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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2012 (02.08.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/100351 A1

(51) International Patent Classification:
H04L 12/26 (2006.01) *G06Q 20/10* (2012.01)
G06Q 30/06 (2012.01)

(21) International Application Number:
PCT/CA2012/050042

(22) International Filing Date:
27 January 2012 (27.01.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/437,153 28 January 2011 (28.01.2011) US

(71) Applicant *(for all designated States except US)*: **ROYAL CANADIAN MINT/MONNAIE ROYALE CANADIENNE** [CA/CA]; 320 Sussex Drive, Ottawa, Ontario K1A 0G8 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **EVERETT, David** [GB/GB]; Redroofs, The Roundway, Rustington BN16 2BW (GB).

(74) Agent: **BLAKE, CASSELS & GRAYDON LLP**; 45 O'Connor Street, Suite 2000, Ottawa, Ontario K1P 1A4 (CA).

(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, 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, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, MD, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

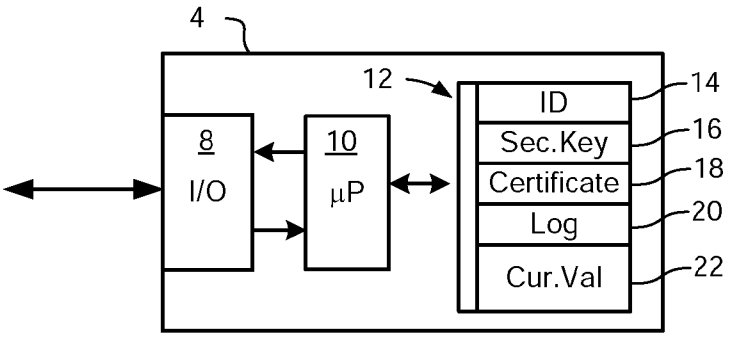
Published:

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

WO 2012/100351 A1

(54) Title: ELECTRONIC TRANSACTION RISK MANAGEMENT

Figure 2



(57) Abstract: A method of detecting unauthorized activity in an electronic message transfer system comprising a plurality of devices, each device being configured to generate and receive cryptographically secured transfer messages for exchanging content with other devices in the system. In each device, audit information is accumulated in a memory of the device. The device periodically forwards at least part of its accumulated audit information to a secure server.

ELECTRONIC TRANSACTION RISK MANAGEMENT

TECHNICAL FIELD

[0001] The present disclosure relates to electronic transaction systems, and in particular to a system and methods for managing risks associated with electronic transactions within an un-trusted environment.

BACKGROUND

[0002] For the purpose of the present description, an "untrusted environment" shall be understood to mean any communications or networking environment in which it is possible for attackers to modify messages, delete messages or even add or replay messages. The public Internet is a common example of an untrusted environment, since it is not possible to prohibit attackers from modifying, deleting, adding or duplicating messages.

[0003] For the purposes of the present description, a "sensitive transaction" shall be understood to refer to any message exchange or communications session between two or more parties, in which it is desired that message content(s) should be reliably transferred between the parties, and be secure against unauthorized viewing and/or manipulation. Examples of "sensitive transactions" include, but are not limited to: financial transactions such as electronic funds transfers and eCommerce; remote sensing and telemetry data transfer messaging; and electronic voting schemes.

[0004] Internet-based electronic transaction systems are well known in the art. In order to mitigate risks associated with sensitive transactions in an un-trusted environment such as the Internet, such systems typically employ a secure server, which acts as an intermediary between parties to any electronic transaction. In some cases, the secure server merely serves to authenticate the parties. More commonly, the secure server both authenticates the parties and controls the actual funds transfer. As a result, the secure server is able to provide both parties with confidence that the transaction has been completed properly, and also enables the server to generate a detailed audit trail, by which the service provider can detect fraudulent or otherwise inappropriate use of the system by any party. A limitation of this arrangement is that the requirement for users to log into the central server in order to perform any transaction, is inconvenient, and thus so limits user acceptance of the system.

[0005] Various schemes have been proposed which are intended to enable electronic person-to-person financial transactions in a manner that is directly analogous to fiat cash

transactions, in that the intervention of a central server to mediate the transfer of funds is not used. A central theme of such systems is the provision of security mechanisms that provide at least the same level of security and trustworthiness that is afforded by conventional central server-based systems, but without the inconvenience of requiring the parties to log into a central server. However, these systems suffer a limitation in that, because a user may log into a central server infrequently (or even never), there is no reliable mechanism by which a service provider can build an audit trail that would permit the detection of fraudulent or otherwise inappropriate activity.

SUMMARY

[0006] Accordingly, the present invention sets out to provide a practical way of overcoming the above limitations of the prior art.

[0007] Accordingly, an aspect of the present invention provides a method of detecting unauthorized activity in an electronic message transfer system comprising a plurality of devices, each device being configured to generate and receive cryptographically secured value transfer messages for exchanging amounts monetary value with other devices in the system. In each device, audit information is accumulated in a memory of the device. The device periodically forwards at least part of its accumulated audit information to a secure server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Further features and advantages will become apparent from the following detailed description, taken in combination with the appended drawings, in which:

[0009] FIG. 1 is a block diagram schematically illustrating a secure message exchange system in which methods in accordance with the present invention may be implemented;

[0010] FIG. 2 is a block diagram schematically illustrating a subscriber's communications device, usable in the system of FIG. 1; and

[0011] FIG. 3 is a block diagram of a diagram schematically illustrating an alternative subscriber's communications device, usable in the system of FIG. 1.

[0012] It will be noted that throughout the appended drawings, like features are identified by like reference numerals.

DETAILED DESCRIPTION

[0013] It is anticipated that users (subscribers) of an online service that enables sensitive transactions will be required to indicate their acceptance of a published set of terms and conditions, as a condition of their use of the system. Among other things, these terms and conditions will set out limitations in the proper use of the service, including, for example, that the user agrees to not use the service for illegal or unethical purposes.

[0014] Upon acceptance of the terms and conditions, the user may be provided with an electronic storage and transfer device generally of the type described in Applicant's co-pending international patent applications Nos. PCT/CA2010/000435 filed March 30, 2010 and PCT/CA2010/001434 filed September 17, 2010, both of which designate the United States of America, the disclosures of both of which are incorporated herein by reference.

[0015] Referring to FIG. 2, as described in PCT/CA2010/001434, the storage and transfer device 4 comprises an input/output (I/O) interface 8 configured to enable the device 4 to send and receive messages through the communications medium 6; a controller 10 responsive to received messages to record transfers of content to the device 4 and to transfer content from the device 4; and a memory 12 storing a respective unique identifier 14 of the device 4, a private (or secret) key 16 and a certificate 18 uniquely assigned to the device 4, a log 20 of content transfers to and from the device 4, and a current content (Cur.Val) 22 of the device 44.

[0016] The secret key 16 and a certificate 18, facilitate message encryption and digital signature functionality using, for example, well-known Public Key Infrastructure (PKI) techniques. For this purpose, the secret key 16 can be securely generated by the storage and transfer device 4 and the certificate 18 would typically be generated by a trusted Issuing Authority, such as, for example, Verisign (TM).

[0017] As described in PCT/CA2010/001434, in a "transfer-out process", the device 4, operates to generate a cryptographically secured content (asset value) transfer message containing the content to be transferred, a nonce for enabling detection and proper handling of duplicate messages, a digital signature generated using the secret key 16, and the certificate 18. With this information, a receiving device 4 can execute a "transfer-in" process in which the certificate can be used to verify the digital signature, and so detect any corruption of the message during transport through the network, detect (and discard) duplicate messages by the use of protected sequencing or equivalent identifying information in the message, and finally update its current content (Cur.Val) 22 with the content

conveyed in the message. In addition, the processor 10 can record information about each transfer-in and transfer-out in the log 20. Among other things, the log may be accessed by the user to obtain a record of transactions.

[0018] It is anticipated that the device 4 may be constructed in two variants. In a first variant, the device 4 is constructed as a physical device suitable for distribution to and use by an individual person. In a second variant, the device 4 is constructed as server configured to emulate a desired number of physical storage devices allocated to individual users. In this latter case, a user may access their device 4 by means of suitable application software stored on a communications device. In principle, the log can be used to construct an audit trail (at least in respect of the particular device) and so could be used to detect non-compliant use of the device 4. However, in practice, it is possible for a user to use their device 4 to engage in person-to-person financial transactions without logging in to a central server that could access the log 20 to obtain the required transaction information. In this situation, it is possible that the service provider might never be able to ensure that the system is free from abuse.

[0019] The following three strategies may be employed for addressing this problem.

[0020] 1. Encoding utilization limits into the firmware of the processor 10. Such utilization limits can take any of a variety of different forms, depending on the type of data stored in the memory 12, either within the log 20 or in other data storage fields (not shown) provided in the memory 12 for that purpose. For example, utilization limits based on an accumulated amount of asset value transferred, or a total number of transactions can be readily defined. Other utilization limits may also be defined, as desired. In operation, when the utilization limit has been reached, the processor 10 may reject any further requests to transfer content in to, or out of the device 4, until the user either logs in to a central server and resets their device 4, or alternatively contacts the service provider to exchange their device 4 for a new one. In either scenario, the service provider is enabled to access the memory 12 of the device 4, and thereby detect non-compliant use of the device 4.

[0021] 2. Encoding transaction limits into the firmware of the processor 10. A representative transaction limit may, for example, take the form of a maximum content amount (such as, for example, a monetary amount) that can be transferred in any given transfer message. If the transaction limit is exceeded, the processor 10 may issue a notification to the user requesting that they log onto a central server to obtain authorization for the transaction. Here again, once the user completes the log on procedure, the secure

server can access and analyze all or part of the data stored in the memory 12, and thereby detect non-compliant use of the device 4.

[0022] 3. Configuring the firmware of the processor 10 to embed encrypted audit information in each content transfer message, for example within a predefined field of the message. The audit information may comprise data stored in the memory 12 (or be derived from such stored data), that can be analysed to detect unauthorized or otherwise non-compliant use of the device 4. This audit information may, for example, include an accumulated amount of asset value transferred, or a total number of transactions, as well as any of a variety of possible fault codes that could be generated by the processor 10 during operation. Such fault codes could, for example, comprise a total number of transfer-in or transfer-out processes that were not successfully completed. Other audit information may be defined as desired and accumulated in the memory 12 for inclusion in content transfer messages. In order to ensure secure encryption of the audit information, a provider's secret key (PSK) 24 (see FIG. 3) that is known only to the service provider may be installed in the device 4.

[0023] During each transfer-put process, the processor 10 can extract the audit information from the memory 12, encrypt it using the PSK 24, and attach the encrypted audit information to the content transfer message prior to applying the digital signature (based on the user's Secret key 16) and certificate 18. With this arrangement, the digital signature encompasses the encrypted audit information, so that attempts to fraudulently manipulate the encrypted audit information can be detected (and result in failure of the transaction). Encryption of the audit information using a Provider's Secret Key (PSK) 24 separate from the user's secret key 16 ensures that the recipient of any content transfer messages (with the sole exception of the service provider itself) will be unable to access and read the audit information.

[0024] The embedding of encrypted audit information in each content transfer message enables the service provider to enter into specific service agreements with selected parties (such as, for example, on-line merchants) whereby each party agrees to forward a copy of some (or all) received content transfer messages to the service provider. Upon receipt of these copied messages, the service provider can decrypt and analyse the embedded audit information. It is anticipated that, by entering into appropriate agreements with on-line merchants (and other parties who may be expected to interact with a large number of individual users), the service provider will receive copies of a significant portion (although likely not all) of the asset transfer messages being exchanged between all users of the

system. Consequently, the service provider can analyse the decrypted audit information to detect unauthorized activities, as well as derive statistically valid metrics regarding the status of the system as a whole.

[0025] The embodiment(s) of the invention described above is(are) intended to be exemplary only. The scope of the invention is therefore intended to be limited solely by the scope of the appended claims.

WE CLAIM:

1. A method of detecting unauthorized activity in an electronic message transfer system comprising a plurality of devices, each device being configured to generate and receive cryptographically secured transfer messages for exchanging content with other devices in the system, the method comprising, in each device:

accumulating audit information in a memory of the device; and

periodically forwarding at least part of the accumulated audit information to a secure server.

2. The method of claim 1, wherein at least one device is configured to:

detect a predetermined condition; and

in response to the detected condition, notify a user of the device to contact a service provider to reset the device, wherein during a subsequent reset operation, at least part of the accumulated audit information is forwarded to the secure server.

3. The method of claim 2, wherein the predetermined condition is selected from the list of: an accumulated number of transactions; an accumulated value of funds exchanged with other devices; a limit value of funds transferred in any single transaction; a limit value of funds stored in the device.

4. The method of claim 1, wherein at least one device is configured to: embed encrypted audit information in each transfer message generated by the device, and wherein copies of at least some transfer messages are forwarded to the secure server.

5. An electronic message transfer system comprising:

a plurality of devices, each device being configured to generate and receive cryptographically secured transfer messages for exchanging content with other devices in the system, in each device comprising:

a memory for accumulating audit information; and

means for periodically forwarding at least part of the accumulated audit information to a secure server.

6. The system of claim 5, wherein at least one device is configured to:

detect a predetermined condition; and

in response to the detected condition, notify a user of the device to contact a service provider to reset the device, wherein during a subsequent reset operation, at least part of the accumulated audit information is forwarded to the secure server.

7. The system of claim 6, wherein the predetermined condition is selected from the list of: an accumulated number of transactions; an accumulated value of funds exchanged with other devices; a limit value of funds transferred in any single transaction; a limit value of funds stored in the device.

8. The system of claim 5, wherein at least one device is configured to: embed encrypted audit information in each transfer message generated by the device, and wherein copies of at least some transfer messages are forwarded to the secure server.

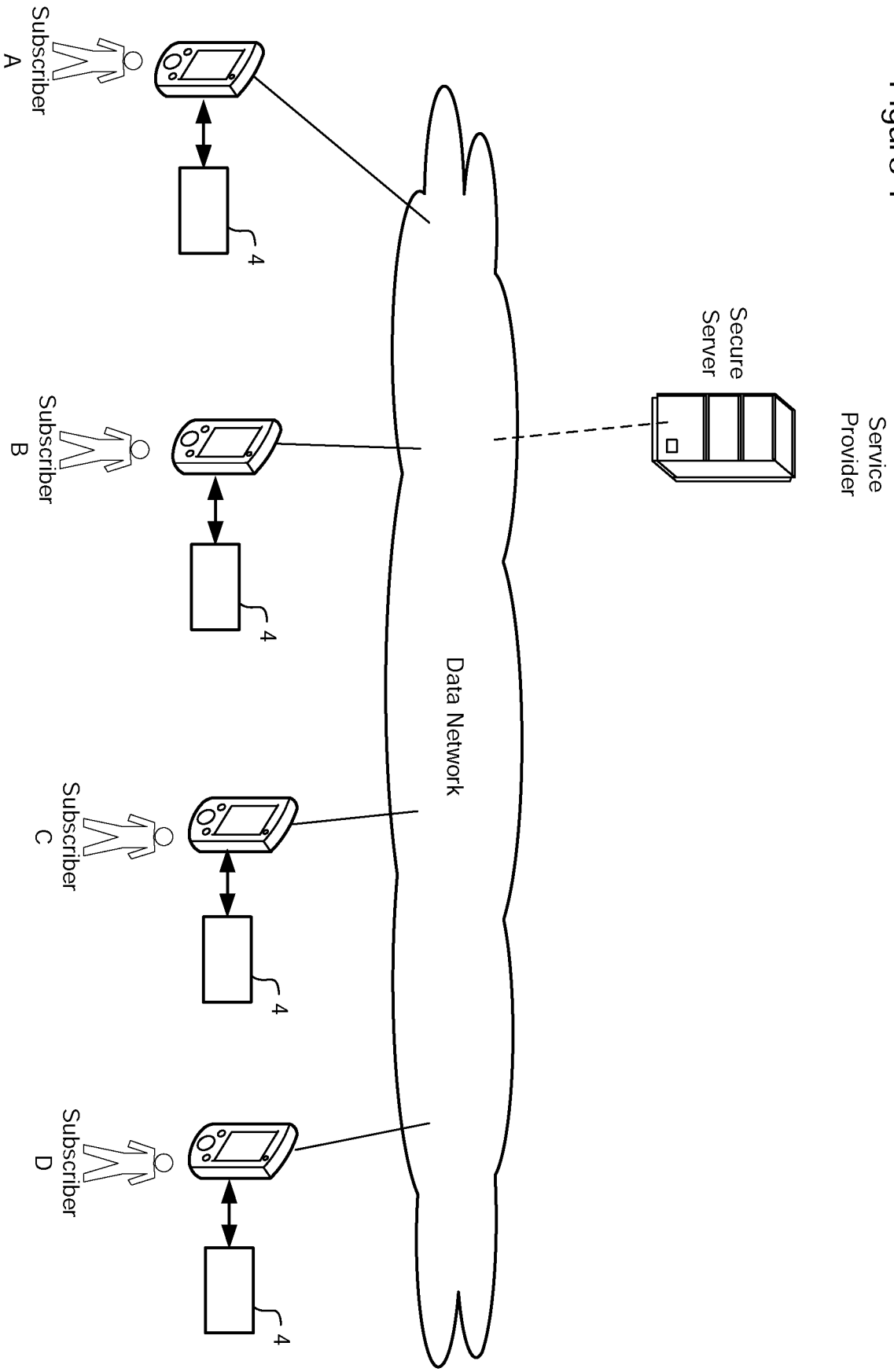

Subscriber A
Subscriber B
Subscriber C
Subscriber D
4
Data Network
Secure Server
Service Provider

Figure 1

Figure 2

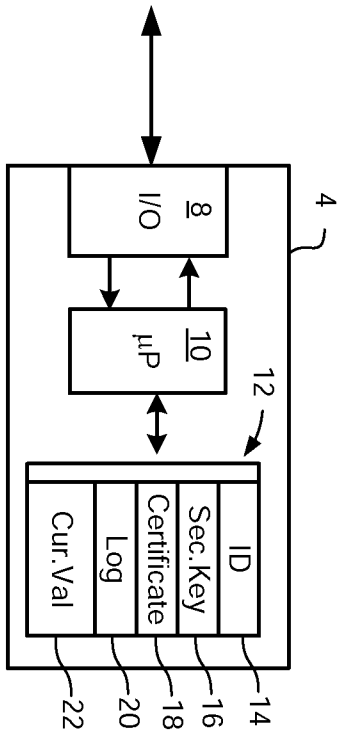
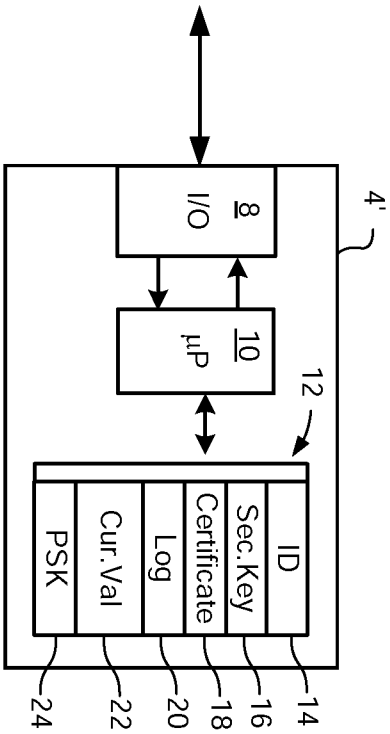


Figure 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2012/050042

A. CLASSIFICATION OF SUBJECT MATTER

IPC: ***H04L 12/26*** (2006.01) , *G06Q 30/06* (2012.01) , *G06Q 20/10* (2012.01)

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: H04L 12/26 (2006.01), G06Q 30/06 (2012.01), G06Q 20/10 (2012.01)

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

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

Databases: EPOQUE (Epodoc, English Full-text), Canadian Patents Database, IEEEXplore, Google

Keywords: detect unauthorized/illegal/fraud/innapropriate, financial/electronic/sensitive transaction, manage/mitigate risk, audit trail/info/data, secure server, generate/transmit/receive/transfer/exchange, secure message/data/content, cryptographic, memory, notify user,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0255652 A1 (TUMMINARO et al.) 1 November 2007 (01-11-2007) *abstract; paragraphs [0020]-[0329]; figs. 3-16*	1-8
Y	US 7 822 688 B2 (LABROU et al.) 26 October 2010 (26-10-2010) *abstract; col. 4, line 59 - col. 18, line 40; figs. 2-4*	1-8
Y	US 5 903 652 (MITAL) 11 May 1999 (11-05-1999) *abstract; col. 3, line 23 - col. 6, line 42; figs. 1-6*	1-8
Y	US 2010/0133337 A1 (VAN RENSBURG) 3 June 2010 (03-06-2010) * paragraphs [0025]-[0031]; claim 6*	1-8
A	US 2008/0215465 A1 (CAPADOUCA) 4 September 2008 (04-09-2008) *whole document*	1-8
A	US 2003/0069858 A1 (KTTLITZ et al.) 10 April 2003 (10-04-2003) *whole document*	1-8

[X] Further documents are listed in the continuation of Box C. [X] 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
18 April 2012 (18-04-2012)	15 May 2012 (15-05-2012)

Name and mailing address of the ISA/CA
Canadian Intellectual Property Office
Place du Portage I, C114 - 1st Floor, Box PCT
50 Victoria Street
Gatineau, Quebec K1A 0C9
Facsimile No.: 001-819-953-2476

Authorized officer
Daniela Savin (819) 934-4890

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 2007/0011099 A1 (SHEEHAN) 11 January 2007 (11-01-2007) *whole document*	1-8
A	JP 2003-044769 A (YOSHITAKE et al.) 14 February 2003 (14-02-2003) *machine translated English abstract and description*	1-8
A	US 2003/0105707 A1 (AUDEBERT et al.) 5 June 2003 (05-06-2003) *whole document*	1-8
A	WO 2005/084177 A2 (DANCKAERT et al.) 15 September 2005 (15-09-2005) *whole document*	1-8
A	US 2002/0077978 A1 (O'LEARY et al.) 20 June 2002 (20-06-2002) *whole document*	1-8
A	EP 1 107 198 A2 (YOUNG et al.) 13 June 2001 (13-06-2001) *whole document*	1-8

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2007255652A1	01 November 2007 (01-11-2007)	BRPI0710021A2	02 August 2011 (02-08-2011)
		BRPI0710089A2	23 August 2011 (23-08-2011)
		CA2647602A1	06 March 2008 (06-03-2008)
		CA2647636A1	06 March 2008 (06-03-2008)
		CN101454794A	10 June 2009 (10-06-2009)
		CN101454795A	10 June 2009 (10-06-2009)
		EP2008237A1	31 December 2008 (31-12-2008)
		EP2013842A1	14 January 2009 (14-01-2009)
		EP2266083A2	29 December 2010 (29-12-2010)
		EP2304678A1	06 April 2011 (06-04-2011)
		EP2344994A1	20 July 2011 (20-07-2011)
		EP2407918A1	18 January 2012 (18-01-2012)
		EP2407919A1	18 January 2012 (18-01-2012)
		MX2008012503A	12 December 2008 (12-12-2008)
		MX2008012504A	05 May 2009 (05-05-2009)
		US2009119190A1	07 May 2009 (07-05-2009)
		US7873573B2	18 January 2011 (18-01-2011)
		US2007230371A1	04 October 2007 (04-10-2007)
		US2007233615A1	04 October 2007 (04-10-2007)
		US2007244811A1	18 October 2007 (18-10-2007)
		US2007255620A1	01 November 2007 (01-11-2007)
		US2007255653A1	01 November 2007 (01-11-2007)
		US2007255662A1	01 November 2007 (01-11-2007)
		US2008032741A1	07 February 2008 (07-02-2008)
		US2009287601A1	19 November 2009 (19-11-2009)
		US2009319425A1	24 December 2009 (24-12-2009)
		US2010063935A1	11 March 2010 (11-03-2010)
		US2011320347A1	29 December 2011 (29-12-2011)
		WO2008027620A1	06 March 2008 (06-03-2008)
		WO2008027621A1	06 March 2008 (06-03-2008)
		WO2009114876A2	17 September 2009 (17-09-2009)
		WO2009152184A1	17 December 2009 (17-12-2009)
		WO2010082960A1	22 July 2010 (22-07-2010)
		WO2011163525A1	29 December 2011 (29-12-2011)
US7822688B2	26 October 2010 (26-10-2010)	CN1897027A	17 January 2007 (17-01-2007)
		CN1908981A	07 February 2007 (07-02-2007)
		CN1922623A	28 February 2007 (28-02-2007)
		EP1388797A2	11 February 2004 (11-02-2004)
		EP1388991A2	11 February 2004 (11-02-2004)
		EP1710980A2	11 October 2006 (11-10-2006)
		EP1723593A2	22 November 2006 (22-11-2006)
		EP1758053A1	28 February 2007 (28-02-2007)
		JP2007527062A	20 September 2007 (20-09-2007)
		JP4469376B2	26 May 2010 (26-05-2010)
		JP2004072777A	04 March 2004 (04-03-2004)
		JP4603252B2	22 December 2010 (22-12-2010)
		JP2004164597A	10 June 2004 (10-06-2004)
		JP2006294035A	26 October 2006 (26-10-2006)
		JP2007042103A	15 February 2007 (15-02-2007)
		KR20060114032A	03 November 2006 (03-11-2006)
		KR100860628B1	29 September 2008 (29-09-2008)
		US2005027543A1	03 February 2005 (03-02-2005)
		US7349871B2	25 March 2008 (25-03-2008)
		US2004030894A1	12 February 2004 (12-02-2004)
		US7353382B2	01 April 2008 (01-04-2008)
		US2006206709A1	14 September 2006 (14-09-2006)
		US7606560B2	20 October 2009 (20-10-2009)
		US2007022058A1	25 January 2007 (25-01-2007)
		US7784684B2	31 August 2010 (31-08-2010)
		US2004098350A1	20 May 2004 (20-05-2004)
		US7801826B2	21 September 2010 (21-09-2010)
		US2005187873A1	25 August 2005 (25-08-2005)
		US2004107170A1	03 June 2004 (03-06-2004)
		WO2005079254A2	01 September 2005 (01-09-2005)
US5903652A	11 May 1999 (11-05-1999)	None	

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US5903652A	11 May 1999 (11-05-1999)	None	
US2010133337A1	03 June 2010 (03-06-2010)	CN101632103A	20 January 2010 (20-01-2010)
		CN101632103B	01 June 2011 (01-06-2011)
		EP2126856A1	02 December 2009 (02-12-2009)
		IL199452D0	28 March 2010 (28-03-2010)
		JP2010514312A	30 April 2010 (30-04-2010)
		US7992792B2	09 August 2011 (09-08-2011)
		WO2008075143A1	26 June 2008 (26-06-2008)
US2008215465A1	04 September 2008 (04-09-2008)	AU2008200973A1	18 September 2008 (18-09-2008)
		AU2008200973B2	03 November 2011 (03-11-2011)
		CA2623331A1	01 September 2008 (01-09-2008)
		EP1965346A1	03 September 2008 (03-09-2008)
		MX2008003005A	25 February 2009 (25-02-2009)
		US7752093B2	06 July 2010 (06-07-2010)
US2003069858A1	10 April 2003 (10-04-2003)	None	
US2007011099A1	11 January 2007 (11-01-2007)	US2007011099A1	11 January 2007 (11-01-2007)
		WO2007008860A2	18 January 2007 (18-01-2007)
		WO2007008860A3	03 May 2007 (03-05-2007)
JP2003044769A	14 February 2003 (14-02-2003)	None	
US2003105707A1	05 June 2003 (05-06-2003)	AU2002342916A1	10 June 2003 (10-06-2003)
		WO03046778A2	05 June 2003 (05-06-2003)
WO2005084177A2	15 September 2005 (15-09-2005)	WO2005084177A2	15 September 2005 (15-09-2005)
		WO2005084177A3	09 March 2006 (09-03-2006)
US2002077978A1	20 June 2002 (20-06-2002)	AU6869201A	02 January 2002 (02-01-2002)
		AU2001268692B2	17 March 2005 (17-03-2005)
		CA2414038A1	27 December 2001 (27-12-2001)
		CN1454364A	05 November 2003 (05-11-2003)
		EP1309933A1	14 May 2003 (14-05-2003)
		EP1309933A4	14 September 2005 (14-09-2005)
		JP2003536174A	02 December 2003 (02-12-2003)
		WO0199019A1	27 December 2001 (27-12-2001)
EP1107198A2	13 June 2001 (13-06-2001)	AU784041B2	19 January 2006 (19-01-2006)
		AU2049101A	12 June 2001 (12-06-2001)
		AU2002250134A1	12 September 2002 (12-09-2002)
		DE60032863D1	22 February 2007 (22-02-2007)
		EP1014646A2	28 June 2000 (28-06-2000)
		EP1014646A3	20 December 2000 (20-12-2000)
		EP1107198A3	31 July 2002 (31-07-2002)
		EP1107198B1	10 January 2007 (10-01-2007)
		JP2001243386A	07 September 2001 (07-09-2001)
		JP2005174326A	30 June 2005 (30-06-2005)
		JP2005190472A	14 July 2005 (14-07-2005)
		PL356106A1	14 June 2004 (14-06-2004)
		US6850991B1	01 February 2005 (01-02-2005)
		US2002065774A1	30 May 2002 (30-05-2002)
		US2002123965A1	05 September 2002 (05-09-2002)
		US2005135345A1	23 June 2005 (23-06-2005)
		WO0141419A1	07 June 2001 (07-06-2001)
		WO02069085A2	06 September 2002 (06-09-2002)
		WO02069085A3	29 April 2004 (29-04-2004)