(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 May 2014 (22.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/077698 A1

(51) International Patent Classification:
G06F 21/30 (2013.01) *H04L 9/32* (2006.01)
G06F 21/64 (2013.01)

(21) International Application Number:
PCT/NO2013/050198

(22) International Filing Date:
15 November 2013 (15.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20121349 15 November 2012 (15.11.2012) NO

(71) Applicant: **MAESTRO SOFT AS** [NO/NO]; Karenslyst allé 8B, P.O. Box 403 Skøyen, N-0213 Oslo (NO).

(72) Inventor; and
(71) Applicant : **SVENDSEN, Liana Gyulzadyan** [NO/NO]; c/o Maestro Soft AS, Karenslyst allé 8b, P.O. Box 403 Skøyen, N-0213 Oslo (NO).

(74) Agent: **ACAPO AS**; P.O. Box 1880 Nordnes, N-5817 Bergen (NO).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

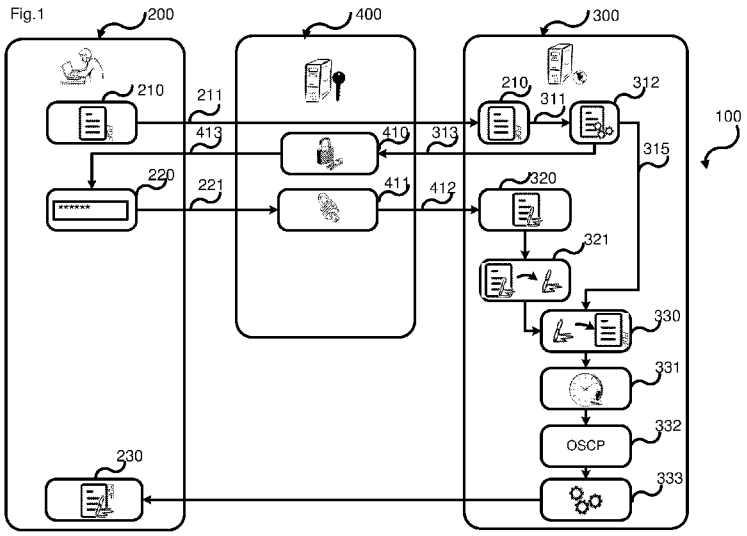
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: SIGNATURE PORTING

Fig.1



(57) **Abstract**: A method for digital signing of documents is provided. This is provided by a signature porting system which extracts signature from a signed document and ports the extracted signature to a prepared document. This enables multi signing of a document.

WO 2014/077698 A1

SIGNATURE PORTING

Background of the Invention

Technical Field

The invention relates to digital signing in general and more specifically a system and a method for digital signing of documents with electronic identification systems.

Background Art

The following abbreviations of the art will be used:

PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
CMS	Cryptographic Message Syntax
ETSI	European Telecommunications Standards institute
CAdES-BES	CMS Advanced Electronic Signatures - Basic Electronic Signature
SEID	Joint project on eID and electronic signature (from Norwegian «Samarbeidsprosjekt om eID og eSignatur»).
SDO	Signed Data object
XML	Extensible Markup Language
PDF	Portable Data Format
PAdES	PDF Advanced Electronic Signature
LTV	Long term validation
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
TSA	Time Stamping Authority
CSP	Cryptographic Service Provider
TTP	Trusted Third Party
e-ID	Electronic Identity

Existing providers of PKI have their own PKI solutions wherein a digital signature can be returned in different signature packaging formats. For instance it can be a CMS signature based on PKCS#7, CMS signature based on ETSI CAdES-BES, XML signature formatted in SEID SDO (http://www.npt.no/ikbViewer/Content/44963/SEID_Leveranse_3_v1.0.pdf) or Adobe PDF signature. In order to read information regarding signature and view the specific documents that is signed some of these formats require a proprietary reading tool. It

is therefore desired to support signing in the Adobe PDF format which is a commonly available format today where both signature and document can be shown in Adobe PDF Viewer, which is commonly available, also world wide. In 2009 ETSI developed profiles for PAdES documents, meeting requirements from the European directive 1999/93/EC (European Directive on A Community Framework for Digital Signatures).

The physical location of the private key itself and the certificate can also form part of the requirements such as the certificate and the private key having to be physically with the user. In this respect it should be referred BankID wherein the certificate and the private key is in fact not with the user but instead with the bank. Other solutions such as Buypass provide the certificate in the chip that the user holds.

From the known art one should refer to the following technologies:

Cryptographic Service Providers
http://msdn.microsoft.com/en-us/library/aa380245.aspx
Using this technology one can achieve desired functionality. However the weakness is the need to install third party software at the user or configuration of existing framework. This is not a viable since there is for instance no guarantee that the solution will have sufficient privileges to modify the configuration locally at the user. At the same time there can be limitations relating to the fact that not all implementations of the client software support lookup in public registers for verification of user certificates.

Digital Signing Using PKI
This solution provides the possibility of digital signing with PKI, nevertheless this comes with several problems attached such as PKI service providers having different implementations of the infrastructure. This results in difficulties in obtaining desired end result in the desired format as well as limitations in multi signing of the same document with different electronic identities (e-ID).

From prior art one should also refer to the Masters Degree thesis titled "*Advanced Electronic Signature*" by Azizi, Fazel Ahmad, published June 2011, Norwegian University of Science and Technology, Department of Telematics. This regards electronic signature with proxy-signature. A method is disclosed where one signs on behalf of a user with other keys that are calculated based on the user's keys. Since the solution discloses a signature creation system signing using a trusted copy or

derived key of the user's private key the solution acts as a trusted third party and entrusted with keys (key ring). The documents discloses different methods for transmitting private or calculated keys to a key holder (key ring) but does not disclose a porting of the signature after having been applied in the signature creation system.

There is therefore a need for a solution that overcomes the above problems.

Disclosure of the Invention

A main objective of the invention is to provide a solution where one arrives at a system and a method for digital signing of documents with electronic identification systems. It is also an objective to arrive at a system and a method for providing a PAdES signature having basis in a CMS, SDO, XML based signature. Furthermore it is an objective to enable a plurality of signatories with different PKI solutions on signing the same document.

Problems to be Solved by the Invention

Therefore, a main objective of the present invention is to provide a method for making a system where one can sign a PDF document in a proprietary signature format supported by a given PKI vendor yet still be able to extract the signature at a later point in time and create a valid PAdES compatible signature. Original signature can be CMS, SDO or XML-based, and in order to view both data having been signed and information on who has signed and other information on signatory is it in some cases necessary to use online services or external viewing application that is not widespread. For this reason it has been a desire to be able to generate a PAdES-document in order to be able to display the signed document and details about the signatories in Adobe Viewer. The problem was that the PKI vendors either did not support signatures in PDF-file or they supported only a limited profile of PDF signature making it impossible to use their PDF signing services. There has also been a desire to be able to multi sign a PDF file with a plurality of signatories where these can use several different PKI solutions. This was impossible since the different PKI solutions returned signatures in different file formats.

For some PKI solutions the user possesses his private key and certificate while in the other PKI solutions both private key and the certificate are stored with an

approved trusted third party (TTP). This has caused problems since normal process for storage of digital signature requires that the signatory has access to his private key and signature. It is therefore impossible for the user to use CSP (Cryptographic Service Provider) to sign the document in the format he desires. Instead the document or a has of the content of the document is transmitted to the PKI vendor who, using several security factors, acquires the user's private key and create a signature over the content (as well as signature over a few other parameters). When the signature over the document is created it is based on a hash of the contents of the PDF file. This means that including signature fields into the original PDF file will change the later hash of the file and make the signature not valid.

Means for Solving the Problems

The objective is achieved according to the invention by a method for digital signing of documents as defined in the preamble of claim 1, having the features of the characterising portion of claim 1.

The objective is achieved according to the invention by a method for digital multi signing of documents as defined in the preamble of claim 3, having the features of the characterising portion of claim 3.

A number of non-exhaustive embodiments, variants or alternatives of the invention are defined by the dependent claims.

The present invention attains the above-described objective by a system for signature porting that extracts signature from a signed document and ports the extracted signature for a prepared document.

Effects of the Invention

The technical differences over existing PKI solutions is that the present invention provides signing of documents such as PDF documents using extraction of received signature from signing from PKI and porting of said signature in order to sign the document in desired format.

The technical differences over the above Master Degree thesis is that in the present invention the user signs using the users' or signatory's own key.

These effects provide in turn several further advantageous effects:

it makes it possible to sign a PDF document in desired PAdES or other PDF signature format, even if the PKI vendor does not directly support this, and

multi signing of a PDF document with signatories that each can use different PKI solutions.

The invention provides a method where one has found a method wherein one by sending extra data together with the PDF document is able to retrieve signature based on a hash of the PDF document with signing fields that are signed later.

If the main certificate chain is available either by OCSP lookup or by physically accessible root certificates one can also construct a valid LTV signature. At the same time a time stamp is added from Time Stamping Authority.

The method also solves the problem of multiple signatures since by sending the PDF document to the different PKI solutions in sequence provides a PDF document with several signatures.

Brief Description of the Drawings

The invention will be further described below in connection with exemplary embodiments which are schematically shown in the drawings, wherein:

Fig. 1 shows the information flow in a signature system based on the solution.

Fig. 2 shows an example of multi signing of a document by 2 users with 2 different PKI solutions.

Fig. 3 shows schematically the structure of a signed PDF document.

Description of the Reference Signs

The following reference numbers and signs refer to the drawings:

100	Signature system
200	User
210	Original PDF document
211	Uploading of original PDF document to Signature porting system
220	Smartcard, OTP generator, pin codes or password.
221	The user authenticates himself with password, pin codes, etc.
230	Digitally signed PAdES PDF document

300	Signature porting system
311	Prepare PDF document and ready it for PKI signing
312	Prepared document.
313	Send request for signing to PKI.
315	Send prepared document for completion of signature.
320	Digital signature in for instance SDO, CMS, PKS#7, XML or other formats
321	Extract signature from received signed document.
330	Port the signature to the PDF document
331	Connect to TSA for time stamping
332	Make OCSP lookup
333	Complete signing and generate PAdES document with LTV
400	Public Key Infrastructure
410	PKI solution's store of certificates and optional keys.
411	PKI solution signs document with private key and certificate.
412	Submission of signature based on User's private keys to signature porting system.
413	Request from PKI for authentication.
101	Multi signature system
1200	User_1
2200	User_2
1300	Multi signature porting system.
1400	Public Key Infrastructure which User_1 is to use for signing (PKI_1)
2400	Public Key Infrastructure which User_2 is to use for signing (PKI_2)
1212	User_1 interaction with systems (such as preparing hardware for authentication, entering password, pin codes)
1213	User_1 authenticates himself with pass word, pin codes.
1401	PKI_1 transmits request to User_1 for authentication
1402	Transmission of signature based on User_1 private keys to Signature porting system.
1340	Processing of signatures and documents from User_1 and PKI_1
1342	Signature porting system transmits request to PKI_1 for signature
1343	Completion and storing of PDF document with signature from User_1
1230	PDF document signed by User_1
2212	User_2 interaction with systems (such as preparing hardware for authentication, entering password, pin codes)

2213	User_2 authenticates himself with password, pin codes.
2340	Processing of documents and signatures from User_2 and PKI_2
2342	Signature porting system transmits request to PKI_2 for signature
2401	PKI_1 transmits request to User_1 for authentication
2402	Transmission of signature based on User_2 private keys to Signature porting system.
2343	Completion and storing of PDF document with signature from User_1 and User_2
12230	PDF document signed by User_1 and User_2
1344	Downloading of PDF document having two signatures to User_1
2344	Downloading of PDF document having two signatures to User_2
102	Details on signed PDF document
500	Structure in signed PDF document
510	Contents
511	Certificate
512	Signed message digest
513	Time stamp

Detailed Description

The invention will be further described in connection with exemplary embodiments which are schematically shown in the drawings, wherein:

Fig. 1 shows schematically a signature system with an interaction between a user, a signature porting system, and a PKI, and

Fig. 2 shows schematically the structure of a signed PDF document signed according to the invention.

Principles forming the basis of the invention

If a data object or a file is signed with a qualified electronic signature then also every copy will be valid signed issues. A qualified electronic signature is attached to the data object through a cryptographic algorithm in such a way that the signature does not validate if the data object is changed. The idea behind the invention is however that a qualified electronic signature can be detached from its signature object and used to apply a valid signature on a copy of the signature object in another signature encapsulation format. This signature porting can be performed without involving signatories, certificate authorities. Depending on the formats that are converted to

and from there will be a need to specify certain basic requirements that the original signature will have to support such as algorithm for calculating hash etc.

Best Modes of Carrying Out the Invention

The embodiment of the apparatus according to the invention shown in Fig. 1 and 2 comprises system with a signature and system with a plurality of signatures on the same document, also known as multi signature system.

It is desirable to use BankID and Buypass PKI to sign PDF in PAdES format. Initially we will support PAdES, part IV LTV profile (Long Term Validation) but also other formats can be implemented.

At the present time, however, BankID does not support signing of PDF in Adobe PDF format but can return a SEID SDO file (encapsulation format). The present invention for signature porting overcomes this problem by porting the signatures from SDO to the PAdES format.

The Buypass PKI provider has limited support for PDF signing, with limitations in file size, as well as missing support for full PAdES LTV format. The Buypass PKI provider nevertheless supports the CMS CADES-BES format, and the present invention therefore enables PAdES signature of PDF documents by porting the signature from the CMS CADES-BES to the PAdES format for PDF documents of any size.

Generally it is possible to port such a signature provided that:

1. PKI provider can return a PKCS#7-compatible signature blob (CMS or CADES-BES) over data or hash of data.
2. PKI provider can process data or hash without coding or decoding or any other changes of data.
3. It is desirable that PKI provider includes all validation information (certificates, CRL and OCSP response) that are required in order to generate a long term validation of all involved certificate chains. This includes main certificate chain from the certificate which is used to signing the root certificate. Moreover it is desirable to have a chain of certificates for providers of validation information (OSCP services, CRL issuers and TSA) included.
4. If PKI providers do not include all necessary information for validations then this information must be possible to acquire by other means (such as via online

services). All missing validation information must be available either in the form of certificates offline or via online services (CRL).

Fig. 1 shows the information flow in a signature system 100 having only a single user with corresponding equipment, preferably co-located, 200 signing a document 210. The user commences the process by uploading 211 of the document 210 to the signature porting system 300.

The signature porting system 300 comprises a plurality of components that can be co-located and which in a typical embodiment are not with the user. In the signature porting system the received document 210 is pre processed and prepared for signing 311 and stored or temporarily stored as a pre processed document 312 and is transmitted to two different routes in the system.

In a first route the document is transmitted 313 as a request for signing to Public Key Infrastructure, commonly abbreviated as PKI 400, and comprises a plurality of sub systems. Amongst these is the PKI solution's storage of certificates and optionally keys 410. This requires authentication so a request for authentication 411 is transmitted to the user 200, which uses Smartcard, OTP generator, pin codes or password 220 for this. The response is that the user authenticates himself 221 with password, pin codes etc. to PKI 400 in such a way that the PKI solution signs the document with a private key and certificate 411. Next the transmission 412 of signature based on user's private keys to the signature porting system 300 which then creates a digital signature 320 in for instance SDO, CMS, PKS#7, XML or other formats. Then signature is extracted 321 from the received file and is transmitted to a unit for porting 330 of the signature to the PDF document.

In a second route the prepared document is transmitted 315 to the unit for porting 330 of the signature to the PDF document. In this process signed message digest is extracted from the document received from PKI and is attached to the prepared PDF document for completion of signature. In this phase time stamp from TSA and OSCP-lookup is missing.
From the unit for porting the process proceeds to a unit 331 for connection to Time Stamping Authority, usually abbreviated TSA, for time stamping, and then to a unit 332 for generating Online Certificate Status Protocol, frequently called OCSP, lookup. TSA provides time from independent trusted third party from for instance atomic clock. The time stamp can be verified and provides necessary proof of time of

signing. OSCP lookup is made in order to verify validity of a user certificate at the time of signing. If for instance the certificate is expired or locked, the signing process will have to be interrupted. Additionally LTV signature is generated wherein validation data (CA certificates, OSCP lookup or CRL) are stored together with the document in order to make it possible for later validation of digital signature.

Finally in the signature porting system this is sent to a unit 333 for completion of signing and making PAdES document with LTV and which returns to the user a digitally signed PAdES PDF document 230.

Fig. 2 shows schematically an example 101 of multi signing of a document of two users comprising a first user 1200 and a second user 2200 having two different PKI solutions. Each user comprises equipment preferably co-located with each user, while each user can be located separately.

In this example the PDF document is signed preferably first by User_1 1200, then by User_2 2200.
User_1 1200 uploads the PDF document 210 to the multi signature porting system 1300. Next the document is processed in 1340 making document that is transmitted 1342 to signing in PKI system 1400. The PKI system requires authentication 1401 from User_1. User_1 prepares necessary hardware for authentication (chips, smartcard) 1212 and authenticates himself 1213 with OTP, pin codes, password. Based on this signature is generated and transmitted back 1402 to the multi signature porting system 1300.
The signing process is completed in 1343 by contacting OSCP and TSA servers and is stored as PAdES document with LTV 1230. Next this document is prepared in 2340 for preparing for signing by User_2 2200. User_2 can have access to a different PKI solution 2400. The document that is prepared in 2340 is transmitted 2342 to PKI system 2400 for signing. User_2 receives request 2401 for authentication, prepares smartcard, chips 2212 and authenticates himself 2213 using pin codes, OTP or password. PKI 2400 generates digital signature.
When the signature is transmitted back 2402 to the multiple signature system 1300 the signature process is completed in 2343 by porting signature as well as making lookup to OSCP and TSA server and time stamping for storing PAdES LTV signature.

The signed document 12230 is stored ready for download. In the end the document 12230 having signatures from both users can be downloaded 1344 by User_1 for local storage 1344 and downloaded 2344 by User_2 for local storage.
User_1 has signed the original document while User_2 has signed the original document with a signature from User_1.

Note that the multi signing takes place by chaining together a process. In the above example it is the transmission 1343 that connects the signature process from User_1 together with the signature process for User_2. It is therefore possible to extend the process to more than two users by continuing the chaining. Such a chain typically comprises

a start wherein the first user uploads a document to be signed.
a signing from each user, and
a completion wherein the document is assembled and transmitted to each who is to receive the document.

Typically the receivers are the same as those who signed the document.

Fig. 3 shows schematically a structure 500 of a signed PDF document comprising content 510, a certificate 511, a signed message digest 512, and a time stamp 513.

Alternative Embodiments

A number of variations on the above can be envisaged. For instance the signature porting system enables signature porting as long as there is algorithmic compatibility between the formats.

One can also imagine making parts of the signature generation offline, for instance as long as one keeps private keys and then adding other information available online in order to meet the standards.

Industrial Applicability

The invention according to the application finds use in digital signing of documents.

Claims

1. A method for digital signing of documents (210) by a user (200) comprising steps:

reception (211) of a document (210),

preparation for signing (311) and storing or temporarily storing as a prepared document (312),

transmission (313) of the prepared document as request for signing to PKI,

reception (412) of signature from PKI,

generation of a digital signature (320),

extraction (321) of signature from received signature from PKI and transmission to a unit for porting (330) of the signature,

transmission (315) of the prepared document for completion of signature to the unit for porting (330) of the signature to the document,

time stamping (331),

lookup to create OCSP (332),

completion of signing (333), and

returning of signed document (230),

characterised in that the user (200) signs with own private key.

2. The method according to claim 1, wherein the completion of signing generates a PAdES document with LTV.

3. A method for digital signing of documents (210) comprising steps:

reception (211) of a document (210),

signing by at least one user (200, 1200, 2200), comprising

preparation for signing (311) and storing or temporarily storing as a prepared document (312),

transmission (313) of the prepared document as request for signing to PKI,

reception (412) of signature from PKI,

generation of a digital signature (320),

extraction (321) of signature from received signature from PKI and transmission to a unit for porting (330) of the signature,

transmission (315) of the prepared document for completion of signature to the unit for porting (330) of the signature to the document,

time stamping (331),

lookup to create OCSP (332),
completion of signing (333), and
transmission (2340) to a subsequent user (2200) for signing,
returning (1344, 2344) of signed document (230, 12230),
characterised in that the users (200, 1200, 2200) signs with own private key.

4. The method according to claim 3, wherein the completion of signing generates a PAdES document with LTV.

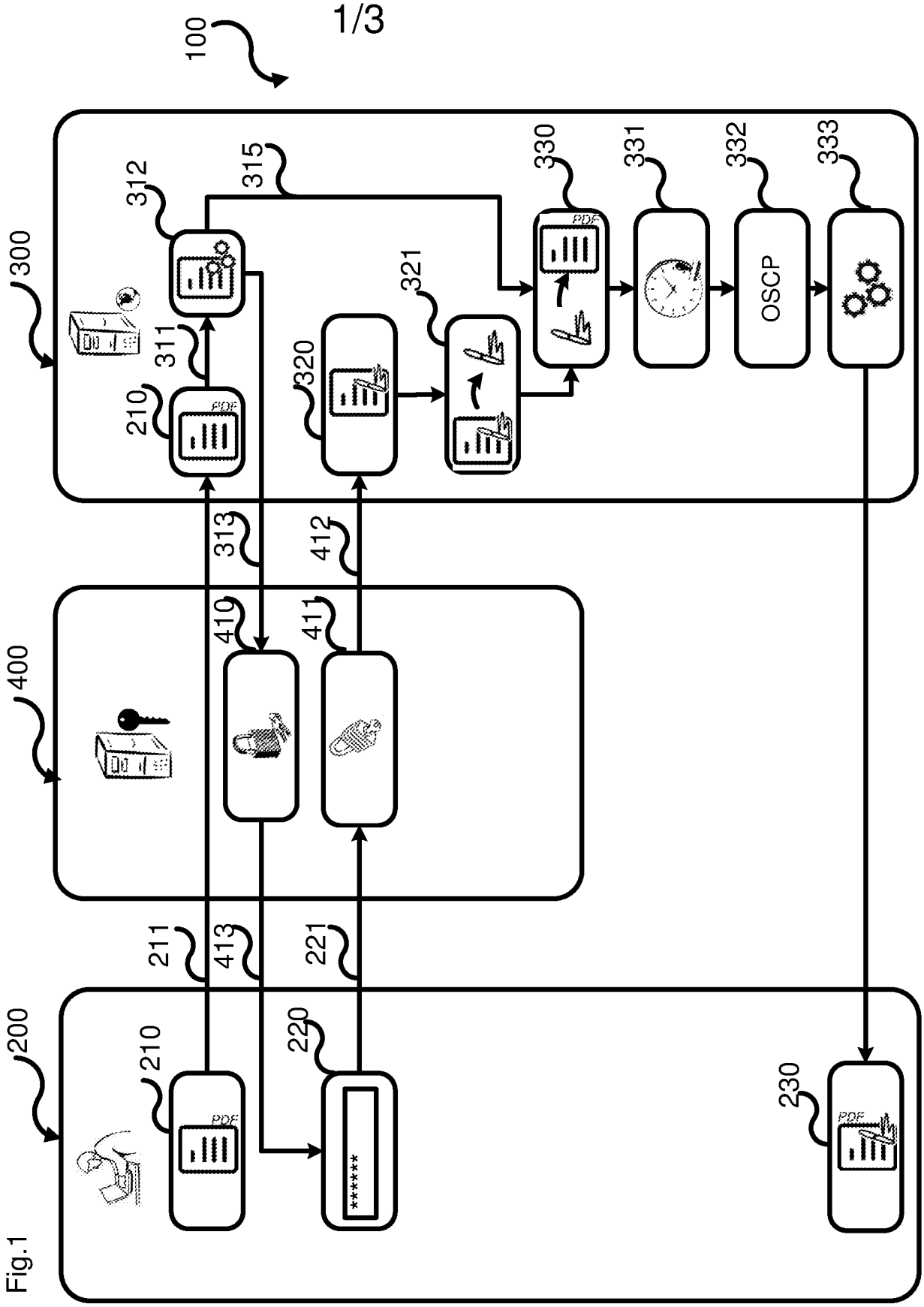

100
300
312
315
330
331
332
333
OSCP
321
311
210
320
313
412
400
410
411
211
413
221
200
210
220
230
PDF
****

Fig.1

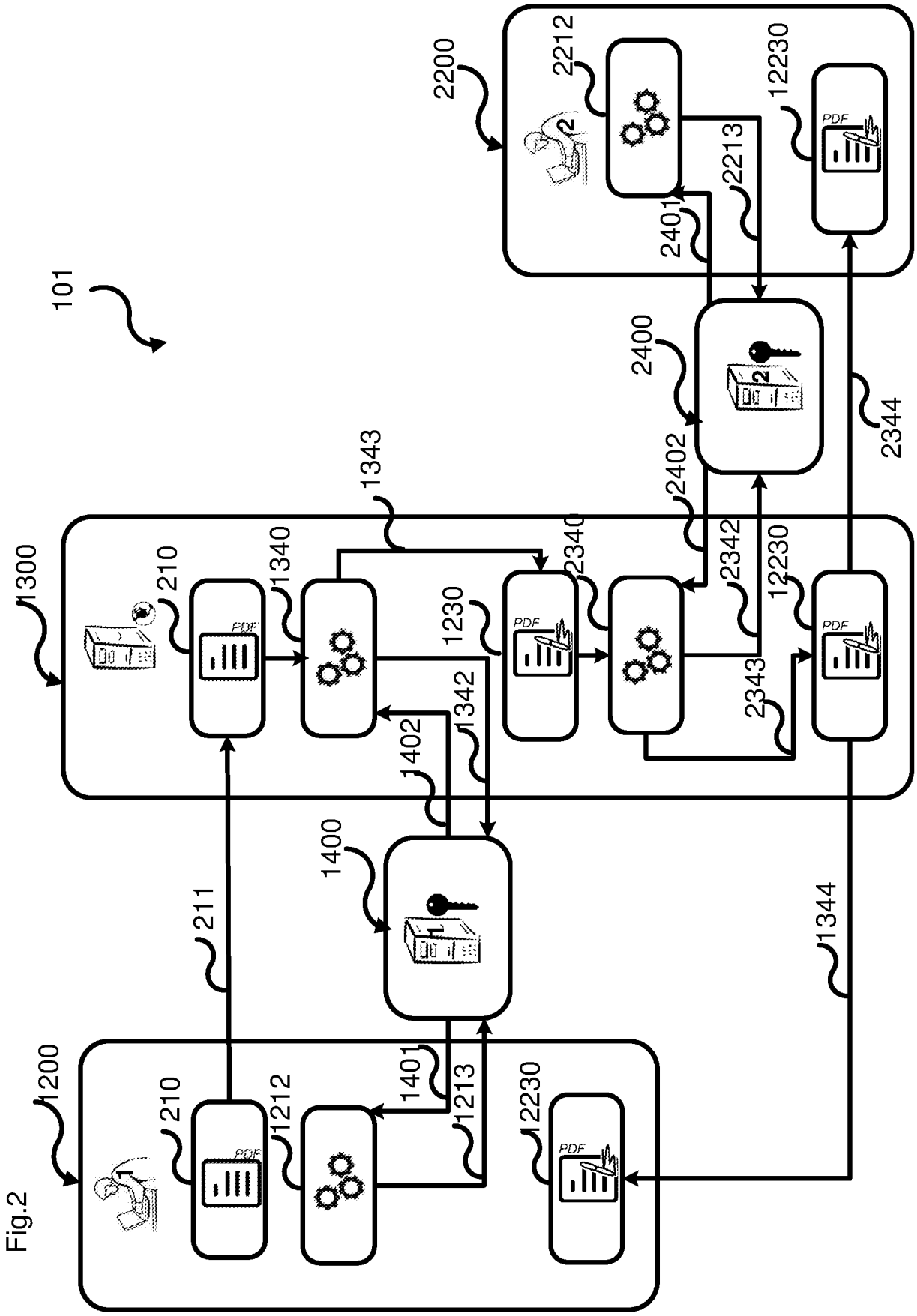

101
1200
210
1212
1401
1213
12230
1400
211
1344
1300
210
1340
1343
1230
2340
1342
1402
2342
12230
2343
2344
2400
2402
2200
2212
2213
12230
2401
PDF

Fig.2

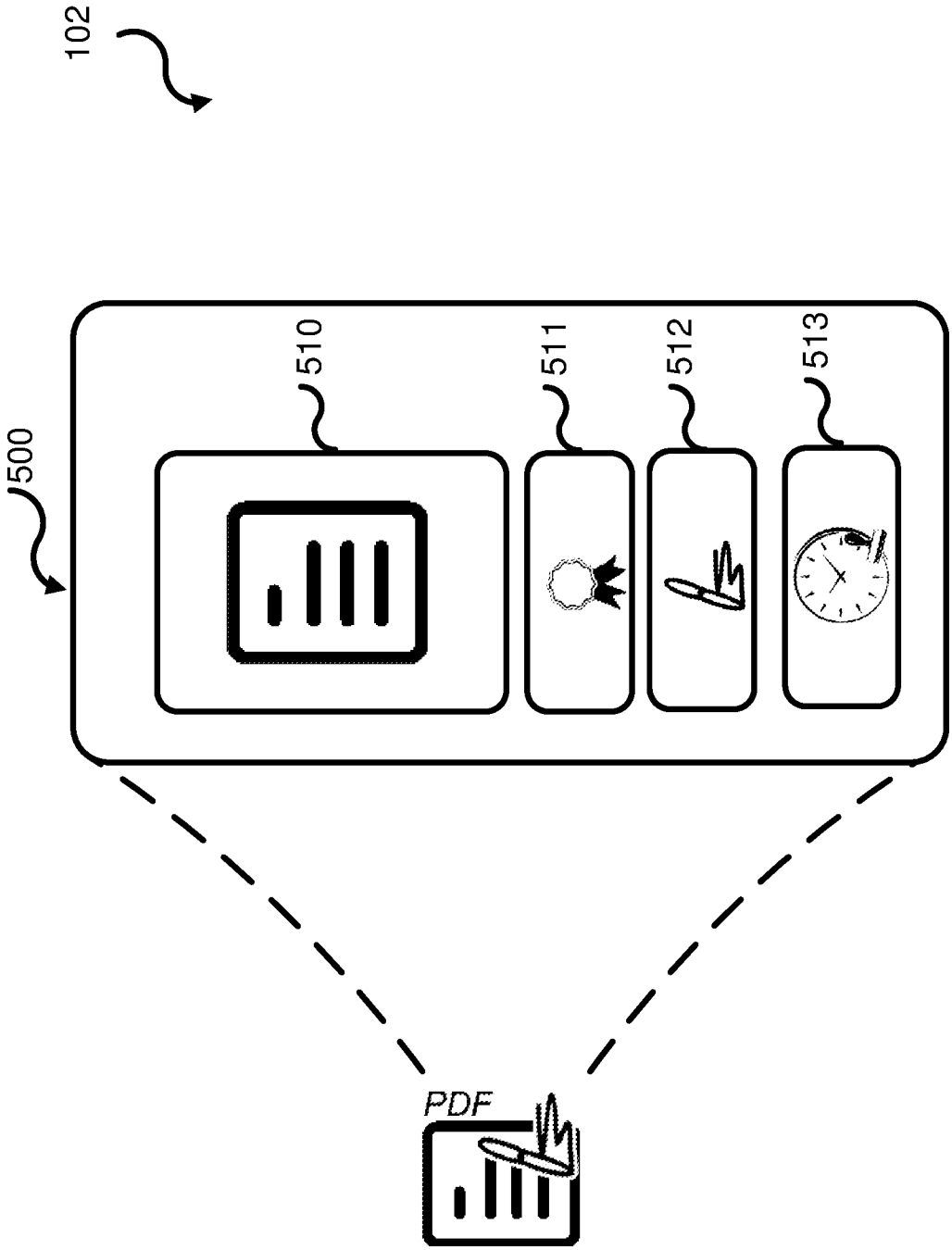


Fig.3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO2013/050198

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30 (2013.01), G06F 21/64 (2013.01), H04L 9/32 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

DK, NO, SE, FI: Classes as above.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI, FULLTEXT: ENGLISH, GERMAN, FRENCH

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y & Y	WO 2012/114602 A1(SEIKO INSTR INC) A1 2012.08.30 Whole document US 2013/0326225 A1 (MURAO, S.) 2013.12.05 Whole document, especially abstract; paragraphs [0008]-[0019], [0105]-[0106]; figures 1-5 US 2009/0024912 A1 (MCCABE A. D et al.) 2009.01.22 Whole document, especially abstract; paragraphs [0002]-[0005], [0009]-[0022]; figures 1-2	1-4 1-4
A	US 2004/0181756 A1 (BERRINGER, R et al.) 2004.09.16 Paragraphs [0042]-[0045]	1-4
A	WO 2008/004221 A2 (WONDERNET LTD) 2008.01.10 Claims 1-14	1-4
A	JP 2009-4853 A (NIPPON TELEGRAPH & TELEPHONE) 2009.01.08 Translated abstract	1-4

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08/01/2014	05/02/2014
Name and mailing address of the ISA Nordic Patent Institute Helgeshøj Allé 81 DK - 2630 Taastrup, Denmark. Facsimile No. + 45 43 50 80 08	Authorized officer Kristoffer Bakkerud Telephone No. +47 22 38 75 84

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO2013/050198

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/0208944 A1 (PAVLICIC, M) 2007.09.06 Figure 1-5; paragraphs [0004], [0005], [0013]-[0029], [0040]	1-4
A	US 2001/0002485 A1 (BISBEE, S.F et al.) 2001.05.31 Paragraph [0039]	1-4
A	Advanced Electronic Signature, Azizi Fazel Ahmad , (2012, June), Norwegian Univeristy of Science and Technology Department of Telematics [accessed 2013.01.05] Chapters 3.3.6 and 4	1-4

Patent document cited in search report / Publication date	Patent family member(s) / Publication date
WO 2012114602 A1 2012.08.30	JP 2012175553 A 2012.09.10 CN 103370901 A 2013.10.23 US 2013326225 A1 2013.12.05 DE 112011104944T T5 2014.01.23
US 2009024912 A1 2009.01.22	WO 2009012478 A2 2009.01.22 CA 2731116 A1 2009.01.22 US 2009292786 A1 2009.11.26 WO 2010151630 A2 2010.12.29 CA 2766745 A1 2010.12.29 AU 2010264441 A1 2012.02.09 SG 177356 A1 2012.02.28 EP 2446376 A2 2012.05.02 JP 2012531672 A 2012.12.10
US 2004181756 A1 2004.09.16	WO 0195078 A1 2001.12.13 AU 7529801 A 2001.12.17 US 2006179320 A1 2006.08.10
WO 2008004221 A2 2008.01.10	NONE
JP 2009004853 A 2009.01.08	NONE
US 2007208944 A1 2007.09.06	WO 2007106280 A1 2007.09.20 KR 20080106532 A 2008.12.08 EP 1999631 A1 2008.12.10 CN 101395599 A 2009.03.25
US 2001002485 A1 2001.05.31	US 5615268 A 1997.03.25 WO 9712460 A1 1997.04.03 CA 2232170 A1 1997.04.03 AU 7105896 A 1997.04.17 US 5748738 A 1998.05.05 NO 981170 A 1998.05.13 TR 9800462T T1 1998.06.22 EP 0850523 A1 1998.07.01 PL 326075 A1 1998.08.17 CZ 9800787 A3 1998.10.14 MX 9801991 A 1998.10.31 CN 1202288 A 1998.12.16 HU 9802232 A2 1999.01.28 NZ 318941 A 1999.07.29 JPH 11512841 A 1999.11.02 WO 9957847 A1 1999.11.11 CA 2334804 A1 1999.11.11 AU 3741099 A 1999.11.23 BR 9610720 A 1999.12.21

Patent document cited in search report / Publication date	Patent family member(s) / Publication date
	AU 5597299 A 1999.12.23 AU 714220B B2 1999.12.23 NO 20005571 A 2001.01.03 BR 9910221 A 2001.01.09 EP 1076954 A1 2001.02.21 US 6237096 B1 2001.05.22 WO 0141360 A2 2001.06.07 CA 2393116 A1 2001.06.07 ID 28890 A 2001.07.12 TR 200100282T T2 2001.07.23 CN 1308803 A 2001.08.15 PL 344052 A1 2001.09.24 HU 0102397 A2 2001.10.28 IL 123663 A 2002.03.10 US 6367013 B1 2002.04.02 MXPA 00010807 A 2002.05.08 JP 2002514799 A 2002.05.21 ZA 200007121 A 2002.05.29 EP 1236305 A2 2002.09.04 AU 758834B B2 2003.04.03 BR 0016079 A 2003.06.10 EA 003620 B1 2003.08.28 NZ 508562 A 2003.10.31 WO 2004010271 A2 2004.01.29 CA 2492986 A1 2004.01.29 AU 2003259136 A1 2004.02.09 MXPA 02005311 A 2004.04.21 NZ 519261 A 2004.04.30 US 2004093493 A1 2004.05.13 AU 776251B B2 2004.09.02 KR 100455326B B1 2004.11.09 IL 139396 A 2004.12.15 KR 100455327B B1 2004.12.31 JP 2005502927 A 2005.01.27 AP 1369 A 2005.02.04 MXPA 05000696 A 2005.04.08 HK 1017540 A1 2005.04.29 BR 0312774 A 2005.05.03 EP 1540881 A2 2005.06.15 KR 20050074430 A 2005.07.18 NZ 530378 A 2005.09.30 CN 1682490 A 2005.10.12 SG 115692 A1 2005.10.28 Patent family annex sheet no. 2 of 3

Patent document cited in search report / Publication date	Patent family member(s) / Publication date
	AT 307437T T 2005.11.15
	EP 1617590 A2 2006.01.18
	EP 1617589 A2 2006.01.18
	DK 1236305T T3 2006.03.06
	JP 2006511984 A 2006.04.06
	ES 2251415T T3 2006.05.01
	EA 007089 B1 2006.06.30
	DE 60023340T T2 2006.07.27
	AT 334525T T 2006.08.15
	NZ 537994 A 2006.09.29
	HK 1035091 A1 2007.01.05
	DE 69932512T T2 2007.02.15
	AT 358371T T 2007.04.15
	HK 1087862 A1 2007.10.12
	DE 60034159T T2 2007.12.13
	JP 2009238254 A 2009.10.15
	AT 481788T T 2010.10.15
	HK 1087863 A1 2010.12.03
	ES 2352743T T3 2011.02.22
	JP 2011087323 A 2011.04.28
	HK 1083252 A1 2013.05.10