PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2019/083943	06.12.2019	06.12.2018

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/08 H04L9/30 H04L9/32

Applicant
SECURE-IC SAS

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ 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 Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and 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

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Yamajako-Anzala, A Telephone No. +49 89 2399-0

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/EP2019/083943

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ 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 (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-12
	No:	Claims	13, 14
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-14
Industrial applicability (IA)	Yes:	Claims	1-14
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

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 SATTAM S AL-RIYAMI ET AL: "Certificateless Public Key Cryptography", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20031021:122149, 21 October 2003 (2003-10-21), pages 1-40, XP061000641,

D2 WO 2013/116928 A1 (CONNECT IN PRIVATE CORP [PA] ET AL.) 15 August 2013 (2013-08-15)cited in the application

2 The present application does not meet the criteria of Art. 33(1) PCT, because the subject-matter of **claim 13**, as far as it was understood (see item 9 below) is not novel in the sense of Art. 33(2) PCT.

2.1 document **D2** discloses (the references in parentheses applying to this document):

An identity-based cryptosystem comprising a trusted center, said trusted center being configured to determine system parameters and a master private key from a trusted center security parameter and a trusted center identifier, said system parameters comprising a prime number, two algebraic groups of order equal to said prime number, an admissible bilinear map, a first cryptographic hash function, a second cryptographic hash function, a third cryptographic hash function, and a trusted center public key associated with said trusted center identifier, said trusted center being configured to:
- generate said prime number, said two algebraic groups and said admissible bilinear map by running a Bilinear Diffie-Hellman parameter generator that takes as input said trusted center security parameter;
- select a first cryptographic hash function, a second cryptographic hash function, and a third cryptographic hash function from a predefined set of cryptographic hash functions;
- determine a first value by applying the first cryptographic hash function to said trusted center identifier;
- randomly select a master secret key; and

- determine said trusted center public key by applying an exponentiation function defined by a base and an exponent, said base being equal to said first value, and said exponent being equal to said master private key. (see algorithm Setup in **paragraph 40**)

2.2 As a consequence, **claim 13** is not novel (Art. 33(2) PCT).

3 Moreover, it should be noted that the subject-matter of independent **claim 13** is also not novel in the sense of Art. 33(2) PCT against the teachings of document **D1** (see cited passages in the Search Report).

4 The present application does not meet the requirements of Art. 33(1) PCT since the subject-matter of independent **claim 1**, as far as it was understood (see item 9 below), does not involve an inventive step in the sense of Art. 33(3) PCT.

4.1 Document **D1**, which is considered to represent the closest prior art, discloses (the references in parentheses applying to this document) :

A transmitter device for sending an encrypted message to a receiver device in an identity-based cryptosystem, the transmitter device being associated with a transmitter identifier (**page 5, lines 13,14**: "An entity B can encrypt a message for A using [...] an identifier ID_A..."), wherein the transmitter device is configured to receive a transmitter partial private key from a trusted center (**page 13, lines 5-7**: "Partial-Private-Key-Extract: This algorithm takes as input an identifier ID_A [...],and carries out [...] steps to construct the partial private key for entity A with identifier ID_A..."), the transmitter device being configured to:

- send a request for two public session keys to the receiver device (**page 3, lines 17,18**: "Entity A's public key might be made available to other entities..."; **page 13, lines 18,19**: "Set-Public-Key: This algorithm takes params and entity A's secret value [...] as inputs and constructs A's public key as $P_A = <X_A, Y_A>$");
- receive from the receiver device ~~a first ciphertext set, said first ciphertext set being derived from an encryption and authentication of~~ two public session keys (**page 3, lines 17,18**: "Entity A's public key might be made available to other entities...");
- ~~decrypt and authenticate the two public session keys from the first ciphertext set using a receiver identifier and the transmitter partial private key~~;
- determine a second ciphertext set from the transmitter partial private key, from the receiver identifier, and from the two public session keys, said second ciphertext comprising an encrypted message (**page 14, line 34 - page 15, line 4**: "Encrypt: To encrypt M [...] for entity A with identifier ID_A [...] and public key $P_A = <X_A, Y_A>$ [...] Compute and output the ciphertext: $C = <rP, \sigma \oplus H_2(e(Q_A,$

$Y_A)^r$),M⊕H4(σ)>...");
- send said second ciphertext set to the receiver device (It has to be noted that this step is implicitly disclosed).

4.2 The difference between the subject-matter of **claim 1** and that of document **D1** resides in that the two public session keys are received from the receiver device as a first ciphertext set and in that the transmitter decrypts and authenticates the two public session keys from the first ciphertext set using a receiver identifier and the transmitter partial private key.

4.3 This difference has the technical effect of protecting the distribution of keys from tampering.

4.4 The objective technical problem to be solved may therefore be regarded as how to protect the distribution of public keys when the trusted center is partially trusted.

4.5 Document **D1** discloses a certificateless public key encryption system secure only if the trusted center does not collude with an attacker which is an obvious disadvantage to the person skilled in the art. Based on this hint and faced with the above technical problem the skilled person would be prompted to look for solutions to securely distribute the public keys while reducing the trust put in the trusted center and would come across document **D2** which discloses a secure certificateless public key encryption system where the trust is established from the public identity of the server and not fixed parameters that could be altered (see **paragraph 15** in document **D2**). The skilled person would use such a scheme to distribute the public keys encrypted and authenticated in the case the generation center is not fully trusted. Thereby, the skilled person would combine the teachings of **D1** and these of **D2** and would arrive at the subject-matter of **claim 1** in an obvious manner in order to solve the objective technical problem stated above.

4.6 As a consequence, **claim 1** is not allowable under Art. 33(1) PCT for lack of inventive step of its subject-matter.

5 Referring to the objection raised above, **claim 6** also does not involve an inventive step in the sense of Art. 33(3) PCT since its subject-matter corresponds to that of **claim 1**.

6 The dependent claims do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to novelty (Art. 33(2) PCT) and inventive step (Art. 33(3) PCT). In particular :

6.1 The additional features of **claims 2, 4, 5, 7-10, 12** are disclosed in document **D1** (see cited passages in Search Report).

6.2 The additional features of **claims 3, 11** are disclosed in document **D2** (see cited passages in Search Report).

6.3 The additional features of **claim 14** are disclosed in document **D1** or **D2** each document taken alone (see cited passages in Search Report).

Re Item VII

Certain defects in the international application

7 The cited prior art is not acknowledged in the description (Rule 5.1(a)(ii) PCT).

8 The claims do not include reference numerals relating to the technical features referred to therein, Rule 6.2 (b) PCT.

Re Item VIII

Certain observations on the international application

9 The present application lacks clarity in the sense of Art. 6 PCT.

9.1 **Claim 1** is directed towards an apparatus. It is noted that the wording of the claim uses expressions such as "for ". According to the PCT International Search and Preliminary Examination Guidelines, 5.23, such formulations are not limiting the scope of protection of the claim. In order to overcome the objection it is therefore suggested to redraft **claim 1** by replacing, where appropriate, "for" by "adapted to".

9.2 A similar objection as the one made above applies to **claim 6**.

9.3 The expressions "identifier,," and "byrunning" in **claim 13** appear to contain a typographic error and therefore renders the precise scope of protection unclear.

9.4 The expression "wherein-said" in **claim 7** appears to contain a typographic error and therefore renders the precise scope of protection unclear.

9.5 The expressions "apply a decipher to the third ciphertext [...] said decipher using said secret key as a decryption key", "apply said decipher to the fourth ciphertext" in **claim 3** is grammatically incorrect as decipher is a verb and not a noun and therefore renders the precise scope of protection unclear. It is

suggested to replace the first expression by "decipher the third ciphertext [...] using said secret key as a decryption key" and the second expression by "decipher the fourth ciphertext"

9.6 A similar objection as the one made above applies to **claim 12**.

9.7 Any general statements aiming at extending the scope of protection but not supported by a precise description (the last paragraph in the description is an example of such statements) should be removed.