the description, pages
 - ☐ the claims, Nos.
 - ☐ the drawings, sheets/figs
 - ☐ the sequence listing (*specify*):
5. ☐ This report has been established:
- ☐ taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rules 66.1(d-bis) and 70.2(e)).
 - ☐ without taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91(Rules 66.4bis and 70.2(e)).

6. ☒ With regard to top-up searches (Rules 66.1 *ter* and 70.2(f)):
- ☒ A top-up search was carried out by this Authority on 01.12.2015 (all discovered documents are listed in the Supplemental Box Relating to Top-up Search).
 - ☐ Additional relevant documents have been discovered during the top-up search.
 - ☐ No top-up search was carried out by this Authority because it would serve no useful purpose.
7. ☐ Supplementary international search report(s) from Authority(ies) has/have been received and taken into account in establishing this report (Rule 45bis.8(b) and (c)).

* If item 4 applies, some or all of those sheets may be marked "superseded".

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>1-36</u>
	No: Claims	
Inventive step (IS)	Yes: Claims	<u>1-36</u>
	No: Claims	
Industrial applicability (IA)	Yes: Claims	<u>1-36</u>
	No: Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.

PCT/EP2015/050354

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

- 1 Reference is made to the following documents:
 - D1 US 2013/246203 A1 (LARACEY KEVIN [US]) 19 September 2013
 - D2 WO 2004/049621 A1 (LOHMAC PTE LTD [SG]; PALOMAKI MACK KALEVI [SG]; LOHMANN OLAF FRITZ HAN) 10 June 2004
 - D3 WO 2013/034192 A1 (NAXOS FINANCE SA [LU]; EZEQUIEL RUIZ RODRIGUEZ [PA]) 14 March 2013
- 2 Document D1 is regarded as being the prior art closest to the subject-matter of claim 1, and discloses:

A system for permitting a communication of at least one set of controlled credentials connected to a presenter from a server to a network endpoint ([0110]: the transaction management system stores or has access to stored credentials. These credentials are released to parties after proper authorisation), said system comprising:

at least one network endpoint ([0110]: "payment credentials are used to obtain payment transaction authorisation from the appropriate payment network...");

at least one accepting appliance configured to send an accepting appliance communication, said accepting appliance communication containing ~~a secret keycode pertaining to said presenter and~~ a once-off shared keycode ([0030], wherein the "checkout token" is equated to the one-off shared keycode);

at least one presenting appliance configured to send a presenting appliance communication, said presenting appliance communication containing a presenter identifier pertaining to said presenter and said once-off shared keycode ([0035]: "the mobile device 102 transmits the token to the transaction management system..."; [0098]: "the transaction lookup request includes information associated with the identity of the customer");

at least one server that further comprises a processor, at least one communications interface and memory storing at least one entry pertaining to said at least one set of connected controlled credentials ([0062]: the transaction management system stores or has access to a database storing payment credentials for the presenter), each entry being affiliated to at least

one record, the record pertaining to any one presenter and comprises a presenter identifier and a secret keycode bound to the presenter identifier ([0034]: the transaction management system stores authentication credentials for the presenters);

wherein said at least one server is configured to:

- a) receive said accepting appliance communication;
- b) receive said presenting appliance communication;
- c) seek a match of said once-off shared keycode contained in said accepting appliance communication with said once-off shared keycode contained in said presenting appliance communication ([0109]: "the system 230 matches the customer checkout token received or looked up at 425");
- ~~d) initiate a search for a target record by linking said secret keycode in said accepting appliance communication with said presenter identifier in said presenting appliance communication, both said accepting appliance communication and said presenting appliance communication containing the same once-off shared keycode;~~
- ~~e) conduct the search for said target record that comprises both said secret keycode and said presenter identifier;~~
- ~~f) identify an entry affiliated with said target record;~~
- g) permit the retrieval of said at least one set of connected controlled credentials pertaining to said entry and permit the release of said at least one set of connected controlled credentials to said network endpoint, said network endpoint being a permitted recipient of a type of said at least one set of connected controlled credentials ([0110]: "to look up the actual payment credentials...the actual credentials are used to obtain payment transactions authorisation from the appropriate payment network").

- 3 The subject-matter of claim 1 therefore differs from this known system in that a secret keycode is provided in the accepting appliance communication and in that the secret keycode is linked with the present identifier in a target record, the target record being used to identify the connected controlled credentials to be released (see crossed out text). The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.

PCT/EP2015/050354

- 4 These features have the effect of ensuring that the presenter at the accepting appliance is the legitimate owner of the presenter device. Therefore, the problem solved by the present invention could be formulated as how to guarantee both authenticity of the credential set and the authenticity of the presenter bearing the credential set.
- 5 The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:
- 5.1 Document D1 discloses a different approach for trying to verify that the presenter device is used by the legitimate owner. According to D1 a secret keycode is verified by the server side at the start of a payment application at the presenting appliance (i.e. independently of any presenting appliance communication). Therefore, D1 teaches away from the solution of claim 1.
- 5.2 Document D2 discloses a transaction authentication system where information received from an accepting appliance (POS) and from a presenter appliance (customer's mobile phone) is matched using a unique transaction code (one-off keycode) and is used by a financial server to authorise a transaction. According to D2 the customer inputs a secret keycode in the POS to prove that he/she is the legitimate owner of the presenting device. D2 fails to disclose the search, retrieval and release of controlled credentials using the secret keycode and the identity received over different communications.
- 5.3 D3 discloses a further transaction authentication method and system using a telephone as presenting appliance, wherein the presenter needs to provide two different PIN codes to authenticate the transaction. A first "validating PIN" is introduced in the telephone whereas an "authenticating PIN" is introduced in the POS. This leads away from the authentication solution of claim 1.
- 5.4 Therefore, there is no indication in the prior art at hand that would prompt the person skilled in the art to modify the system of D1 in order to arrive to a solution according to claim 1.
- 6 The same reasoning applies mutatis mutandis to corresponding claim 25 that is also regarded as defining new and inventive subject-matter.
- 7 Claims 2-14 and 26-36 are dependent on either claim 1 or claim 25 and as such also meet the requirements of the PCT with respect to novelty and inventive step.



MAMC

EUROPEAN PATENT OFFICE
P.O. Box 5818
2280 HV RIJSWIJK (ZH)
Netherlands

By: Online filing

Diegem, November 10, 2015

Gevers ref. PAT2505161PC00 / MAMC / AAFV

International Patent Application No. PCT/EP2015/050354
Mainline Patents Holdings Ltd

DEMAND FOR INTERNATIONAL PRELIMINARY EXAMINATION

Dear Sirs,

We herewith enclose a Demand for International Preliminary Examination in respect of this application and the requisite fee is to be deducted from our Deposit Account at the European Patent Office.

We also enclose a response to the objections raised in the Written Opinion accompanying the International Search Report (WO-ISA), namely, those raised in Boxes V, VII and VII.

In response to the objections raised in the WO-ISA, we enclose new pages 3a, 5, 6, 12, 13, 16 to 18, 20, 21, 25 to 30 and 32 to 40 to replace pages 5, 6, 12, 13, 16 to 18, 20, 21, 25 to 30 and 32 to 39 presently on file. An annotated version of the new pages is enclosed for information.

The Examiner has cited the following documents as being relevant to the claims of the present application:-

D1: US 2013/0246203

D2: WO 2004/049621

D3: WO 2013/034192

1. BASIS FOR THE AMENDMENTS

1.1. New claim 1 corresponds to claim 1 as originally filed but revised to:

1.1.1. Delete the feature "while maintaining the privacy prevailing in said controlled credentials" as the Examiner indicated that this phrase relates to a result to be achieved;

NV **GEVERS** PATENTS SA
Intellectual Property House
Holidaystraat, 5
B-1831 Diegem - Brussels (Belgium)

T : +32 2 715 37 11
F : +32 2 535 99 00
patents@gevers.eu
www.gevers.eu

BTW-TVA : BE 0451.659.120
RPR Brussel - RPM Bruxelles
BE87 732 0047379 94 CREGEBB (CBC)
BE53 310 1012647 53 BBRUBEBB (ING)

BRUSSELS - PARIS - GENÈVE - ANTWERPEN - DIEGEM - GENT - HASSELT - LIÈGE - NIEUCHÂTEL - TOULOUSE
Büro des General-Patents-Verwalters - Ufficio di Patenti e Marchi - Ufficio di Brevetti e Marchi - Bureau des Brevets et Marques - Bureau des Brevets et Marques - Bureau des Brevets et Marques
Full text - Vollständiger Text - Texte complet - www.gevers.patents.be - www.gevers.patents.be - www.gevers.patents.be

- 1.1.2. Add “... from a server to a network endpoint” – support for this feature is to be found in claim 22 as originally filed;
- 1.1.3. Add “said at least one set of controlled credentials connected to said presenter comprising at least one set of connected controlled credentials” – support for this is to be found in claim 1 as originally filed and claim 17 as originally filed where “connected credential set” is recited;
- 1.1.4. Recite “at least one server” – support for this is to be found in paragraph [0011] of the description as originally filed where a controlling server and a different server are described.
- 1.1.5. Revise the steps for consistency with the revisions discussed in paragraphs 1.1.2 to 1.1.4 above.
- 1.2. New claim 2 is supported by claim 1 as originally filed where the feature of the “controlling server” is recited.
- 1.3. New claims 3 to 11 correspond to respective ones of claims 4 to 12 but revised for consistency with the revisions made to new claim 1.
- 1.4. New claims 12 to 14 are based in claim 13 as originally filed. The features have been separated so that the use of “or/and” is no longer required.
- 1.5. New claims 15 and 16 correspond to respective ones of claims 14 and 15 as originally filed but revised for consistency with the revisions made to new claim 1.
- 1.6. New claim 17 corresponds to claim 16 as originally filed but revised to clarify the function of the auxiliary parameters. In particular, the introduction of correlation is supported at paragraph [0073] page 27, lines 26 to 28
- 1.7. New claims 18 and 19 correspond to respective ones of claims 17 and 18 as originally filed but revised for consistency with the revisions made to new claim 1.
- 1.8. New claims 20 and 21 correspond to respective ones of claims 20 and 21 as originally filed but revised for consistency with the revisions made to new claim 1.
- 1.9. New claim 22 corresponds to claim 19 as originally filed but revised for consistency with the revisions made to new claim 1.
- 1.10. New claims 23 and 24 correspond to respective ones of claims 2 and 3 as originally filed.
- 1.11. New claim 25 corresponds to claim 22 as originally filed but revised to have commensurate scope with new claim 1. In particular, the feature “at a server” has been introduced in each of the steps (a) to (g) as each of these steps is performed by a server.
- 1.12. New claim 26 corresponds to claim 23 as originally filed by revised for consistency with the revisions made to new claim 25.
- 1.13. New claim 27 is supported by claim 1 as originally filed where the feature of the “controlling server” is recited.
- 1.14. New claims 28 to 34 correspond to respective ones of claims 28 to 31 but revised for consistency with the revisions made to new claim 25.

- 1.15. New claims 35 and 36 correspond respectively to the features of claims 20 and 21 as originally filed but revised for consistency with the revisions made to new claim 25.
- 1.16. New claim corresponds to claim 32 as originally filed by revised for consistency with the revisions made to new claim 25.
- 1.17. It is submitted that the new claim set is fully supported by the description and claims as originally filed.

2. CLARITY – ARTICLE 6 PCT

- 2.1. It is noted that the Examiner has indicated that claims 1, 19 to 22 and 32 to 34 are not clear.
- 2.2. As indicated by the Examiner in paragraph 6.1, there does not appear to be any limitation relating to the feature of “while maintaining the privacy prevailing in said controlled credentials”. As a result it has been deleted as discussed in paragraph 1.1.1 above.
- 2.3. In relation to the Examiner’s understanding of claim 1, namely, that the “credentials are released in a controlled way ..., they are communicated to an additional party ... without any confidentiality or privacy measures”, it will readily be understood that this is not in fact the case.
- 2.4. New claim 1 has been revised to specify that the communication is between a server and a network endpoint as discussed in paragraph 1.1.2 above, and it is submitted that it is now clear that there is privacy during all communications.
- 2.5. In relation to the feature “presenting peripheral”, this feature has been replaced with “presenting appliance” throughout the claims.
- 2.6. It is submitted that the requirements of Article 6 PCT have been met.

3. NOVELTY – ARTICLE 33(2) PCT

- 3.1. It is noted that the Examiner has not raised any novelty objections to the independent claims at least.
- 3.2. It is therefore submitted that the requirements of Article 33(2) PCT have been met.

4. INVENTIVE STEP – ARTICLE 33(3) PCT

- 4.1. The Examiner has indicated that the independent claims do not involve an inventive step in view of the disclosure of D1 and D2.
- 4.2. We do not believe that any of the cited prior art documents relate to the same technical field as the present invention as they relate to registering payment account details at an acquiring apparatus and generating payment transaction authorizations at that acquiring apparatus.
- 4.3. However, if the Examiner believes that D1 is to be considered as being the closest prior art document, new claim 1 differs from the disclosure thereof by at least the following features:
 - 4.3.1. “at least one accepting appliance”;

- 4.3.2. "said accepting appliance containing a secret keycode ... pertaining to said presenter";
- 4.3.3. "...search for a target record linking said secret keycode in said accepting appliance communication with said presenter identifier in said presenting appliance communication ...";
- 4.3.4. "... said target record that comprises both said secret keycode ... and said presenter identifier ...";
- 4.3.5. "... an entry ... affiliated with said target record"; and
- 4.3.6. "... retrieval of said at least one set of controlled credentials pertaining to said entry ..."
- 4.4. The objective problem to be solved by these differences is to be able to provide an improved system in which presenters may proffer credential sets during exchanges with others in a controlled manner that guarantees both authenticity of the credential set and the authenticity of the presenter bearing the credential set. Ideally, the environment in which such an exchange is to take place provides complete confidentiality and privacy for the credential sets themselves when they are exchanged. This is described in paragraph [0007], page 3, lines 19 to 24 of the description as originally filed.
- 4.5. The differences identified in paragraph 4.2 above solve this problem by providing a secret keycode in an accepting appliance communication which is linked with the presenter identifier in a target record, the target record being retrieved to enable an entry having at least one set of controlled credential to be retrieved and subsequently transmitted to the network endpoint.
- 4.6. Whilst D1 may appear to be in the same or related technical field, it does not appear to address the same objective technical problem as the claims of the present application.
- 4.7. In any case, it is to be noted that the problem to be solved does not need to be novel (see T92/92) and that it is possible to provide an alternative system which solves the same technical problem (see T780/94, T107/92, T323/03 and T824/05). Therefore, it is not necessary to show improvement over the prior art in accordance with T588/93 and that an earlier solution to the same technical problem does not preclude the solution of the same problem in another, non-obvious way (see T1791/08).
- 4.8. In this case, the fact that the secret keycode is linked to a presenter identifier and stored in a target record having an entry which relates to at least one set of controlled credentials involves an inventive step.
- 4.9. The method as disclosed in D1 is a two-step process where the presenter is first authenticated by entering the User Name/Password combination to have accessed to the App/Portal on the mobile device, and, thereafter a message with a share common ID is transmitted to the central server to authorise a transaction. The central server matches the share common ID with the share common ID in the request message from the merchant device (similar to the accepting appliance) and releases the credit information of the presenter to the payment server once the share common ID is matched without further regard to the User Name or other identifiers relating to the presenter.
- 4.10. This will cause a problem when multiple messages with the same common ID are receive at the shared server, and there is a possibility that the presenters are not matched correctly to the relevant transactions resulting in one or more payments being apply to one or more unintended transactions.
- 4.11. The present invention addresses this issue as "what the presenter knows" and "what the presenter has" are never together in the same device. For fraud or unintended transfer of secure information to occur, both the

- presenting appliance and shared keycode, but not just one of them, need to be compromised and made available to the same fraudster.
- 4.12. In the present invention, shared keycodes in appliance communications are matched at the controlling server and then a secret keycode and presenter identifier are used to retrieve the controlled credentials from a target record and forward the controlled credentials to a network end point. This provides a “permitted emission” of actual entries of credentials controlled at the controlling server to the network end point.
- 4.13. In accordance with the present invention, credentials are provided at a presenting location by a presenting appliance and are required at an accepting location by an accepting appliance or end point. The credentials are controlled by at least one server which operates to :
- 4.13.1. Receive an accepting appliance communication containing a shared keycode and a secret keycode;
- 4.13.2. Receive a presenting appliance communication containing a presenter identifier and a copy of the shared keycode;
- 4.13.3. Seek to match the accepting appliance communication with the presenting appliance communication using the shared keycode;
- 4.13.4. Having matched the accepting appliance communication with the presenting appliance communication, pair the presenter identifier in the presenting appliance communication with the secret keycode in the accepting appliance communication;
- 4.13.5. Search for a target record which contains the pairing of the same presenter identifier and the same secret keycode;
- 4.13.6. Identify an entry affiliated to the target record which pertains to controlled credentials;
- 4.13.7. Retrieve the controlled credentials from the identified entry; and
- 4.13.8. Release the controlled credentials to the accepting appliance or end point.
- 4.14. By having the controlled credentials communicated from a server to the accepting appliance or end point only when there are two matches of data, namely, the shared keycode and the presenter identifier and secret keycode, a robust and safe system is provided from transferring controlled credentials from one appliance to another. In effect, a secure channel is established between the presenting appliance and the accepting appliance or end point via the server(s) only when the matches are identified.
- 4.15. In the present invention, only one communication message is sent by each of the presenting device and the accepting device to the server. Each communication message includes the shared keycode or a copy thereof so that the two messages can be matched at the server and the server will only authorise the release of the appropriate credentials should the presenter ID (in the presenting appliance communication) and secret keycode (in the accepting appliance communication) are matched. If multiple messages with the same share keycode are received at the server (but which do not have matching presenter ID and secret keycode), the transaction will not be processed further.
- 4.16. This second matching step, which is not present in D1, provides a safe guard and ensures the credentials are only released for a correct request.

NV **GEVERS PATENTS SA**
Intellectual Property House
Holidaysstraat, 5
B-1831 Diegem - Brussels (Belgium)

T : +32 2 715 37 11
F : +32 2 535 99 00
patents@gevers.eu
www.gevers.eu

BTW-TVA : BE 0451.659.120
RPR Brussel - RPM Bruxelles
BE87 732 0047379 94 CREGBEBB (CBC)
BE53 310 1012647 53 BBRUBEBB (ING)

BRUSSELS – PARIS – GENÈVE – ANTWERPEN – DIEGEM – GENT – LIASSET – LIÈGE – NEUCHÂTEL – TOULOUSE
Extrait from the General Terms and reverse side - Uitdrukking van de Algemene Voorwaarden die hierop zijn - Extrait des Conditions Générales voir verso
Teil 102 - Vollständige Text - Texte complet - voir verso - General Terms and conditions

- 4.17. D1 requires the presenter to login, using a User Name/Password combination, to the App/Portal on a mobile device to obtain access to the service. As a result, "what the presenter knows" and "what the presenter has" are available in the same place, that is, on the mobile device. This will compromise the integrity of the presenter account should the mobile device be stolen or is misplaced.
- 4.18. Furthermore, the User Name/Password entered into the mobile device will be cached in the memory of the mobile device and may be recovered by a skilled person or may be intercepted during the transmission to a central server. Once the User Name/Password combination is compromised, any third party can subsequently make use of this User Name/Password combination and authorise the central server to release the financial information from any device and authorise the payment for any unintended transactions.
- 4.19. The use of the User Name/Password combination in D1 is not the same as the use of the secret keycode and the presenter identifier as used in the present invention. The purpose of entering the User Name/Password combination on the mobile device of D1 is to obtain access or "restricted admission" to a user profile registered at a payment transaction management system for transactions with billing entities.
- 4.20. It is emphasized that the linking of the keycode with the presenter identifier and with another keycode is not disclosed or suggested by the disclosure of D1.
- 4.21. It is therefore submitted that new claim 1 involves an inventive step over the disclosure of D1 when considered alone.
- 4.22. It is noted that the Examiner indicates that "the same technical effect can be achieved by providing a keycode through the accepting appliance to convey the PIN" and refers to D2, page 24, lines 3 to 6 and D3, page 8, line 30 to page 9, line 31.
- 4.23. The relevant passage of D2 refers to the implementation of a PIN system in which the PIN is entered by the customer through a keypad of a POS terminal or computer. In this case, a transaction is associated with such a PIN but this relates to the accepting appliance and not to the presenting appliance.
- 4.24. Whilst D2 appears to disclose a single transaction related to an accepting appliance, there is no link between respective communications between a presenting appliance and a server and an accepting appliance and the server where both shared keycodes in the presenting communication (presenting appliance to server) and the accepting appliance communication (accepting appliance to server) are matched at the server to enable the transfer of credentials between the presenting appliance and the accepting appliance or end point.
- 4.25. It is therefore submitted that a person skilled in the art, starting from the disclosure of D1, would not look to the disclosure of D2 to arrive at the solution provided by the present invention and as defined in new claim 1.
- 4.26. The relevant passage of D3 relates to the authentication and validation of a transaction using two different PIN codes, a validating PIN entered by the user and an authenticating PIN entered by the user on a different device.
- 4.27. As discussed in paragraph 4.13 above, only one communication is sent between the presenting appliance and the server and the accepting appliance and the server where the shared keycodes are matched before the credentials are retrieved and transferred accordingly.
- 4.28. It is therefore submitted that a person skilled in the art, starting from the disclosure of D1, would not look to the disclosure of D3 to arrive at the solution provided by the present invention as defined by new claim 1.

- 4.29. It is therefore submitted that new claim 1 involves an inventive step over the disclosure of D1 when combined with the disclosure of either one of D2 or D3.
- 4.30. Similar reasoning can be applied *mutatis mutandis* for the corresponding independent method claim, new claim 25.
- 4.31. As dependent claims 2 to 24 and 26 to 37 depend from respective independent claims possessing inventive step, it is submitted that each of these claims also possesses inventive step as being directed to solving the same technical problem.
- 4.32. It is therefore submitted the requirements of Article 33(3) PCT have been met.

5. DEFECTS IN THE INTERNATIONAL APPLICATION

- 5.1. In accordance with paragraph 4 of the WO-ISA, reference signs have been added to the claims where considered to be appropriate in accordance with Rule 6.2(b) PCT.
- 5.2. New page 3a has been revised to include new paragraphs [0007a] to [0007c] which acknowledge the disclosures of D1 to D3 in accordance with Rule 5.1(a)(ii) PCT (paragraph 5 of the WO-ISA).

6. OTHER AMENDMENTS

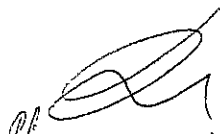
- 6.1. New pages 5, 6, 12, 13, 16 to 18, 20, 21 and 23 to 30 have been revised to bring the terminology used in the description into conformity with that used in the claims. In addition, these pages have been revised for consistency with the rest of the description and the drawings as originally filed.
 - 6.1.1. New pages 5 and 6 have been revised to remove superscripts and/or references and asterisks which do not link to anything else within the description as originally filed – see in particular, the last line of paragraph [0008] and paragraphs [0009] [0012] and [0013].
 - 6.1.2. New pages 12, 16 to 18, 20 and 21 have been revised to replace the term “peripheral” with the term “appliance” for consistency with the claims and with the description – see for example, the use of the terms “accepting appliances” (last line of paragraph [0048]) and “presenting appliances” (page 17, line 31).
 - 6.1.3. New page 13 has been revised to remove an unnecessary “.” (full stop) in the first line of paragraph [0042].
 - 6.1.4. New page 16 to 18 have also been revised to correct the reference numerals for consistency with other parts of the description and the drawings. In particular:
 - 6.1.4.1. “appliance 108” has been changed to “appliance 109” in paragraph [0048] as this paragraph is directed to “accepting appliances” which are shown in Figure 1 as having the reference number “109”;
 - 6.1.4.2. “communication channel 106” has been changed to “communication channel 107” in paragraph [0048] as this paragraph is directed to “accepting appliances” as discussed in paragraph 6.1.5.1 above with Fig. 1 showing the connection to the server 101 via a network referenced as 107;

- 6.1.4.3. “appliance 109” and “communication channel 107” in paragraph [0049] have been changed to read “appliance 108” and “communication channel 106” as this paragraph is directed to the “presenting appliances” (see page 17, line 19);
- 6.1.4.4. “router 103” has been replaced with “server 101” in paragraph [0049] (see page 17, line 24) and it is clear from the description that the wireless devices do not communication with a “router” as mentioned in the same paragraph but with a server 101 as stated at page 17, line 22;
- 6.1.4.5. “presenting appliances” in paragraph [0048], page 17, line 31 has been revised to read “presenting appliances 108 and server 101” as it is clear from Fig. 1 that “the connection between the presenting appliances” need to be connected to something else to form “a second communications channel 106”;
- 6.1.4.6. “presenting peripheral 105, 107, 109” in paragraph [0051] at page 18, line 20 has been revised to recite “presenting appliance 108” for consistency with the claims and description as discussed in paragraph 6.1.2 above – it is clear from Fig. 1 that “105” relates to a presenting appliance communication; “107” refers to a network or communications channel; and “109” relates to an accepting appliance; and
- 6.1.4.7. “embodiments, this invention” at page 18, line 24 of paragraph [0051] has been revised to read “embodiments of this invention” – the addition of the word “of” does not add subject matter to the description as originally filed.
- 6.1.5. New page 20, in addition to the revisions discussed in paragraph 6.1.2 above, paragraph [0055] has been revised:
- 6.1.5.1. to add reference number “108” at line 13 for consistency with the description and claims so that it now reads “presenting appliance 108”;
- 6.1.5.2. to revise line 15 to read “permitting the server to release ...” – the addition of the word “to” does not add subject matter to the description as originally filed.
- 6.1.6. New page 21 also includes a correction of a reference numeral at line 19 – reference numeral “111” does not apply to the accepting appliance and hence the reference numeral has been corrected to read “109”. Support for this revision is discussed in paragraph 6.1.4.6 above.
- 6.1.7. New page 25 has been revised to incorporate reference numeral “1005” for the accepting appliance at line 2 thereof. Support is to be found at page 24, lines 31 and 32 where “accepting appliance 1005” is stated.
- 6.1.8. New page 25 has also been revised at the end of paragraph [0066] to add a full stop (“.”) for the end of the sentence.
- 6.1.9. New page 26 has been revised for clarity. In particular, the reference numerals “1002”, “1013”, “1014”, “1015” have been repeated in respective paragraphs [0068], [0069], [0070] and [0071] and some of these reference numerals have been deleted for clarity.
- 6.1.10. In addition, at the last line of paragraph [0069], the term “presenter identifier 1002” has been revised to read “presenting interactor” for consistency with the last line of paragraph [0067].

- 6.1.11. New page 26 has also been revised line 19 to include the word “an” such that it now reads “In such an embodiment, ...” – the addition of the word “an” does not add any subject matter to the description as originally filed. Similarly, at line 20, “... connected the presenting interactor ...” has been revised to read “... connected with the presenting interactor ...”.
- 6.1.12. New page 27 has been revised in a similar way to new page 26 in that superfluous reference numerals (“1016” at line 4 and “1017” at line 29).
- 6.1.13. New page 27 has also been revised to add reference numeral “1003” at line 16 (“presenting appliance 1003”) – this is for consistency with line 2.
- 6.1.14. New page 28 has been revised at line 25 to remove superfluous reference numerals.
- 6.1.15. New page 29 has been revised to remove superfluous reference numerals at lines 2, 17, 21, 23 and 31. In addition, “Server 1001” has been revised to read “server 1001” at line 14 and reference numeral “1002” has been added at line 30.
- 6.1.16. New page 30 has been revised to remove superfluous reference numerals at lines 2 and 19 to 21. In addition, “Server 1001” has been revised to read “server 1001” at line 5.
- 6.2. It is submitted that none of the above revisions to pages 5, 6, 12, 13, 16 to 18, 20, 21 and 25 to 30 add subject matter to the present application.

We look forward to receiving a positive IPRP in due course.

Yours faithfully


Margaret Mackett

Enclosures: New pages 3a, 5, 6, 12, 13, 16 to 18, 20, 21, 25 to 30 and 32 to 40 together with an annotated version thereof.

NV **GEVERS** PATENTS SA
Intellectual Property House
Holidaysstraat, 5
B-1831 Diegem - Brussels (Belgium)

T : +32 2 715 37 11
F : +32 2 535 99 00
patents@gevers.eu
www.gevers.eu

BTW-TVA : BE 0451.659.120
RPR Brussel - RPM Bruxelles
BE87 732 0047379 94 CREGBEBB (CBC)
BE53 310 1012647 53 BERUBEBB (ING)

BRUSSELS - PARIS - GENÈVE - ANTWERPEN - DIEGEM - GENT - HASSELT - LIÈGE - NEUCHÂTEL - TOULOUSE
Extract from the National Forms on reverse side - Extracts from the Administrative Correspondence of the Office - Extract from the Conditions of Sale of the Office
Full text - Vervolgende tekst - Texte complet - complete text - complete text - complete text

3a

[0007a] US-A-2013/0246203 discloses conducting payment transactions in which fraud is reduced. Payment credentials of a customer are never provided to a merchant and cannot be accessed for use in the payment transaction unless an access request is provided from an authorized device designated by the
5 customer. In one embodiment, the authorized device comprises a mobile phone.

[0007b] WO-A-2004/049621 discloses an authentication system in which a first terminal communicates with a facilitator over a first telecommunications channel and a second terminal communicates with an operator over a second
10 telecommunications channel, the facilitator and the operator being able to communicate with one another. No identity data is provided to the first terminal by the operator, the facilitator or the second terminal, and no identity data of the first terminal is provided to the second terminal by the operator, the facilitator or the first terminal, and, communication between the first terminal
15 and the facilitator and between the second terminal and the operator does not contain data regarding the identity details of the user.

[0007c] WO-A-2013/034192 discloses a method for validating an electronic transaction in which identifying data is transferred from a mobile phone to a point-of-sale terminal and which needs to be validated by a PIN code provided
20 to the server during a voice telephone call.

- communications contain the same shared keycode; (e) conduct a search for said target record that comprises both said secret keycode and said presenter identifier; (f) identify an entry affiliated with said target record, said entry pertaining to a set of controlled credentials connected to the presenter; (g) permit the retrieval of said credential set pertaining to said entry and permit the release of said credential set to said network endpoint, said endpoint being the permitted recipient of a set of controlled credentials connected to said presenter, and said endpoint being either the accepting appliance or that of a designated third party linked to the accepting appliance.
- 10 [0009] Another aspect of the invention comprises a method to permit a communication of at least one set of controlled credentials connected to a presenter, from a server to a network endpoint, while maintaining the privacy prevailing in said controlled credentials connected to the presenter; and wherein a server comprises one or more records, each record pertaining to a presenter (given
- 15 party enrolled with the server as a presenter and/or as an acceptor), and each record comprising a presenter identifier (and/or acceptor identifier) and a (presenter and/or acceptor) secret keycode bound to said presenter identifier, and each record is affiliated with an entry pertaining to a set of controlled credentials (associated with said party) connected to said presenter; the method comprising: (a) at an accepting
- 20 appliance, making a once-off shared keycode available to a/the presenting interactor; (b) at the accepting appliance, receiving a (presenter) secret keycode pertaining to the presenting interactor wherein said (presenter) secret keycode is input at the accepting appliance by the presenting interactor; (c) at the accepting appliance, communicating an accepting appliance communication to at least one of
- 25 the servers, said accepting appliance communication containing the once-off shared keycode and the (presenter) secret keycode; (d) at a presenting appliance of the presenting interactor, receiving the once off shared keycode; (e) at the presenting appliance, retrieving a presenter identifier pertaining to the presenting interactor from a storage location on the presenting appliance; and (f) at the presenting
- 30 appliance, communicating a presenting appliance communication to said server, said presenting appliance communication containing the once-off shared keycode and the presenter identifier, wherein (g) upon receipt of said accepting appliance

communication and said presenting appliance communication, at a the server processing the communications to ascertain if it is permitted to communicate a set of controlled credentials connected to the presenter, thereby permitting its retrieval at a server and thereby permitting its release to a network endpoint, said endpoint
5 being a permitted recipient, and said endpoint being either the accepting appliance or that of a designated third party linked to the accepting appliance.

[0010] In an aspect of the invention, all credential sets connected to the presenter (or aliases affiliated to credential sets) may be comprised as entries in said record.

[0011] In another aspect of the invention, all credential sets connected to the
10 presenter (and aliases affiliated) may be comprised as separate entries on a different server communicable with a controlling server. Alternatively, some credential sets connected to the presenter and aliases affiliated may be comprised as entries in said record, whereas others may be comprised as separate entries on said server or separate entries on different servers.

15 [0012] The accepting appliance communication may be communicated to said server over a first communication channel and the presenting appliance communication may be communicated to said server over a second communication channel.

[0013] In an aspect of the invention, the once-off shared keycode may be generated
20 at the server and communicated to the accepting appliance before said once-off shared keycode is made available to the presenting interactor or/and the presenting appliance.

[0014] In another aspect of the invention, the once-off shared keycode may be generated at the accepting appliance before said once-off shared keycode is made
25 available to the presenting interactor or/and the presenting appliance.

[0015] A copy of the once-off shared keycode may be communicated from the accepting appliance to the presenting appliance via a wireless technology, the wireless technology optionally selected from a group comprising Wifi, bluetooth, NFC or RFID.

30 [0016] In an aspect of the invention, a validity period may be assigned to the

seeking to match the predetermined auxiliary parameter contained in the accepting appliance communication with the corresponding predetermined auxiliary parameter contained in the presenting appliance communication.

5 [0032] If a validity period is assigned to the once-off shared keycode, said shared keycode may be unique over the duration of its validity period.

[0033] In another aspect of the invention, a method comprising (a) an accepting appliance making a once-off shared keycode available to the presenting interactor; (b) receiving a presenter secret keycode belonging to the presenting interactor at the accepting appliance wherein said presenter secret keycode is input at the terminal by
10 the presenting interactor; (c) communicating an accepting appliance communication from the accepting appliance to the server, the accepting appliance communication comprising the once-off shared keycode and the presenter secret keycode; (d) the presenting appliance receiving the once off shared keycode; (e) the presenter appliance retrieving a presenter identifier belonging to the presenting interactor
15 from a storage location on the presenting appliance; and (f) the presenting appliance communicating a presenting appliance communication to the controlling server, the presenting appliance communication comprising the once-off shared keycode, and the presenter identifier.

[0034] The target record at said server may also further comprise an alias
20 associated with said entry pertaining to each credential set connected to the presenter, and the presenting appliance communication may further contain a copy of an alias selected from a list of aliases itemized at the presenting appliance, and wherein the step of conducting a search for a target record that comprises the same presenter identifier and secret keycode also utilizes the alias contained in the
25 presenting appliance communication to search for a target record comprising the same said alias in addition to the same presenter identifier and secret keycode.

[0035] The credential set may be comprised as an entry in said target record on said controlling server configured to permit the retrieval and release of the controlled credentials, and the steps of retrieving the credential set and releasing the credential
30 set are performed at said controlling server configured to permit the retrieval and release of the controlled credentials.

[0036] The credential set may be comprised as an entry on a different server separate to the said controlling server configured to permit the retrieval and release of the controlled credentials, the separate entry being affiliated with the target record, and wherein the steps of retrieving and releasing the credential set may be performed at either said controlling server configured to permit the retrieval and release of the controlled credentials or the different server separate to that controlling server configured to permit the retrieval and release of the controlled credentials.

[0037] A further aspect of the invention comprises a presenting appliance configured to perform one or more of the presenting appliance steps described above.

[0038] Another aspect of the invention comprises an accepting appliance configured to perform one or more of the accepting appliance steps described above.

[0039] An additional aspect of the invention comprises a server configured to perform one or more of said server steps described above.

[0040] A further aspect of the invention comprises a system comprising two or more of the presenting appliances, two or more of the accepting appliances, and said controlling server configured to perform one or more of the embodiments as described above.

[0041] An additional aspect of the invention comprises a computer readable storage medium carrying a computer program stored thereon, said program comprising computer executable instructions adapted to perform one or more of the method steps described above when executed by one or more processing modules.

Detailed Description

[0042] Figure 1 is a diagram illustrating the central system to preserve privacy in a manner that also facilitates permitted release of a stored credential set to a recipient approved by the participant to whom the credential set pertains. The system 100 is secure in that it protects the credential sets from unauthorized access by unauthorized would-be recipients of the credential sets, and also prevents the credential sets from use by those who would fraudulently present a credential set as

keycode. The accepter identifier is a unique string that is used to identify a given accepter record within the accepter record collection. The accepter secret keycode (if applicable) is a string known only to the accepter. When an accepter interacts with the system with a view to facilitating the release of a presenter credential set associated with the presenting interactor with a designated recipient (such an accepter is referred to as an "accepting interactor") the accepter identifier of the accepting interactor is provided, and the accepting interactor's accepter secret keycode (if utilized) can then be employed to authenticate the accepting interactor before any credential sets are disclosed.

10 [0046] It will be appreciated that while in this described embodiment of the invention, the presenter records and accepter records are distinct and are typically maintained as separate record collections, in other embodiments of the invention, the server 101 may comprise a single record collection comprising both presenter and accepter records. Furthermore, it will also be appreciated that while in one
15 embodiment, an accepter's and/or presenter's credential sets are stored on a server, multiple servers are also envisaged, wherein each server is tasked with the storage of records comprising one or more credential set types.

[0047] It is additionally envisaged that in some embodiments of the invention, the server 101 will solely comprise presenter records, and will comprise no accepter
20 records. Preferably, in such embodiments, the server 101 and potential accepting interactors will be capable of communicating with one another via their existing software systems. This embodiment of the invention is advantageous because pre-enrolment of accepters is not required, and this removes an obstacle to uptake of the claimed system and method amongst potential accepting interactors. This therefore
25 improves ease of use of the system and method.

[0048] The server 101 is communicable with one or more appliances 109 over a communication channel. It will be appreciated that the communication channel 107 may comprise the Internet, a proprietary network, or a combination of the two. Appliance 109 may be disparately located, and may connect to the communication
30 channel 107 by way of one or more of a variety of technologies, such as PSTN, Ethernet, DSL, ISDN, Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. The appliances 109

may be any of a variety of devices including desktop personal computers, laptops, tablet personal computers, personal digital assistants, mobile phones, smartphones etc. The appliance 109 may alternatively comprise bespoke computing systems as used in a variety of industries including banking, finance, aviation, travel, homeland security, border control, energy, transport, retail and/or telecommunications. Accordingly, the appliances may comprise devices configured to act as Point of Sale devices. In the context of the invention, these appliances will be referred to as "accepting appliances".

[0049] The server 101 is also communicable over a communication channel 106 with one or more appliances 108. Such appliances may comprise, for example, wireless devices communicable with the server 101 via a wireless base station or router. The wireless devices may comprise any form of wireless device including laptops, tablet personal computers, personal digital assistants, mobile phones, smartphones etc. Such peripheral devices may further comprise devices communicable over communication channel 106 via a wired connection, and thus may, for example, include desktop computers as well as industry-specific bespoke computing systems mentioned above, including but not limited to Point of Sale systems. In the context of the invention, these peripheral devices will be referred to as "presenting appliances". In an embodiment, the presenting appliance may also be password-protected or may require additional permission from the presenter to initiate communication. The presenting peripherals may be disparately located, and may communicate with the server 101 over communication channel 108 via a variety of means such as PSTN, Ethernet, DSL and ISDN. Presenting appliances comprising wireless devices may communicate with server 101 by way of one or more of a variety of wireless communications technologies, such as Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. The communication channel 106 may comprise the Internet, a proprietary network, or a combination of the two. The presenting appliances 108 are configured with an application that facilitates communication with the server 101. As the connection between the accepting appliances 109 and the server 101 comprise a first communications channel 107 and the connection between the presenting appliances 108 and server 101 comprise a second communications channel 106, the system 100 may be regarded as being "multichannel" in

composition. This ensures a more secure mechanism by which credential sets and other sensitive data may be stored and released to network endpoint 110 while remaining in a state of privity. The network endpoint 110 in some embodiments may be either a separate appliance or the accepting appliance itself depending on
5 designated destination in the accepting appliance communication.

[0050] While in this embodiment, it has been described that the credential sets and connected aliases are comprised in the presenter and/or acceptor records on the server, in other embodiments of the invention, it is anticipated that said credential sets and connected aliases may be affiliated with said presenter and/or acceptor
10 records in alternative ways. For example, the credential sets and affiliated aliases may be comprised in one or more record sets separate to the record set(s) on the server that comprise the records comprising the identifiers and secret keys. These separate record sets may be housed on one or more different servers. In some embodiments of the invention, the different servers housing the credential sets are
15 administered by the controllers responsible for the issuance of the instruments comprising said credential sets.

[0051] Figure 2 is a flowchart illustrating how a new potential applicant enrolls with the server 101 as a presenter in accordance with an embodiment of the invention. At step 200, a web page hosted by the server 101 is accessed by the new
20 presenter applicant, preferably using their presenting appliances 108. The web page is configured such that at this step, the new presenter applicant provides general enrolment details such as name, address, email address, country of residence, etc. and submits these to the server 101. It will be appreciated that while in some embodiments of this invention, the enrolment details are provided directly to the
25 server 101, in other embodiments, the enrolment details may be pre-provided indirectly for pre-processing prior to entry of the details in the server 101. The web page may be accessed over a connection for the duration of the procedure, or else secure connections may merely be used only where sensitive information (such as a credential set or additional data such as a presenter's secret keycode) is being
30 transmitted. It will also be appreciated that alternative means of enrolment are possible such as by way of submitting a completed form by mail, fax, etc.

[0054] At step 206, the new presenter applicant is given the opportunity to set specific preferences associated with the processing and usage of credential sets associated with particular governmental or commercial oversight bodies and the interaction types to which they pertain. By way of example, with respect to a credential set pertaining to an airline loyalty membership, the presenter may be given the option to set additional preferences in accordance with their membership preferences, such as preferred airline meal, seat reference, or local airport. By way of a further example, with respect to a credential set pertaining to a credit card, the presenter may be given the option to enable functionalities such as card preference usage, direct currency conversion, value added tax refunding for travelers or splitting payment over multiple cards.

[0055] At step 208, the new presenter applicant is then prompted to install a bespoke application on their presenting appliance 108. The bespoke application is configured to facilitate communication with the server as required during the process of permitting that the server to release a credential set and the process of authenticating such a transmitted permission as will be described in greater detail below. During the course of installing the bespoke application, the application is associated with a unique presenter identifier that is retained on the presenting appliance. In a preferred embodiment, the presenter identifier is assigned by the server, and is embedded in the application before, during or after the application is installed on the presenting appliance. Alternatively, the presenter identifier may be derived from a sequence of characters native to the presenting appliance, for example an IMEI number or serial number. This sequence of characters may be modified to arrive at a unique presenter identifier. In addition to retention on the presenting appliance, the presenter identifier is also added to the presenter record in the presenter record collection on the server 101. During the course of installing the bespoke application, the application is also provided with the aliases connected to the credential sets stored in step 204 for a given presenter. Accordingly, when the application is used in an interaction by the new presenter, it has at its disposal both a presenter identifier and the aliases connected to the new presenter's credential sets such that the presenter identifier and an alias may be communicated to the server 101 as appropriate.

[0056] In a preferred embodiment, a generic version of the application may be

initially installed on a new presenter applicant's presenting appliance. Subsequent to the process depicted in steps 200-208, the new presenter applicant may be prompted to authenticate their account by replying to an email, and/or by confirming their presenter's secret keycode in reply to a prompt from the server. Subsequent to this authentication, the generic version of the application on the new presenter applicant's presenting appliance may be customized with the new presenter applicant's presenter identifier, the aliases connected to the new presenter applicant's credential sets, and the new presenter applicant's preferences as configured in step 206. This data may be stored in an encrypted format on the new presenter applicant's presenting appliance. Figure 3 is a flowchart similar to that of Figure 2 depicting the steps via which a party may enroll as an acceptor with the server 101 in accordance with an embodiment of the invention. As previously indicated, the invention envisages embodiments where the acceptor must actively enroll with the server, as well as embodiments where it is not necessary for the acceptor to enroll with the server. Furthermore, in other embodiments of the invention, enrolment of the acceptor may be done "passively" as will be described in greater detail below. At step 300, a web page hosted by the server 101 is accessed by the party (hereafter referred to as a "new acceptor applicant"), preferably using the accepting appliance 109. In a fashion analogous to step 200 of Figure 2, the web page is configured such that at this step, the new acceptor applicant provides general enrolment details such as the name of the individual or organization, address, email address, etc. and submits these to the server 101. The web page may be accessed over a secure connection for the duration of the procedure, or else secure connections may merely be used only where sensitive information (such as an acceptor's secret keycode or an acceptor's credential set) is being transmitted. It will be further appreciated that enrolment of new acceptor applicant may take place by way of other means such as by mail or fax. Alternatively, if the acceptor operates an accepting appliance that is remote controlled by a linked third party (such as, for example, Terminal Management Systems used by Acquirers to manage card payment Point of Sale devices, enrolment of an acceptor may be initiated by the linked third party. In such scenarios, it may not be necessary for the acceptor to provide any information themselves.

endpoint 1004 is linked to an accepting appliance 1005), and whereby the accepting appliance 1005 is configured to generate and transmit an accepting appliance communication to the server 1001. The presenting interactor 1002 may decide to interact at such facility with a view to permitting a reading of a credential set
5 connected to the presenting interactor 1002 to be released to the network endpoint 1004 or the accepting appliance 1005. The accepting interactor may also decide to interact at such facility with a view to requesting a reading of a credential set connected to the accepting interactor to be returned to the network endpoint 1004 or accepting appliance 1005 when receiving the credential set connected to the
10 presenting interactor 1002 at the network endpoint 1004 or the accepting appliance 1005. More specifically, a state of privacy prevailing in the credentials connected to the presenting interactor 1002 is preserved in the preferred embodiment of the present invention, whereby a reading of the set of credentials connected to the presenting interactor 1002 is not visible to or accessible by the accepting interactor
15 nor communicated to or by presenting appliance 1003, but only communicated confidentially to the network endpoint 1004 or accepting appliance 1005.

[0066] In Figure 10, and at the event precedent 1010, a signal is conveyed at the network endpoint 1004 or the accepting appliance 1005 to a presenting interactor 1002, indicating that the said method devised in the present invention is a method
20 available at the network endpoint 1004 or accepting appliance 1005 for the presenting interactor 1002, whereby the network endpoint 1004 is equipped with such accepting appliance 1005 and wherein such accepting appliance 1005 is configured to communicate with Server 1001. In effect, the said method devised in the present invention is one of the methods available at the network endpoint 1004
25 for obtaining credentials from presenting interactor 1002.

[0067] In Figure 10, and at the event precedent 1011, a presenting interactor 1002 decides to initiate an interaction at the facility operated at the accepting interactor as per the process of the method devised by the present invention by availing of the presenting appliance 1003 configured to generate and transmit a presenting
30 appliance communication to such server 1001, and availing of an accepting appliance 1005, configured to generate and transmit an accepting appliance communication to such server 1001. In effect, the presenting interactor 1002 selects

to initiate an interaction at the facility of the accepting interactor as per the process of the method devised by the present invention, declining to initiate an interaction at the facility operated at the accepting interactor as per any other process of prior methods available at the network endpoint 1004 for obtaining credentials from
5 presenting interactor 1002.

[0068] At stage 1012, an interaction is initiated by activating the accepting appliance 1005 that is configured to facilitate accepting appliance communications with server 1001. On activation at 1012, a once-off shared keycode is produced
10 1012 at the accepting appliance 1005. In one embodiment, the shared keycode is generated by the server 1001 and transmitted to the accepting appliance 1005. In another embodiment, the shared keycode is generated at the accepting appliance 1005.

[0069] At stage 1013, an interaction is initiated by activating the presenting appliance 1003 that facilitates presenting appliance communications with server
15 1001. On activation at 1013, a presenter identifier is retrieved from a storage location on the presenting appliance 1003. In one embodiment, a list of aliases associated to the credentials connected the presenting interactor 1002 related to the presenter identifier also retrieved from some storage location on the presenting appliance 1003. In such an embodiment, such a list of aliases associated to the
20 credentials connected with the presenting interactor are itemized on the presenting appliance 1003 for selection by the presenting interactor 1002.

[0070] At stage 1014, a shared keycode is rendered available at the accepting appliance 1005 to presenting interactor 1002 and presenting appliance 1003. In one embodiment of 1014, it is rendered human-readable at accepting appliance 1005. In
25 another embodiment of 1014, it is rendered machine-readable at accepting appliance 1005.

[0071] At stage 1015, the shared keycode is obtained accordingly at the presenting appliance 1003. In one embodiment, it is obtained by reading it at the accepting appliance 1005 and inputting it in to the presenting appliance 1003. In another
30 embodiment, it is obtained by scanning it at the accepting appliance 1005 and capturing it on to the presenting appliance 1003. In one embodiment, the accepting

appliance 1005 transmits the once-off shared keycode directly 1014 to the presenting appliance 1003, whereas in another embodiment, the accepting appliance 1005 makes the shared keycode available 1014 to the presenting interactor 1002, who enters it at 1016 into the presenting appliance 1003. In some embodiments of the invention, a validity period may be assigned to the shared keycode. This ensures that if a received accepting appliance communication and a received presenting appliance communication are not corroborated within a certain timeframe by seeking to match the once-off shared keycodes (as discussed further below) within a certain timeframe (the validity period), then the interaction may lapse and thereby become void rendering further processes redundant. Upon expiry of the validity period of a shared keycode, the same shared keycode thus may be re-used in a subsequent iteration of the method. Accordingly, a validity period can ensure that shorter, less complex secret keys can be used because shared keycode re-use is thereby feasible. This is advantageous in embodiments of the invention where it is necessary for the presenting interactor to enter the shared keycode into the presenting appliance 1003, as reduced keycode complexity makes this embodiment of the method more manageable.

[0072] In some embodiments, the presenting appliance 1003 may also display a list of aliases pertaining to different presenter credential sets connected to said presenting interactor 1002. The presenting interactor 1002 then selects an alias associated to the desired credential set connected to the presenting interactor 1002.

[0073] At stage 1016, the accepting appliance seeks to obtain the secret keycode of the presenting interactor 1002 by prompting the presenting interactor 1002 to enter the presenter's secret keycode on the accepting appliance 1005. In one embodiment, the accepting appliance 1005 may additionally display at 1012 a predetermined auxiliary parameter to the presenting interactor 1002 in order to further correlate the interaction and corroborate the accepting appliance communication and the presenting appliance communication.

[0074] At 1017, the secret keycode is obtained by the accepting appliance 1005. In one embodiment, the presenting interactor 1002 uses a keypad to enter the secret keycode on the accepting appliance 1005. In another embodiment, the presenter

interactor 1002 may use a device to convey the secret keycode to the accepting appliance 1005.

[0075] At stage 1019, the accepting appliance 1005 then transmits an accepting appliance communication to the server 1001 permitting release of a specific credential set(s) connected to the presenting interactor 1003 to the facility
5 of the recipient permitted by the presenting interactor 1002. The accepting appliance communication contains the presenter's secret keycode as obtained at 1017 and the once-off shared keycode as generated at 1012. The accepting appliance communication may also contain an identifier pertaining to the accepting
10 interactor if retrieved following 1012 and any auxiliary predetermined parameters if captured following 1012.

[0076] At stage 1018, the presenting appliance 1003 transmits a presenting appliance communication to the server 1001 allowing retrieval of the specific credential set(s) connected to the presenting interactor 1002, in storage at the
15 location identified by the presenting interactor 1002. The presenting appliance communication contains a presenter identifier retrieved in 1013 and the once-off shared keycode obtained at 1015. The presenting appliance communication may also contain an alias associated to the chosen credential set if itemized at 1013 and selected at 1016, and may also contain any predetermined auxiliary parameters if
20 captured following 1016.

[0077] At 1020, the server 1001 seeks to match the received accepting appliance communications and received presenting appliance communications by seeking to match the once-off shared keycode contained in accepting appliance communications and the once-off shared keycode contained in presenting appliance
25 communications. In some embodiments, the accepting appliance communication and/or the presenting appliance communication may be assigned a validity period 1020. If the accepting appliance communication and presenting appliance communications are not matched within the designated validity period, the interaction lapses and is deemed void rendering further processes redundant.
30 Where an interaction lapses and becomes void rendering further processes redundant, the data pertaining to the interaction (i.e. the interactor

communications) can be purged from the system, freeing up resources for the processing of further received permissions. In other embodiments, a value or predetermined auxiliary parameters may have been contained in the accepting appliance communication in 1019 and presenting appliance communication in 1018.

5 If so, the value is used in addition to shared keycode as the predetermined auxiliary parameter to seek a match of an accepting appliance communication and presenting appliance communication in 1020.

[0078] At stage 1021, and in the event a match is found at 1020, the server 1001 initiates a search by linking 1021 the presenting identifier contained in the
10 presenting appliance communication and the secret keycode contained in the accepting appliance communication, wherein the shared keycode contained in the presenting appliance communication is the same as the shared keycode contained in the accepting appliance communication as per 1020. If no match is found at 1020, the method does not thus proceed with 1021, and the server 1001 may return a
15 message accordingly to the accepting appliance 1005 or the presenting appliance 1003.

[0079] At stage 1022, the server 1001 conducts a search for a target record within its collection of presenter records comprising the presenter identifier contained in the matched presenting appliance communication and the secret
20 keycode contained in the matched accepting appliance communication. In one embodiment, and in the event 1022 an alias associated to the presenter identifier is contained in the presenting appliance communication as per 1018, the alias is also used to ascertain 1022 a target record comprising that alias in addition to the presenter identifier and secret keycode of the presenting interactor 1002.

25 [0080] At stage 1023, and in the event a record comprising the presenter identifier and presenter's secret keycode is located in 1022, a search is continued by identifying 1023 an entry affiliated to the target record located in 1022, wherein the entry pertains to the set of credentials connected to the presenting interactor 1002. (In one embodiment, the credential set concerned may be the credential set
30 connected to the alias selected by the presenting interactor 1002 at step 1022). In one embodiment, the entry identified contains a reading comprising the credentials

connected to the presenting interactor 1002. In another embodiment, the entry identified contains a pointer locating the credentials connected to the presenting interactor 1002. In the event a record comprising the presenter identifier and presenter's secret keycode is not located in step 1022, the process does not thus
5 proceed with 1023 and the server 1001 may return a message accordingly to the accepting appliance 1005 or/and the presenting appliance 1003.

[0081] At 1024, a search is completed by permitting a retrieval of a reading of the credentials connected to the presenting interactor 1002 in storage at the location identified in 1023, and permitting a release of the reading of the credentials
10 connected to the presenting interactor to the facility of the recipient permitted by the presenting interactor 1002.

[0082] At stage 1025, a reading is retrieved from storage at the location indicated by the presenting interactor 1002. In one embodiment, a reading is stored and retrieved 1025 at the controlling server configured to perform the method devised in
15 1020 to 1024. In another embodiment, a reading is stored and retrieved 1025 at another server different to the controlling server configured to perform the method devised in 1020 to 1024.

[0083] At stage 1026, a reading of the credentials is released 1026 to the facility of the recipient permitted by the presenting interactor 1002. In one embodiment, the
20 reading is released and dispatched to the network endpoint 1004. In another embodiment, the reading is released and dispatched to the accepting appliance 1005.

[0084] In Figure 10, and as the events subsequent at 1027 and 1028, a message is returned by the server 1001 to the presenting appliance 1003 for the presenting
25 interactor 1002, indicating if the reading has been retrieved as identified and released as permitted by the presenting interactor 1002; in such supplemental embodiments, a recording is retained at the server 1001 listing a status of events occurring between 1020 and 1024, ad reviewable to the presenting interactor 1002 at the presenting appliance 1003.

30 [0085] The embodiments in the invention described with reference to the drawings comprise a computer apparatus and/or processes performed in a computer

European Intellectual Property Architects

Patents, Trademarks, Designs, Copyright and Domain Name



MAMC

EUROPEAN PATENT OFFICE
P.O. Box 5818
2280 HV RIJSWIJK (ZH)
Netherlands

Diegem, February 4, 2016

Gevers ref. PAT2505161PC00 / MAMC / AAFV

International patent application No. PCT/EP2015/050354 filed on January 09, 2015
Mainline Patents Holdings Ltd

RESPONSE TO SECOND WRITTEN OPINION

Dear Sirs,

Further to the second Written Opinion issued by the International Preliminary Examining Authority (WO-IPEA) dated December 7, 2015, we enclose new pages 32 to 40 to replace pages 32 to 40 presently on file. An annotated version of the new pages is also enclosed for information.

It is noted that the Examiner indicates that the claims presently on file do not meet the clarity requirements under Article 6 PCT. New pages 32 to 40 address those issues as follows:-

1. Paragraph 1.1 of the WO-IPEA:

- 1.1. New claims 1 and 25 have been revised to ensure that the expression "connected controlled credentials" as used throughout the claims refers to the feature or expression "controlled credentials connected to the presenter".
- 1.2. The expression "said at least one set of controlled credentials connected to said presenter comprising at least one set of connected controlled credentials" has been deleted from both claims 1 and 25.
- 1.3. It is submitted that this deletion does not introduce subject-matter as it is clear that the expression "at least one set of controlled credentials connected to a presenter" is equivalent to the deleted expression, that is, there are controlled credentials which are connected to the presenter which comprise connected controlled credentials.

2. Paragraph 1.2 of the WO-IPEA:

- 2.1. New claim 1 has been revised to recite "... and a secret key code ..." at line 19 thereof in accordance with the Examiner's suggestion.
- 2.2. New claim 1 has also been revised so that step e) recites "conduct the search ..." in accordance with the Examiner's suggestion.

NV **GEVERS PATENTS SA**
Intellectual Property House
Holidaystraat, 5
B-1831 Diegem - Brussels (Belgium)

T : +32 2 715 37 11
F : +32 2 535 99 00
patents@gevers.eu
www.gevers.eu

BTW-TVA : BE 0451.659.120
RPR Brussel - RPM Bruxelles
BE87 732 0047379 94 CREGBEBB (CBC)
BE53 310 1012647 53 BBRUBEBB (ING)

BRUSSELS - PARIS - GENÈVE - ANTWERPEN - DIEGEM - GENT - HASSELT - LIÈGE - NIMHAYEL - TOULOUSE
Extract from the General Terms and Conditions - Uittreksel van de Algemene Voorwaarden als bijlage - Extraat des Conditions Générales voir verso
Full text - Volledige tekst - Texte complet : www.gevers.eu/general-terms-and-conditions

3. Paragraph 1.3 of the WO-IPEA:

- 3.1. Claim 25 has been revised so that step e) recites "conducting the search for the target record" as indicated by the Examiner.

4. Paragraph 1.4 of the WO-IPEA:

- 4.1. New claim 25 has been amended as proposed by the Examiner.
- 4.2. In particular, the expression "at a server" has been removed from each of the method steps, and, the preamble of the claim has been revised to recite "the method comprising the following steps performed at at least one server".

5. Paragraph 1.5 of the WO-IPEA:

- 5.1. New claims 18, 19, 32 and 33 have been revised to read "... said records comprise entries of at least one set of connected controlled credentials ..." to add clarity to the claims as pointed out by the Examiner.
- 5.2. These claims relate to alternatives where entries are on the controlling server (claim 18) and the entries are on a different server (claim 19). In the former case, the steps of the method are performed on the controlling server, and, in the latter case, the steps are performed on a different server.
- 5.3. Moreover, if there is only the controlling server (claim 18), the communication of the retrieved connected controlled credentials is performed by the controlling server.
- 5.4. However, if there is a different server (claim 19), the communication of the retrieved connected controlled credentials may be performed by either the controlling server or the different server.
- 5.5. Similar comments apply *mutatis mutandis* with respect to claims 32 and 33 (although claim 33 was not mentioned by the Examiner).

6. Paragraph 1.6 of the WO-IPEA:

- 6.1. New claims 18 and 19 have been revised to refer to the steps f) and g) of claim 1 and the communication is performed according to the server on which the steps are performed as discussed in paragraphs 5.2 to 5.4 above.
- 6.2. As a result, the expression "said search for at least one set of connected controlled credentials is performed at said controlling server, retrieval of said at least one set of connected controlled credentials is" has been deleted from claim 18.
- 6.3. Similarly, the expression "said search for at least one set of connected controlled credentials is performed at said controlling server, retrieval of said at least one set of connected controlled credentials" has been deleted from claim 19.
- 6.4. New claims 32 and 33 have also been revised to refer to the steps (f) and (g) of claim 25 and the communication is performed according to the server on which the steps are performed as discussed in paragraph 5.5 above.

NV **GEVERS PATENTS SA**
Intellectual Property House
Holidaystraat, 5
B-1831 Diegem - Brussels (Belgium)

T : +32 2 715 37 11
F : +32 2 535 99 00
patents@gevers.eu
www.gevers.eu

BTW-TVA : BE 0451.659.120
RPR Brussel - RPM Bruxelles
BE87 732 0047379 94 CREGBEBB (CBC)
BE53 310 1012647 53 HBRUBEBB (ING)

Page 3 of 3

6.5. As a result, the expressions "of searching for said at least one set of connected controlled credentials" and "performing the steps of retrieving said at least one set of connected controlled credentials as said different server and" have been deleted from claim 33.

7. Paragraph 1.7 of the WO-IPEA:

7.1. New claim 26 has been revised as proposed by the Examiner.

8. Paragraph 1.8 of the WO-IPEA:

8.1.1. New claims 28 and 33 have been revised to be dependent on claim 25 or 26 but with the addition of the following clarifying phrase "said at least one server comprises a controlling server ... and ...".

8.1.2. It is submitted that this revision removes the contradiction with claim 27.

9. Other points

9.1. The term "designated" in claim 1, step (g) has been replaced with the term "permitted" to be consistent with claim 25 and the description as filed where it is stated that the network endpoints are permitted recipients rather than designated recipients of the connected controlled credential (see, for example, paragraphs [0008], [0020] and [0027]).

9.2. Other amendments have been made to the terminology in the dependent claims for consistency with the terminology used in the independent claims from which they depend.

9.3. Reference numerals have been corrected in some of the dependent claims.

9.4. Claim 34 presently on file has been deleted as it is essentially the same as new claim 33. New claims 34 to 36 correspond to respective ones of claims 35 to 37 presently on file.

9.5. Claim dependencies have been changed for consistency with the disclosure of the application.

It is therefore submitted that the objections under Article 6 PCT have been resolved and that a positive International Preliminary Report on Patentability under Chapter II should be issued in due course.

Yours faithfully,



Margaret MACKETT

Enclosures: New pages 32 to 40 together with an annotated version thereof.

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:
- 5 at least one network endpoint;
- at least one accepting appliance (109) configured to send an accepting appliance communication (104), said accepting appliance communication containing a secret keycode (109a) pertaining to said presenter and a once-off shared keycode (109b);
- 10 at least one presenting appliance (108) configured to send a presenting appliance communication (105), said presenting appliance communication containing a presenter identifier (108a) pertaining to said presenter and said once-off shared keycode (108b);
- 15 at least one server that further comprises a processor, at least one communications interface and 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 comprises a presenter identifier and a secret keycode bound to the presenter identifier;
- 20 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);
 - 25 d) initiate a search for a target record by linking said secret keycode in said accepting appliance communication (104) with said presenter identifier 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) conduct the search for said target record that comprises both said secret keycode (109a) and said presenter identifier (108a);

5 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
10 connected controlled credentials.

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

15 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
20 configured to generate said once-off shared keycode, receive said secret keycode (109a) from said presenter and transmit said accepting appliance communication to said controlling server (101).

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

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

5

7. The system of any one of the preceding claims, wherein said presenting appliance communication further contains an alias associated to said 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
10 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 presenter identifier (108a) and said secret keycode.

8. The system of any one of the preceding claims, wherein said network
15 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 controlled credentials.

9. The system of any one of claims 1 to 7, wherein said network endpoint
20 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.

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

11. The system of claim 2, wherein said at least one set of connected controlled credentials comprises an entry on another of said at least one server which is affiliated to said target record on said controlling server (101).

12. The system of any one of the preceding claims, 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.

5

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.

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

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

16. The system of any one of the preceding claims, wherein said accepting appliance communication (104) further contains one or more predetermined auxiliary parameters, and said presenting appliance communication also further
20 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
25 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 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
5 is performed from said controlling server.

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
10 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 different server.

20. The system of any one of claims 2 to 5, wherein, if no match between
15 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 such status thereat.

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

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

23. The system of any one of the preceding claims, wherein each of said servers, network endpoints (110), and presenting and accepting appliances (108,

109) each further comprises at least one of: a processor, communication interfaces, memory, input consoles and output consoles.

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

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 at at
10 least one server:

- (a) receiving an accepting appliance communication (104), said communication containing a secret keycode (109a) pertaining to said presenter and a once-off shared keycode (109b);
- (b) receiving a presenting appliance communication (105), said
15 communication containing a presenter identifier (108a) pertaining to said presenter and once-off shared keycode (108b);
- (c) seeking 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);
- 20 (d) initiating a search for a target record by linking said secret keycode (109a) of said accepting appliance communication (104) and said presenter identifier (108a) 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);
- 25 (e) conducting the search for the target record comprising both said secret keycode (109a) and said presenter identifier (108a);
- (f) identifying an entry (103) affiliated with said target record, said entry pertaining to said at least one set of connected controlled credentials; and

(g) permitting 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
5 credentials.

26. The method of claim 25, wherein the target record comprising said presenter identifier (108a) and secret keycode (109a) further comprises an alias associated to said presenter identifier (108a) and affiliated to said entry (103)
10 pertaining to said at least one set of connected controlled credentials, and said presenting appliance communication (105) further contains an alias associated to said 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
15 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.

20 28. The method of claim 25 or 26, wherein said at least one server comprises a controlling server (101) and said at least one set of connected controlled credentials comprises an entry on a 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
25 steps (e) to (g) are performed at one of: said controlling server (101) and a different server.

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
30 (104), said presenting appliance communication (105) and said once-off shared

keycode, and step (c) further comprises establishing whether said validity period has expired.

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

31. The method of any one of claims 25 to 29, wherein each of said
presenting appliance communication (105) and said accepting appliance
communication (104) further contains one or more predetermined auxiliary
10 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
parameters in said accepting appliance communication.

15 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
method further comprises releasing said at least one set of connected controlled
credentials from said controlling server.

20

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
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
25 method further comprises releasing said at least one set of connected controlled
credentials from one of: said controlling server and said different server.

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 such status at said controlling server (101).

35. The method of claims 27 or 28, wherein, if no target record is found,
5 terminating further configured actions and recording such status at said controlling server (101).

36. The method of claim 27 or 28, further comprising recording the status of the events at said controlling server (101) and relaying such status to at least
10 one of: said accepting appliance (109) and said presenting appliance (108).

REIVINDICACIONES MODIFICADAS
PARA REALIZAR EL EXAMEN DE
PATENTABILIDAD

REIVINDICACIONES

1. Un sistema (100) para permitir una comunicación de al menos un grupo de credenciales controladas conectadas a un presentador desde un servidor a
5 un punto final de red, dicho sistema caracterizado porque comprende:

al menos un punto final de red;

al menos un aparato de aceptación (109) configurado para enviar una comunicación de aparato de
10 aceptación (104), dicha comunicación de aparato de aceptación contiene un código clave secreto (109a) que pertenece a dicho presentador y un código clave compartido una vez apagado (109b);

al menos un aparato de presentación (108)
15 configurado para enviar una comunicación de aparato de presentación (105), dicha comunicación de aparato de presentación contiene un identificador de presentador (108a) que pertenece a dicho presentador y dicho código clave compartido una vez apagado (108b);

20 al menos un servidor que además comprende un procesador, al menos una interfaz de comunicaciones y memoria que almacena al menos una entrada (103) que pertenece a dicho al menos un grupo de credenciales controladas conectadas, cada entrada está afiliada al menos
25 a un registro (102), el registro que pertenece a cualquier

presentador y comprende un identificador de presentador y un código clave secreto unido al identificador de presentador;

5 en donde dicho al menos un servidor está configurado para:

 a) recibir dicha comunicación de aparato de aceptación (104);

 b) recibir dicha comunicación de aparato de presentación (105);

10 c) buscar una coincidencia de dicho código clave compartido una vez apagado (109b) contenido en dicha comunicación de aparato de aceptación (104) con dicho código clave compartido una vez apagado (108b) contenido en dicha comunicación de aparato de presentación (105);

15 d) iniciar una búsqueda de un registro objetivo al conectar dicho código clave secreto en dicha comunicación de aparato de aceptación (104) con dicho identificador de presentador en dicha comunicación de aparato de presentación (105), ambas de dicha comunicación
20 de aparato de aceptación y dicha comunicación de aparato de presentación contienen el mismo código clave compartido una vez apagado (108b, 109b);

 e) conducir la búsqueda de dicho registro objetivo que comprende ambos de dicho código secreto (109a)
25 y dicho identificador de presentador (108a);

f) identificar una entrada (103) afiliada con dicho registro objetivo;

g) permitir la recuperación de dicho al menos un grupo de credenciales controladas conectadas que pertenecen a dicha entrada (103) y permiten la liberación de dicho al menos un grupo de credenciales controladas conectadas a dicho punto final de red (110), dicho punto final de red es un receptor permitido de un tipo de dicho al menos un grupo de credenciales controladas conectadas.

10 2. El sistema de conformidad con la reivindicación 1, caracterizado porque dicho al menos un servidor comprende un servidor de control (101).

15 3. El sistema de conformidad con la reivindicación 2, caracterizado porque el servidor de control (101) además está configurado para generar dicho código clave compartido una vez apagado, y hacerlo disponible en el aparato de aceptación (109).

20 4. El sistema de conformidad con la reivindicación 2, caracterizado porque dicho para toda la aceptación además está configurado para generar dicho código clave compartido una vez apagado, recibir dicho código clave secreto (109a) de dicho presentador y transmitir dicha comunicación de aparato de aceptación a dicho servidor de control (101).

25 5. El sistema de conformidad con la

reivindicación 3, caracterizado porque dicho aparato de presentación además está configurado para recibir dicho código clave compartido una vez apagado de dicho aparato de aceptación (109), recuperar dicho identificador de presentador de su memoria y transmitir dicha comunicación de aparato de presentación (105) a dicho servidor de control (101).

6. El sistema de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque dicho registro comprende dicho identificador de presentador y dicho código clave secreto además comprende un alias asociado con el identificador de presentador y afiliado con dicha entrada (103) que pertenece a dicho al menos un grupo de credenciales controladas conectadas.

7. El sistema de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque dicha comunicación de aparato de presentación además contiene un alias asociado con dicho identificador de presentador y afiliado con dicha entrada (103) que pertenecen a dicho al menos un grupo de credenciales controladas conectadas, en donde dicha búsqueda de dicho registro objetivo además utiliza dicho alias contenido en dicha comunicación de aparato de presentación (105) para buscar dicho registro objetivo que comprende dicho alias además de comprender dicho identificador de presentador

(108a) y dicho código clave secreto.

8. El sistema de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque dicho punto final de red comprende dicho aparato de
5 aceptación (109) y está configurado como un receptor designado de uno o más tipos de dicho al menos un grupo de credenciales controladas conectadas.

9. El sistema de conformidad con cualquiera de las reivindicaciones 1 a 7, caracterizado porque dicho
10 punto final de red está conectado a dicho aparato de aceptación y está configurado como un receptor designado de uno o más tipos de dicho al menos un grupo de credenciales controladas conectadas.

10. El sistema de conformidad con la
15 reivindicación 2, caracterizado porque dicho al menos un grupo de credenciales controladas conectadas comprende una entrada en dicho registro objetivo (102) en dicho servidor de control (101).

11. El sistema de conformidad con la
20 reivindicación 2, caracterizado porque el por lo menos un grupo de credenciales contraladas conectadas comprende una entrada en otro de dicho al menos un servidor que está afiliado a dicho registro objetivo en dicho servidor de control (101).

25 12. El sistema de conformidad con cualquiera de

las reivindicaciones precedentes, caracterizado porque un periodo de validez es asignado a dicha comunicación de aparato de aceptación (104), y en donde el paso c) además comprende establecer si ha expirado dicho periodo de validez.

13. El sistema de conformidad con cualquiera de las reivindicaciones 1 a 11, caracterizado porque se asigna un periodo de validez a dicha comunicación de aparato de presentación (105), y en donde el paso c) además comprende establecer si ha expirado dicho periodo de validez.

14. El sistema de conformidad con cualquiera de las reivindicaciones 1 a 11, caracterizado porque se asigna un periodo de validez a dicho código clave compartido una vez apagado, y en donde el paso c) además comprende establecer si el periodo de validez ha expirado.

15. El sistema de conformidad con la reivindicación 14, caracterizado porque dicho código clave compartido una vez apagado es único por la duración de su periodo de validez.

20 16. El sistema de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque dicha comunicación de aparato de aceptación (104) además contiene uno o más parámetros auxiliares predeterminados y dicha comunicación de aparato de presentación además también comprende dicho uno o más parámetros auxiliares

predeterminados.

17. El sistema de conformidad con la reivindicación 16, cuando depende de cualquiera de las reivindicaciones 2 a 5, caracterizado porque dicho servidor de control (101) busca coincidir con al menos uno de dichos parámetros auxiliares predeterminados de dicha comunicación aparato de presentación (105) con dicho(s) parámetro(s) auxiliar predeterminado(s) correspondiente(s) de dicha comunicación de aparato de aceptación (104) para proporcionar además al menos uno de: correlación y corroboración.

18. El sistema de conformidad con cualquiera de las reivindicaciones 2 a 5, caracterizado porque, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas conectadas en dicho servidor de control (101), se realizan los pasos f) y g) en dicho servidor de control, y la comunicación de dicho al menos un grupo de credenciales controladas conectadas se realiza a partir de dicho servidor de control.

19. El sistema de conformidad con cualquiera de las reivindicaciones 2 a 5, caracterizado porque, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas conectadas en un servidor diferente a dicho servidor de control, los pasos f) y g) se realizan en dicho servidor diferente, y la comunicación de

dicho al menos un grupo de credenciales controladas conectadas se realiza utilizando uno de: dicho servidor de control y dicho servidor diferente.

20. El sistema de conformidad con cualquiera de
5 las reivindicaciones 2 a 5, caracterizado porque, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y comunicación de aparato de presentación (105) en dicho servidor de control (101), dicho servidor de control termina acciones y registros
10 configurados adicionales de tal estado ahí.

21. El sistema de conformidad con cualquiera de las reivindicaciones 2 a 5, caracterizado porque, sino se encuentra ningún registro objetivo en dicho servidor de control (101), dicho servidor de control termina acciones y
15 registros configurados adicionales de tal estado ahí.

22. El sistema de conformidad con cualquiera de las reivindicaciones 2 a 5, caracterizado porque dicho servidor de control (101) además está configurado para registrar el estado de los eventos que ocurren y para
20 transmitir tal estado al menos a uno de: dicho aparato de aceptación (109) y dicho aparato de presentación (108).

23. El sistema de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque cada uno de dichos servidores, puntos finales de red (110), y
25 cada uno de los aparatos de presentación y de aceptación

(108, 109) además comprende al menos uno de: un procesador, interfaces de comunicación, memoria, consolas de entrada y consolas de salida.

24. El sistema de conformidad con cualquiera de
5 las reivindicaciones precedentes, caracterizado porque el sistema es operable por una red de comunicaciones (106, 107, 111).

25. Un método para permitir una comunicación de al menos un grupo de credenciales controladas conectadas a
10 un presentador de al menos un servidor a un punto final de red (110), dicho método comprende los siguientes pasos realizados en al menos un servidor:

(a) recibir una comunicación de aparato de aceptación (104), dicha comunicación contiene un código
15 clave secreto (109a) que pertenece a dicho presentador y un código clave compartido una vez apagado (109b);

(b) recibir una comunicación de aparato de presentación (105), dicha comunicación contiene un
identificador de presentador (108a) que pertenece a dicho
20 presentador y código clave compartido una vez apagado (108b);

(c) buscar una coincidencia de dicho código clave compartido una vez apagado (109b) contenido en dicha
comunicación de aparato de aceptación (104) y dicho código
25 clave compartido una vez apagado (108b) contenido en dicho

comunicado de aparato de presentación (105);

(d) iniciar una búsqueda de un registro objetivo al conectar dicho código clave secreto (109a) de dicha comunicación de aparato de aceptación (104) y dicho
5 identificador de presentador (108a) en dicha comunicación de aparato de presentación (105), ambas de dicha comunicación de aparato de aceptación y dicha comunicación de aparato de presentación contienen el mismo código clave compartido una vez apagado (108b, 109b);

10 (e) conducir la búsqueda del registro objetivo que comprende tanto dicho código clave secreto (109a) y dicho identificador de presentador (108a);

(f) identificar una entrada (103) afiliada con dicho registro de control, dicha entrada que pertenece a
15 dicho al menos un grupo de credenciales controladas conectadas; y

(g) permitir una recuperación de dicho al menos un grupo de credenciales controladas conectadas que pertenecen a dicha entrada y que permiten una liberación de
20 dicho grupo de credenciales controladas conectadas a dicho punto final de red (110), dicho punto final es un receptor permitido de dicho al menos un grupo de credenciales controladas conectadas.

26. El método de conformidad con la
25 reivindicación 25, caracterizado porque el registro

objetivo que comprende dicho identificador de presentador (108a) y código clave secreto (109a) además comprende un alias asociado con dicho identificador de presentador (108a) y afiliado con dicha entrada (103) que pertenece a
5 dicho al menos un grupo de credenciales controladas conectadas, y dicha comunicación de aparato de presentación (105) además contiene un alias asociado con dicho identificador de presentador (108a) y afiliado con dicha entrada que pertenece a dicho al menos un grupo de
10 credenciales controladas conectadas, y en donde el paso (e) además comprende hacer coincidir alias respectivos de dicho registro y dicha comunicación de aparato de presentación.

27. El método de conformidad con la reivindicación 25 ó 26, caracterizado porque dicho al menos
15 un servidor comprende un servidor de control (101) y los pasos (a) a (g) se realizan ahí.

28. El método de conformidad con la reivindicación 25 ó 26, caracterizado porque al menos un servidor comprende un servidor de control (101) y dicho al
20 menos un grupo de credenciales controladas conectadas comprende una entrada en un servidor diferente a dicho servidor de control (101), dicha entrada está afiliada con dicho registro objetivo, y en donde el paso de identificar un grupo de credenciales se realiza en dicho servidor
25 diferente, y en donde los pasos (e) a (g) se realizan en

uno de: dicho servidor de control (101) y un servidor diferente.

29. El método de conformidad con cualquiera de las reivindicaciones 25 a 28, caracterizado porque además
5 comprende asignar un periodo de validez al menos a uno de: dicha comunicación aparato de aceptación (104), dicha comunicación de aparato de presentación (105) y dicho código clave compartido una vez apagado, y (c) además comprende establecer si ha expirado dicho periodo de
10 validez.

30. El método de conformidad con la reivindicación 29, caracterizado porque dicho código clave compartido una vez apagado es único por la duración de su periodo de validez.

31. El método de conformidad con cualquiera de las reivindicaciones 25 a 29, caracterizado porque cada una de dicha comunicación de aparato de presentación (105) y dicha comunicación de aparato de aceptación (104) además contiene uno o más parámetros auxiliares predeterminados, y
15 en donde el paso (c) además comprende buscar una coincidencia de al menos uno de dichos parámetros auxiliares predeterminados en dicha comunicación de aparato de presentación con al menos uno de parámetros auxiliares predeterminados correspondientes en dicha comunicación de
20 aparato de aceptación.

32. El método de conformidad con la reivindicación 27, caracterizado porque dichos registros comprenden entradas de al menos un grupo de credenciales controladas conectadas en dicho servidor de control (101),
5 que realiza los pasos (f) y (g) en dicho servidor de control, y el método además comprende liberar dicho al menos un grupo de credenciales controladas conectadas de dicho servidor de control.

33. El método de conformidad con la reivindicación 25 ó 26, caracterizado porque dicho al menos un servidor comprende un servidor de control (101), y, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas conectadas en un servidor diferente a dicho servidor de control (101), realizar los
10 pasos (f) y (g) en dicho servidor diferente, y el método además comprende liberar dicho al menos un grupo de credenciales controladas conectadas de uno de: dicho servidor de control y dicho servidor diferente.

34. El método de conformidad con la reivindicación 27 ó 28, caracterizado porque, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y comunicación de aparato de presentación (105), terminar acciones y registros configurados adicionales de tal estado en dicho servidor de
20 control (101).
25

35. El método de conformidad con la reivindicación 27 ó 28, caracterizado porque, si no se encuentra ningún registro objetivo, terminar acciones y registro configurados adicionales de tal estado en dicho servidor de control (101).

36. El método de conformidad con la reivindicación 27 ó 28, caracterizado porque además comprende registrar el estado de los eventos en dicho servidor de control (101) y confiar tal estado al menos a uno de: dicho aparato de aceptación (109) y dicho aparato de presentación (108).