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/GB2018/052458	30.08.2018	05.09.2017

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/34 G06F21/60 G06F21/44 H04L29/06

Applicant
ISTORAGE LIMITED

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:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0
Fax: +49 89 2399 - 4465

Date of completion of this opinion
see form PCT/ISA/210

Authorized Officer
Widera, Sabine
Telephone No. +49 89 2399-0

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/GB2018/052458

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	7, 15, 16
	No:	Claims	1-6, 8-14, 17
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-17
Industrial applicability (IA)	Yes:	Claims	1-17
	No:	Claims	

2. Citations and explanations

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 document:

D1 US 2008/126802 A1 (LI XIZHE [CN] ET AL) 29 May 2008 (2008-05-29)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claim 1 is not new.

D1 discloses:

A method of securely transferring master keying material between a master dongle and a slave dongle,wherein the slave dongle contains a public key and a private key,wherein the master dongle contains master keying material, and wherein the master keying material is for allowing users of the dongles to securely access encrypted data;the method comprising: *(par. [0008-11] dongle is a "hardware security unit" and master keying material is "hardware security unit information")*
connecting the master dongle and the slave dongle to a data transfer system; *(par. [0027] " The trusted computing systems to be bound are connected through communication interfaces such as serial ports, General-Purpose Input Output interface (GPIO), Universal Serial Bus (USB), infrared and wireless and the like")*
transferring the slave dongle's public key to the master dongle via the data transfer system; using the slave dongle's public key at the master dongle to encrypt the master keying material and hence produce encrypted master keying material at the master dongle; transferring the encrypted master keying material to the slave dongle via the data transfer system; *(par. [0031] and claim 2 "encrypted pipe" private-public key is used for exchange)*
decrypting the encrypted master keying material with the slave dongle's private key at the slave dongle; and *(par. [0031] "can only be decrypted by the private key corresponding to the public key...")*
storing the master keying material at the slave dongle; *(par. [0013] step 14)*

such that a user of any of the dongles can use the master keying material to decrypt data encrypted by the same dongle or the other of the dongles. *(par. [0013] and [0030] step 14)*

3 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 8, 9, 14 and 17 which therefore are also considered not new.

4 Dependent claims 2-7, 10-13, 15 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see citations in the search report.