



US00RE50142E

(19) **United States**
(12) **Reissued Patent**
McCabe et al.

(10) **Patent Number:** **US RE50,142 E**
(45) **Date of Reissued Patent:** **Sep. 24, 2024**

(54) **SYSTEMS AND METHODS FOR
DISTRIBUTED ELECTRONIC SIGNATURE
DOCUMENTS**

(56) **References Cited**
U.S. PATENT DOCUMENTS

(71) Applicant: **DocuSign, Inc.**, San Francisco, CA
(US)

5,040,142 A 8/1991 Mori et al.
5,220,675 A 6/1993 Padawer et al.
(Continued)

(72) Inventors: **Andrew D. McCabe**, Indianola, WA
(US); **Thomas H. Gonser, Jr.**, Alamo,
CA (US)

FOREIGN PATENT DOCUMENTS

(73) Assignee: **DocuSign, Inc.**, San Francisco, CA (US)

AU 2010264441 B2 10/2015
CA 2731116 C 7/2016
(Continued)

(21) Appl. No.: **17/077,551**

OTHER PUBLICATIONS

(22) Filed: **Oct. 22, 2020**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **10,198,418**
Issued: **Feb. 5, 2019**
Appl. No.: **14/537,713**
Filed: **Nov. 10, 2014**

Borozdin et al., “DocuSign Connect Service Guide”, DocuSign, Inc,
2008, 9 pp.

(Continued)

U.S. Applications:

(63) Continuation of application No. 12/176,265, filed on
Jul. 18, 2008, now Pat. No. 8,949,706.
(Continued)

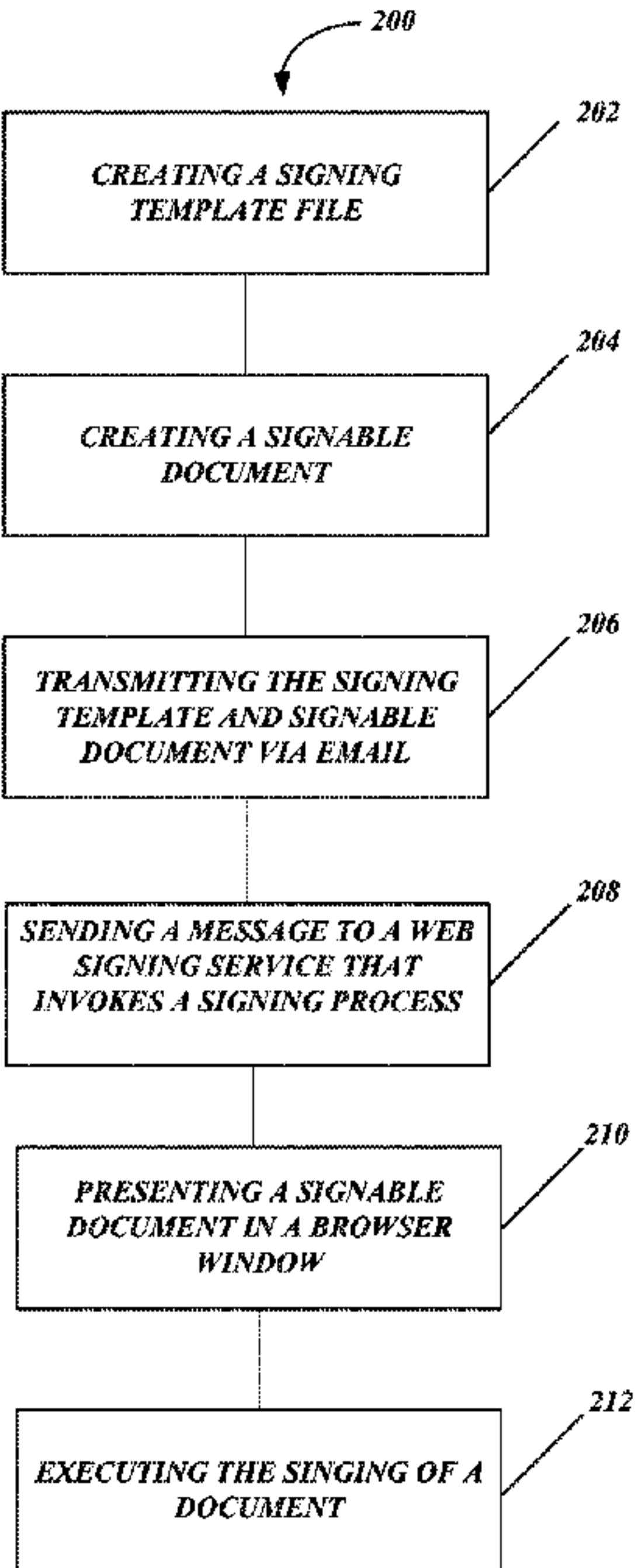
Primary Examiner — Peng Ke
(74) *Attorney, Agent, or Firm* — Shumaker & Sieffert,
P.A.

(57) **ABSTRACT**

Systems and methods for distributed electronic signature documents. A method for distributed electronic signature documents includes creating a signing template that contains information about how a signable document is to be signed. A signable document is created to be distributed to a signer for signing. The signable document is electronically transmitted to the signer. A message is sent using an activatable control in the signing document to a web signing server to invoke the signing process. A browser window is opened on a signer’s computer in order to execute the signing process.

(51) **Int. Cl.**
G06Q 10/10 (2023.01)
G06F 21/64 (2013.01)
G06F 40/174 (2020.01)
(52) **U.S. Cl.**
CPC **G06Q 10/10** (2013.01); **G06F 40/174**
(2020.01); **G06F 21/64** (2013.01)
(58) **Field of Classification Search**
CPC G06F 21/64; G06F 13/24; G06F 13/4291;
G06F 21/645; G06F 2213/0016;
(Continued)

16 Claims, 2 Drawing Sheets



US RE50,142 E

Page 2

Related U.S. Application Data					
(60)	Provisional application No. 60/950,563, filed on Jul. 18, 2007.		7,237,114	B1	6/2007 Rosenberg
			7,340,608	B2	3/2008 Laurie et al.
(58)	Field of Classification Search CPC ... G06F 40/174; G06Q 10/10; B23K 11/0053; B23K 11/14; B23K 9/206; B23P 19/006; B23P 19/062; G06N 3/0454; G06N 3/08; B63H 21/213; B63H 21/22; B63H 23/08; H04L 51/18; H04L 51/34 See application file for complete search history.		7,360,079	B2	4/2008 Wall
			7,395,436	B1	7/2008 Nemovicher
			7,424,543	B2	9/2008 Rice, III
			7,437,421	B2	10/2008 Bhogal et al.
			7,523,315	B2	4/2009 Hougaard et al.
			7,533,268	B1	5/2009 Catorcini et al.
			7,554,576	B2	6/2009 Erol
			7,562,053	B2	7/2009 Twining et al.
			7,568,101	B1	7/2009 Catorcini et al.
			7,568,104	B2	7/2009 Berryman et al.
			7,581,105	B2	8/2009 Dietl
			7,636,500	B1 *	12/2009 Arant G06Q 30/06 715/744
			7,657,832	B1	2/2010 Lin
			7,660,863	B2	2/2010 De Boursetty et al.
(56)	References Cited U.S. PATENT DOCUMENTS		7,788,259	B2	8/2010 Patterson et al.
			7,934,098	B1	4/2011 Hahn et al.
			7,953,977	B2	5/2011 Maruyama et al.
			8,103,867	B2	1/2012 Spitz
			8,132,013	B2	3/2012 Meier
			8,286,071	B1	10/2012 Zimmerman et al.
			8,588,483	B2	11/2013 Hicks et al.
			8,612,349	B1	12/2013 Ledder et al.
			8,650,038	B2	2/2014 Peirson, Jr. et al.
			8,655,961	B2	2/2014 McCabe et al.
			8,949,706	B2	2/2015 McCabe et al.
			9,634,975	B2	4/2017 McCabe et al.
			10,198,418	B2	2/2019 McCabe et al.
			2001/0018739	A1	8/2001 Anderson et al.
			2001/0034739	A1	10/2001 Anecki et al.
			2001/0034835	A1	10/2001 Smith
			2002/0004800	A1	1/2002 Kikuta et al.
			2002/0019937	A1	2/2002 Edstrom et al.
			2002/0026427	A1	2/2002 Kon et al.
			2002/0026582	A1	2/2002 Futamura et al.
			2002/0040431	A1	4/2002 Kato et al.
			2002/0069179	A1	6/2002 Slater et al.
			2002/0069358	A1	6/2002 Silvester
			2002/0099733	A1	7/2002 Teruuchi et al.
			2002/0129056	A1	9/2002 Conant et al.
			2002/0138445	A1	9/2002 Laage et al.
			2002/0143711	A1	10/2002 Nassiri
			2002/0162000	A1	10/2002 Benzler
			2002/0178187	A1	11/2002 Rasmussen et al.
			2002/0184485	A1	12/2002 Dray, Jr. et al.
			2002/0194219	A1	12/2002 Bradley et al.
			2002/0196478	A1	12/2002 Struble
			2003/0048301	A1	3/2003 Menninger
			2003/0051016	A1	3/2003 Miyoshi et al.
			2003/0056100	A1	3/2003 Beatson
			2003/0078880	A1	4/2003 Alley et al.
			2003/0120553	A1	6/2003 Williams
			2003/0120930	A1	6/2003 Simpson et al.
			2003/0131073	A1	7/2003 Lucovsky et al.
			2003/0140252	A1	7/2003 Lafon et al.
			2003/0217275	A1	11/2003 Bentley et al.
			2004/0006594	A1 *	1/2004 Boyer G06Q 10/10 709/204
			2004/0054606	A1	3/2004 Broerman
			2004/0078337	A1	4/2004 King et al.
			2004/0107352	A1	6/2004 Yui et al.
			2004/0117627	A1	6/2004 Brewington
			2004/0133493	A1	7/2004 Ford et al.
			2004/0181756	A1	9/2004 Berringer et al. G06F 21/64 713/176
			2004/0225884	A1	11/2004 Lorenzini et al.
			2004/0230891	A1	11/2004 Pravetz et al.
			2004/0250070	A1	12/2004 Wong
			2004/0255114	A1	12/2004 Lee et al.
			2004/0255127	A1	12/2004 Arnouse
			2005/0004885	A1 *	1/2005 Pandian G06F 17/30557
			2005/0033811	A1	2/2005 Bhogal et al.
			2005/0049903	A1	3/2005 Raja
			2005/0076215	A1	4/2005 Dryer
			2005/0091143	A1	4/2005 Schmidt et al.
			2005/0120217	A1	6/2005 Fifield et al.
			2005/0165626	A1	7/2005 Karpf

(56)

References Cited**U.S. PATENT DOCUMENTS**

2005/0182684 A1 8/2005 Dawson et al.
 2005/0182956 A1 8/2005 Ginter et al.
 2005/0192908 A1 9/2005 Jorimann et al.
 2005/0231738 A1 10/2005 Huff et al.
 2006/0047600 A1 3/2006 Bodenheimer et al.
 2006/0161780 A1 7/2006 Berryman et al.
 2006/0161781 A1 7/2006 Rice et al.
 2006/0174199 A1 8/2006 Soltis et al.
 2006/0205476 A1 9/2006 Jubinville
 2006/0259440 A1 11/2006 Leake et al.
 2006/0261545 A1 11/2006 Rogers
 2006/0294152 A1 12/2006 Kawabe et al.
 2007/0026927 A1 2/2007 Yaldoo et al.
 2007/0079139 A1 4/2007 Kim
 2007/0088958 A1 4/2007 Qa'Im-maqami
 2007/0118732 A1 5/2007 Whitmore
 2007/0130186 A1 6/2007 Ramsey et al.
 2007/0136361 A1 6/2007 Lee et al.
 2007/0143085 A1 6/2007 Kimmel
 2007/0165865 A1 7/2007 Talvitie
 2007/0198533 A1 8/2007 Foygel et al.
 2007/0208944 A1 9/2007 Pavlicic
 2007/0220260 A1 9/2007 King
 2007/0271592 A1 11/2007 Noda et al.
 2007/0289022 A1 12/2007 Wittkotter
 2008/0016357 A1 1/2008 Suarez
 2008/0034213 A1 2/2008 Boemker et al.
 2008/0097777 A1 4/2008 Rielo
 2008/0127307 A1* 5/2008 Fukuta G06F 21/608
 726/3
 2008/0141033 A1 6/2008 Ginter et al.
 2008/0209313 A1 8/2008 Gonser
 2008/0209516 A1 8/2008 Nassiri
 2008/0216147 A1 9/2008 Duffy
 2008/0235577 A1 9/2008 Veluchamy et al.
 2008/0260287 A1 10/2008 Berryman et al.
 2008/0313723 A1 12/2008 Naono et al.
 2009/0024912 A1 1/2009 McCabe et al.
 2009/0025087 A1 1/2009 Peirson, Jr. et al.
 2009/0044019 A1 2/2009 Lee et al.
 2009/0099881 A1 4/2009 Hanna et al.
 2009/0132351 A1 5/2009 Gibson
 2009/0138558 A1 5/2009 Benoit et al.
 2009/0138730 A1 5/2009 Cook et al.
 2009/0144552 A1 6/2009 Fort
 2009/0145958 A1 6/2009 Stoutenburg et al.
 2009/0185241 A1 7/2009 Nepomniachtchi
 2009/0268903 A1 10/2009 Bojinov et al.
 2009/0292786 A1 11/2009 McCabe et al.
 2010/0088364 A1 4/2010 Carter et al.
 2010/0122094 A1 5/2010 Shima
 2010/0153011 A1 6/2010 Obrea et al.
 2010/0217987 A1 8/2010 Shevade
 2010/0235727 A1 9/2010 Ashton et al.
 2010/0274863 A1 10/2010 Foygel et al.
 2010/0287260 A1 11/2010 Peterson et al.
 2010/0293094 A1 11/2010 Kolkowitz et al.
 2011/0093769 A1 4/2011 Dunn et al.
 2011/0119165 A1 5/2011 Zee
 2011/0126022 A1 5/2011 Sieberer H04L 9/3247
 713/180
 2011/0238510 A1 9/2011 Rowen et al.
 2011/0264907 A1 10/2011 Betz et al.
 2011/0314371 A1 12/2011 Peterson et al.
 2012/0180135 A1 7/2012 Hodges et al.
 2012/0209970 A1 8/2012 Scipioni et al.
 2012/0271882 A1 10/2012 Sachdeva et al.
 2012/0304265 A1 11/2012 Richter et al.
 2013/0019156 A1 1/2013 Gonser
 2013/0019289 A1 1/2013 Gonser et al.
 2013/0050512 A1 2/2013 Gonser et al.
 2013/0067243 A1 3/2013 Tamayo-rios et al.
 2013/0159720 A1 6/2013 Gonser et al.
 2013/0179676 A1 7/2013 Hamid
 2013/0254111 A1 9/2013 Gonser et al.

2013/0263283 A1 10/2013 Peterson et al.
 2014/0019761 A1 1/2014 Shapiro
 2014/0164542 A1 6/2014 McCabe et al.
 2014/0325324 A1* 10/2014 Trimble, Jr. G06Q 50/16
 715/205

FOREIGN PATENT DOCUMENTS

CA 2766745 1/2018
 CN 1159238 A 9/1997
 CN 1308803 A 8/2001
 CN 1719371 A 1/2006
 CN 101299256 A 11/2008
 CN 101346983 A 1/2009
 CN 104205122 A 12/2014
 EP 1238321 A1 9/2002
 JP 2000048072 A 2/2000
 JP 2003271529 A 9/2003
 JP 2005267438 A 9/2005
 JP 2008117258 A 5/2008
 JP 2008225527 A 9/2008
 KR 20000049674 A 8/2000
 KR 1020020092595 A 12/2002
 KR 1020070059931 A 6/2007
 KR 100929488 B1 12/2009
 KR 20090122657 A 12/2009
 RU 2291491 C2 1/2007
 RU 2300844 C2 6/2007
 RU 2400811 C2 9/2010
 RU 2400811 A1 12/2011
 WO WO-9607156 A1 3/1996
 WO 2003091834 A2 11/2003
 WO WO-03091834 A2 11/2003
 WO WO-2007075235 A1 7/2007
 WO WO-2008124627 A1 10/2008
 WO WO-2009012478 A2 1/2009
 WO WO-2009012478 A3 1/2009
 WO WO-2010105262 A1 9/2010
 WO 2010151630 A2 12/2010
 WO WO-2010151630 A3 12/2010

OTHER PUBLICATIONS

Brown et al., "Digital Signatures: Can They Be Accepted As Legal Signatures in EID?", Proceedings of the 1st ACM conference on Computer and communications security, Dec. 1, 1993, pp. 86-92.
 Elynx et al., "elynx Adds Workflow Management to Electronic Document Platform—new Workflow Capabilities Provide for Enhanced Electronic Loan Processing", Jan. 2009, 2 pp., URL: <http://www.elynx.com/news/view/82>.
 Harold, "XML Bible", IDG Books Worldwide, Inc., John Wiley & Sons, Mar. 1, 2004, pp. 191-192.
 Herzberg et al., "Surf 'N' Sign: Client Signatures on Web Documents", vol. 37, No. 1, 1998, pp. 61-71, URL: <https://www.proquest.com/openview/0af8fad8acbb44389aebeab903cf84c/1?pq-origsite=gscholar&cbl=35072>.
 International Preliminary Report on Patentability from International Application No. PCT/US2008/070566 dated Feb. 19, 2010, 5 pp.
 International Search Report of International Application No. PCT/US2008/070566 dated Feb. 19, 2009, 2 pp.
 Kamara et al., "Cryptographic Cloud Storage", Financial Cryptography and Data Security, Springer Berlin Heidelberg, Jan. 25, 2010, pp. 136-149.
 Kwok et al., "An Automatic Electronic Contract Document Signing System in a Secure Environment", Seventh IEEE International Conference on E-Commerce Technology, Jul. 19, 2005, pp. 497-502.
 Laurens Leurs et al., "The history of PDF", Feb. 14, 2010, 12 pp.
 Office Action from counterpart Canadian Application No. 2731116 dated Nov. 27, 2014, 3 pp.
 Prosecution History from U.S. Appl. No. 12/176,265, now issued U.S. Pat. No. 8,949,706, dated Sep. 7, 2011 through Dec. 16, 2014, 157 pp.

(56)

References Cited

OTHER PUBLICATIONS

Prosecution History from U.S. Appl. No. 14/537,713, now issued U.S. Pat. No. 10,198,418, dated Jan. 30, 2015 through Sep. 14, 2018, 97 pp.

Response to Office Action dated May 27, 2015, from counterpart Canadian Application No. 2731116 filed Nov. 27, 2014, 30 pp.

Su et al., "Signature-In-Signature Verification Via a Secure Simple Network Protocol", 2010 International Conference on Computational Intelligence and Software Engineering, IEEE, Dec. 10, 2010, 4 pp.

U.S. Appl. No. 16/229,126, filed Dec. 21, 2018, naming inventors McCabe et al.

Wheeler et al., "DocuSign Unveils new Scalable Product and Support Offerings of Electronic Signature and Electronic Contract Execution", DocuSign The fastest way to get a signature, Jan. 2008, 2 pp.

Written Opinion of International Application No. PCT/US2008/070566 dated Feb. 19, 2009, 4 pp.

Zefferer et al., "An Electronic-Signature Based Circular Resolution Database System", Proceedings of the 2010 ACM Symposium on Applied Computing, Mar. 22, 2010, pp. 1840-1845.

"U.S. Appl. No. 12/176,265, Advisory Action mailed Jul. 9, 2012", 3 pgs.

"U.S. Appl. No. 12/176,265, Final Office Action mailed Apr. 17, 2012", 13 pgs.

"U.S. Appl. No. 12/176,265, Final Office Action mailed Jul. 14, 2014", 22 pgs.

"U.S. Appl. No. 12/176,265, Non Final Office Action mailed Feb. 14, 2013", 15 pgs.

"U.S. Appl. No. 12/176,265, Non Final Office Action mailed Sep. 7, 2011", 11 pgs.

"U.S. Appl. No. 12/176,265, Non Final Office Action mailed Nov. 26, 2013", 17 pgs.

"U.S. Appl. No. 12/176,265, Notice of Allowance mailed Oct. 24, 2014", 9 pgs.

"U.S. Appl. No. 12/176,265, Notice of Allowance mailed Dec. 16, 2014", 2 pgs.

"U.S. Appl. No. 12/176,265, Response filed Feb. 26, 2014 to Non Final Office Action mailed Nov. 26, 2013", 12 pgs.

"U.S. Appl. No. 12/176,265, Response filed May 24, 2012 to Final Office Action mailed Apr. 17, 2012", 9 pgs.

"U.S. Appl. No. 12/176,265, Response filed Jul. 15, 2013 to Non Final Office Action mailed Feb. 14, 2013", 11 pgs.

"Application U.S. Appl. No. 12/176,265, Response filed Jul. 17, 2012 to Advisory Action mailed Jul. 9, 2012", 12 pgs.

"Application U.S. Appl. No. 12/176,265, Response filed Oct. 6, 2014 to Final Office Action mailed Jul. 14, 2014", 8 pgs.

"Application U.S. Appl. No. 12/176,265, Response filed Dec. 7, 2011 to Non Final Office Action mailed Sep. 7, 2011", 9 pgs.

"U.S. Appl. No. 12/490,602, Final Office Action mailed Apr. 1, 2013", 14 pgs.

"U.S. Appl. No. 12/490,602, Non Final Office Action mailed Jun. 28, 2012", 13 pgs.

"U.S. Appl. No. 12/490,602, Notice of Allowance mailed Oct. 9, 2013", 9 pgs.

"U.S. Appl. No. 12/490,602, Response filed Jul. 1, 2013 to Final Office Action mailed Apr. 1, 2013", 16 pgs.

"U.S. Appl. No. 12/490,602, Response filed Oct. 29, 2012 to Non Final Office Action mailed Jun. 28, 2012", 13 pgs.

"U.S. Appl. No. 14/179,507, Preliminary Amendment filed Jun. 6, 2014", 9 pgs.

"Australian Application Serial No. 2010264441, First Examiner Report mailed Sep. 25, 2014", 3 pgs.

"Canadian Application Serial No. 2,731,116, Office Action mailed Nov. 27, 2014", 3 pgs.

"Canadian Application Serial No. 2,731,116, Response filed May 27, 2015 to Office Action mailed Nov. 27, 2014", 30 pgs.

"eLynx Adds Workflow Management to Electronic Document Platform—new Workflow Capabilities Provide for Enhanced Electronic

Loan Processing", eLynx, [Online]. Retrieved from the Internet: <<http://www.elynx.com/news/view/82>>, (Jan. 2009), 2 pgs.

"European Application Serial No. 107926404, Examination Notification Art. 94(3) mailed Apr. 8, 2014", 8 pgs.

"European Application Serial No. 107926404, Extended European Search Report mailed Aug. 16, 2013", 8 pgs.

"European Application Serial No. 107926404, Office Action mailed Feb. 6, 2012", 2 pgs.

"European Application Serial No. 10792640.4, Response filed Mar. 12, 2014 to Extended European Search Report mailed Aug. 16, 2013", 14 pgs.

"European Application Serial No. 10792640.4, Response filed Aug. 18, 2014 to Examination Notification Art. 94(3) mailed Apr. 8, 2014", 15 pgs.

"International Application Serial No. PCT/US2008/070566, International Preliminary Report on Patentability mailed Feb. 19, 2010", 5 pgs.

"International Application Serial No. PCT/US2008/070566, International Search Report mailed Feb. 19, 2009", 2 pgs.

"International Application Serial No. PCT/US2008/070566, Written Opinion mailed Feb. 19, 2009", 4 pgs.

"International Application Serial No. PCT/US2010/039768, International Preliminary Report on Patentability mailed Jan. 12, 2012", 5 pgs.

"International Application Serial No. PCT/US2010/039768, International Search Report mailed Feb. 23, 2011", 3 pgs.

"International Application Serial No. PCT/US2010/039768, Written Opinion mailed Feb. 23, 2011", 4 pgs.

"Japanese Application Serial No. 2012-517717, Notification of Reasons of Refusal mailed Jan. 14, 2014", with English translation of claims, 5 pgs.

"Japanese Application Serial No. 2012-517717, Response filed Jun. 12, 2014", 12 pgs.

Borozdin, "DocuSign Connect Service Guide", DocuSign, Inc, (2008), 1-9.

Harold, Elliott Rusty, "XML Bible", IDG Books Worldwide, Inc., (1999), 191-192.

Herzberg, et al., "Surf'N'Sign: Client Signatures on Web Documents", IEEE, vol. 37 Issue 1., (1998), 61-71.

Kamara, et al., "Cryptographic Cloud Storage", Published in "Financial Cryptography and Data Security" Springer., (2010), 136-149.

Laurens, Leurs, "The history of PDF", Prepressure.com, (Feb. 14, 2010), 1-12.

Su, et al., "Signature-In-Signature Verification via a Secure Simple Network Protocol", IEEE, (2010), 1-4.

Wheeler, et al., "DocuSign Unveils new Scalable Product and Support Offerings of Electronic Signature and Electronic Contract Execution", DocuSign the Fastest Way to Get a Signature, (Jan. 2008), 1 pg.

Zefferer, et al., "An Electronic-Signature Based Circular Resolution Database System", ACM, (Mar. 2010), 1840-1845.

"U.S. Appl. No. 14/179,507, Final Office Action mailed Sep. 23, 2016", 6 pgs.

"U.S. Appl. No. 14/179,507, Non Final Office Action mailed Mar. 11, 2016", 11 pgs.

"U.S. Appl. No. 14/179,507, Notice of Allowance mailed Dec. 19, 2016", 6 pgs.

"U.S. Appl. No. 14/179,507, Response filed Jun. 13, 2016 to Non Final Office Action mailed Mar. 11, 2016", 12 pgs.

"U.S. Appl. No. 14/179,507, Response filed Nov. 22, 2016 to Final Office Action mailed Sep. 23, 2016", 9 pgs.

"Australian Application Serial No. 2010264441, Response filed Sep. 1, 2015 to Office Action mailed Sep. 25, 2014", 38 pgs.

"Australian Application Serial No. 2010264441, Response filed Sep. 29, 2015 to Subsequent Examiner Report mailed Sep. 3, 2015", 36 pgs.

"Australian Application Serial No. 2010264441, Subsequent Examiners Report mailed Sep. 3, 2015", 2 pgs.

"Canadian Application Serial No. 2,766,745, Office Action mailed Jun. 2, 2016", 5 pgs.

"Canadian Application Serial No. 2,766,745, Response filed Nov. 30, 2016 to Office Action mailed Jun. 2, 2016", 22 pgs.

(56)

References Cited

OTHER PUBLICATIONS

“Chinese Application Serial No. 201080035470.1, Office Action mailed Apr. 5, 2016”, w/English Translation, 24 pgs.

“Chinese Application Serial No. 201080035470.1, Response filed Oct. 19, 2016 to Office Action mailed Apr. 5, 2016”, w/English Claims, 13 pgs.

“Japanese Application Serial No. 2012-517717, Office Action mailed Oct. 28, 2014”, w/English Translation, 4 pgs.

“Japanese Application Serial No. 2012-517717, Response filed Nov. 6, 2014 to Office Action mailed Oct. 28, 2014”, w/English Translation, 10 pgs.

“Singapore Application Serial No. 10201403551T, Response filed Mar. 24, 2016 to Written Opinion mailed Oct. 28, 2015”, 6 pgs.

“Singapore Application Serial No. 10201403551T, Written Opinion mailed Oct. 28, 2015”, 10 pgs.

* cited by examiner

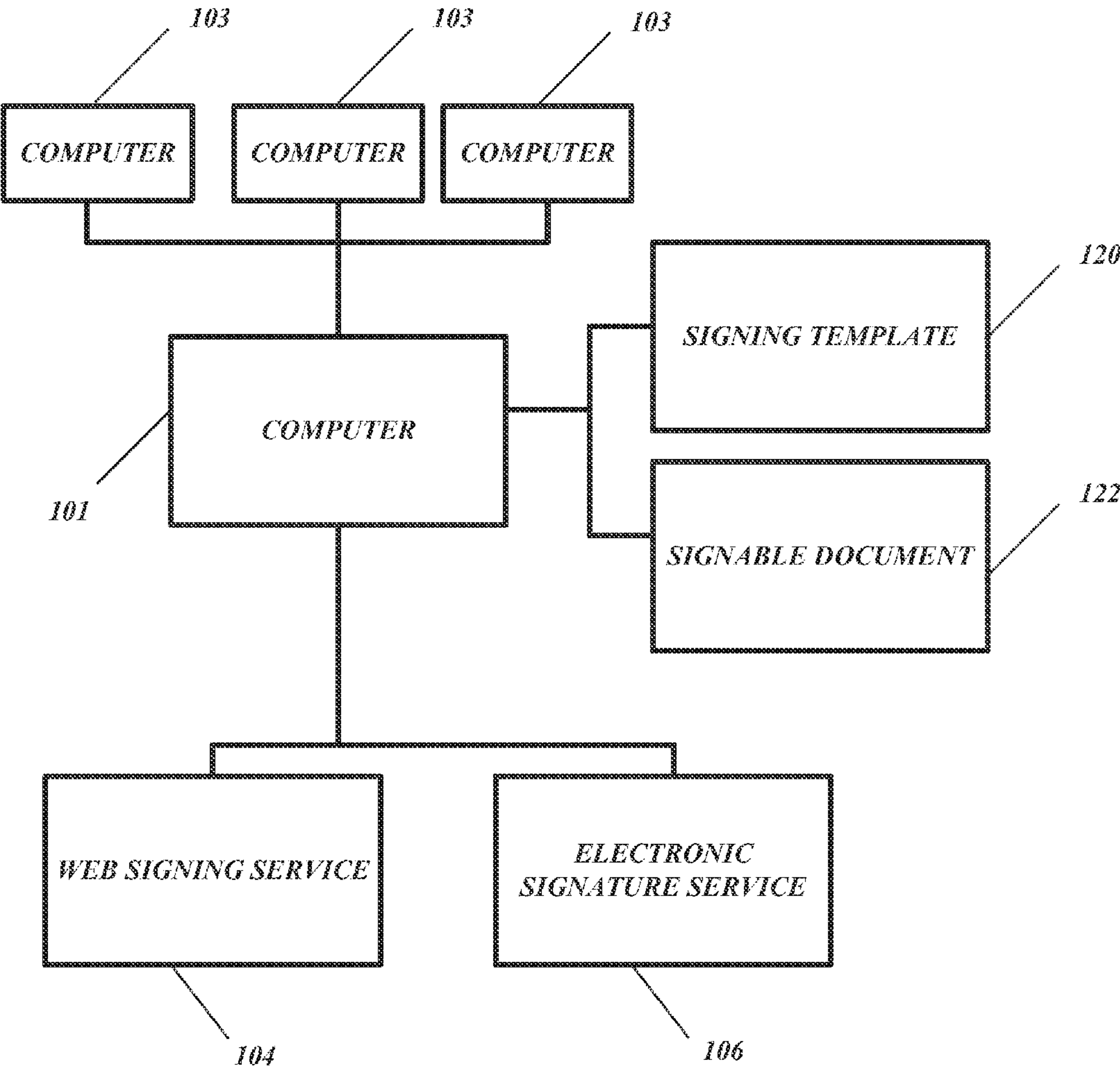


FIG. 1

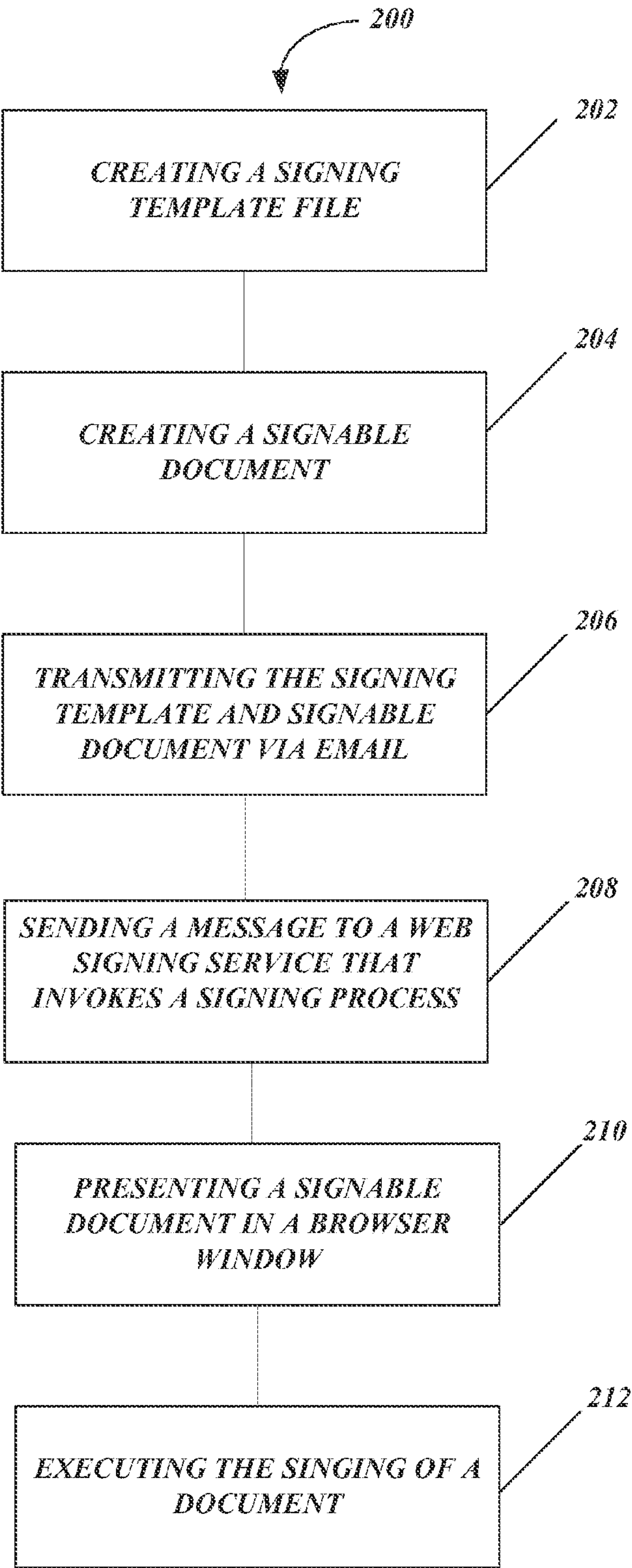


FIG. 2

SYSTEMS AND METHODS FOR DISTRIBUTED ELECTRONIC SIGNATURE DOCUMENTS

Matter enclosed in heavy brackets [] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue; a claim printed with strikethrough indicates that the claim was canceled, disclaimed, or held invalid by a prior post-patent action or proceeding.

[PRIORITY CLAIM] CROSS-REFERENCE TO RELATED APPLICATIONS

[This application is a continuation of U.S. application Ser. No. 12/176,265 filed on Jul. 18, 2008 and claims priority to and the benefit of the filing date of U.S. Provisional Application Ser. No. 60/950,563 filed on Jul. 18, 2007, the contents of which are incorporated by reference.] *This application is a reissue of U.S. Pat. No. 10,198,418, issued Feb. 5, 2019, filed as U.S. application Ser. No. 14/537,713 on Nov. 10, 2014, which application is a continuation application of application Ser. No. 12/176,265, filed Jul. 18, 2008, now U.S. Pat. No. 8,949,706, which claims priority to U.S. Provisional Application No. 60/950,563, filed Jul. 18, 2007.*

BACKGROUND OF THE INVENTION

Email is a popular way of transferring contract documents in the marketplace. Currently, there does not exist an effective system or method for a person to email a document or file to another person and have them fill-in and sign the document in such a way as to enforce a legally binding electronic signature process.

In order to create a legally binding document, the signer must be authenticated, the document may not be modified and the sequence of signing must be controlled. Standard email systems lack the control over any of these processes. One current method is emailing a PKI signed document. A PKI signed document can be cumbersome because it requires the document to be signed by the sender before it is distributed, then again by the signer when they sign the document, and further requires all parties to have special software and certificates to execute the process. This requirement that all parties pre-establish proper technology in order to execute a transaction adds extra burden and cost on both parties to the transaction, which severely limits acceptance of PKI in the marketplace.

Advanced electronic signature services such as DocuSign enable contracts to be signed with an esign-compliant signature process. However, this service lacks the ability to simply email the source document to a person to sign; it requires the signer to visit and authenticate before they sign the document. It further requires the sender to register each document with the service prior to sending it for signature.

SUMMARY OF THE INVENTION

A system and method for distributed electronic signature documents includes creating a signing template that contains information about how a signable document is to be signed, where the signatures are to be placed, who is to sign, and all activities that will be required to complete the transaction. A signable document is created and is then distributed by any means to a signer for signing. The signer opens the signable

document, provides any data being requested should the document have form fields, and initiates the signing process. When initiated, a secure message is sent to a web signing server to invoke the signing process. This process preferably validates the request for a signing and then, if valid, executes the signing process as defined by the signing template.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred and alternative embodiments of the present invention are described in detail below with reference to the following drawings:

FIG. 1 shows an example system for creation, processing and execution of distributed electronic signature documents; and

FIG. 2 shows a preferred method for distributed electronic signature documents.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Systems and methods for distributed electronic signature documents are disclosed herein. One embodiment of the present invention acts like a “Self Addressed Stamped Envelope” and allows a document to be sent for signature via email. Once the signer receives the document, he/she may fill in necessary fields prior to signing. When the signer is ready to sign, a control embedded in the document enables the signing process to be initiated and the signing managed by a web service. The web service authenticates the signer and ensures that the content of the contract can/cannot be modified (determined by the creator of the document). The service preferably enforces the workflow and sequencing of the document and adds any fields to the document that the signer added during review and execution. This approach allows any document to be distributed freely for signature via any means along with the ability to be electronically signed without the need for special software or certificates, and there is no requirement for the sender to take specific actions for each document, but rather allow the document to be distributed freely. In a preferred embodiment, the same signable document may be sent to hundreds of recipients via email, each of which may sign their copy, with the result being that all signed copies and all the data provided by the signed copies is securely captured and available to the sender.

FIG. 1 shows an example system **100** for creation, processing and execution of distributed electronic signature documents. The system **100** includes a single computer **101**, or includes a computer **101** in communication with pluralities of other computers **103**. The computer **101** is connected with a web signing service **104** and an electronic signature service **106** over a network such as the Internet. In one embodiment, a bank of servers, a wireless device, a cellular telephone and/or other data capture/entry device can be used in place of the computer **101**. An application program is run by the computer **101**, which then creates a signing template **120** and/or a signable document **122**. The computer **101** can include an application program that allows the signing template **120** and/or the signable document **122** to be sent for signature via email.

The signing template **120** is a file that preferably contains information about the signing process, locations, sequence and authentication. It contains linkages to any form fields in the signable document that will be used to fully execute the signing template. It may also contain information about the account holder and any limitations on the signing process. It

may identify other parties that will also sign, as well as any authentication requirements for any of the signers. The signable document **122** is a document file that preferably contains text and/or graphics along with a customizable control or link back to the signing template for execution. The web signing server **104** is a web server on the Internet that preferably hosts the application logic to correlate data transmitted by the embedded control in the signable document **122** with signing template **120** rule sets. An electronic signature service **106**, such as the existing DocuSign service, executes the signing template instructions through the web signing server.

FIG. **2** shows a method for distributed electronic signature documents **200** in one embodiment. At block **202** a document originator creates a signing template file that contains information about how a signable document is to be signed. A document originator may be a user, a party to a transaction, an agency or any entity interested in creating a signable document. The signing template file may include but is not limited to the location of signatures and initials for one or more signers; linkage between form fields in the actual document; information to be used to notify or authenticate the signer; information that may be used by decision systems to decide on different signature execution processes based on what is entered into the document during the signing process; the number of times the signable document can be executed; who will pay for the signature process; information governing whether the signable document content is modifiable by the signer; and other controlling information that may be changed or modified at any time by the sender who has access to it on the web server connected to the Internet. The signing template is preferably stored on a web signing server that is connected to the Internet.

In one embodiment, at block **204**, the document originator may create a signable document that is to be distributed to recipients for signing or viewing. The creation of the signing template and signable document preferably occurs in the same application, but may also occur in a different sequence and in different applications. The core signable document preferably includes an embedded control that provides information about the companion signing template. This information is similar to a secure hyperlink that enables the signer to click a button (“SDButton”) or a link in the signable document that contains information about how to connect over the Internet to the signing template for processing. The signable document is preferably paired with a signing template; however, there may be multiple signable documents relating back to one or more Signable Templates.

The document originator, at block **206**, transmits electronically the signing template and signable document to the signer. In an alternative embodiment, the signing template may be distributed via a simple hyperlink back to the signable document stored on a web server available to the Internet. When the signer is ready and when the SDButton is activated, at block **208**, a message is sent to the signing template on the web signing server, which invokes a signing process. This signing process preferably launches a procedure that validates the transaction and uploads the data provided by any form fields in the signable document to the web signing server and invokes a signing process that spawns a local web browser on the signer’s computer and begins a signing process as defined by the signing template.

After the signer has been authenticated by the system by any means defined in the signing template, at block **210** a version of the signable document that is created from the server is presented in the browser window. The signing process uses the current method of signing found in the

DocuSign service, but may accommodate alternative methods of signing found in similar services. At block **212**, the signer signs the document.

Preferably only the form field data from the signer is uploaded to the server and merged into the signing template (which contains the signable document copy). In this embodiment, the signers are not able to modify the underlying documents because this data is not used when the contract is presented to them during the signing process.

In an alternative embodiment, if the sender allows the content to be modified prior to submitting to the web signing server for signing, the entire signable document rather than only the field information is uploaded to the web signing server for handling through the signing process. In this embodiment, the modified document is displayed for the signer to sign in the web signing server.

In another embodiment, the sender does not allow the content to be modified and the entire document is posted to the web signing server for the signing process. Next, a document integrity validation occurs on the posted document to ensure that the underlying content has not been changed.

Once a signable document/signing template pairing has been created, the signable document can be used in many different ways to enable businesses to easily allow electronic signatures to be collected. The following provide non-limiting examples of alternative embodiments as may be desired or dictated by application requirements.

In one example, a business creates a signable document for the company 401k signing sheet and emails it to multiple employees. Each employee opens the file and fills in the form, clicking a button that may say “Sign.” The web signing server responds by presenting a web interface that authenticates and presents the document for signature for each employee and collects the signature and any data provided.

In another example, a business creates a signable document for a sales order form and creates the companion signing template, which requests that after the original signer has signed the document must be countersigned internally by two other people before being completed. To execute a sales transaction, the sales representative opens the document, enters in the data required for the sale, and sends the file to the signer for signature. The signer merely clicks the “Sign” button. The web signing server responds by presenting a web interface that authenticates and provides the document for signature to the first signer. Once the first signer has signed, the document is routed to the other two signers for signatures before it is completed.

A business creates a signable document that is unlocked (i.e. the content is changeable) for the company consulting agreement, and a signing template with instructions about the signing process, which ensures the company signer signs second. This contract is edited by both the company and consultant several times before it is deemed to be the final copy. Once the final copy is reached, either party may click the “Submit for Signature” link or button and the web signing server manages the signing process.

A company has an “Account Setup Form” that currently prospects download, print and fill out manually, and faxing the form back to the company for account setup. Using the systems and methods described herein, the sender company creates the form as a signable document linked to a signing template that defines the signing process for opening an account. When the user clicks on a hyperlink on a web page that says “Open Account,” the form is displayed in the browser window, and the user fills out the form using all

5

form fields defined in the signable document (for example a PDF form). When the user clicks "Sign" the web signing server executes the signing process for the document.

While the preferred embodiment of the invention has been illustrated and described, as noted above, many changes can be made without departing from the spirit and scope of the invention. Accordingly, the scope of the invention is not limited by the disclosure of the preferred embodiment, but to the invention as described above and illustrated in the exemplars shown below.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method for distributed electronic signature documents comprising:
 - generating a signing template [that contains] *specifying first* information about how a document file is to be signed, the *first* information [further] specifying locations within the document file for signatures of one or more users, the *first* information further specifying whether content within the document file that is not modifiable by the one or more users;
 - [storing] *causing* the signing template *to be stored* on a server;
 - generating the document file to be emailed to the one or more users for signing, the document file displaying form fields configured to receive input information from the one or more users and an activatable control *embedded in the document file and comprising second information indicating the signing template, the activatable control being* configured to initiate an upload, over a network *and using the second information indicating the signing template*, of the input information to the signing template stored on the server, the content specified by the signing template not being modifiable by the one or more users through the generated document file;
 - emailing the document file to the one or users over the network;
 - receiving, from a client device of one of the one or more users, input information input into the form fields of the document file; and
 - [executing,] in response to activation of the activatable control by the client device, *causing* an electronic signing process defined by the signing template stored on the server *to be executed, wherein the electronic signing process comprises merging, with the signing template, the input information uploaded from the client device through activation of the activatable control of the document file.*
2. The method of claim 1, wherein executing the electronic signing process comprises:
 - merging, with the signing template, the input information uploaded from the client device through activation of the activatable control of the document file.]
3. The method of claim [2] 1, wherein [executing] the electronic signing process comprises:
 - causing presentation, on the client device, of a web browser displaying a modified version of the document file created from the merged signing template.
4. The method of claim 1, further comprising:
 - responsive to activation of the activatable control displayed in the document file, causing presentation, on the client device, of a login web interface; and
 - authenticating a user from *input* information input into the login web interface.

6

5. The method of claim 1, wherein the form fields and the activatable control are user interface (UI) elements of the document file that are displayable on a display device of the client device.

6. The method of claim 1, wherein the document file is a PDF (Portable Document Format) file, and wherein the [activatable control contains] *second information indicating the signing template specifies* a network link.

7. The method of claim 1 further comprising:

- in response to receiving a signature from the client device, automatically emailing the document file to an additional client device for an additional signature, the additional client device specified by a signing order in the signing template.

8. The method of claim 1, further comprising:

- validating the document file to ensure the content of the document file is not modified.

9. A system comprising:

- one or more processors of a machine; and
- a memory storing instructions that, when executed by the one or more processors, cause the machine to perform operations comprising:
 - generating a signing template [that contains] *specifying first* information about how a document file is to be signed, the *first* information [further] specifying locations within the document file for signatures of one or more users, the *first* information further specifying content the document file that not modifiable the one or more users;

[storing] *causing* the signing template *to be stored* on a server;

generating the document file to be emailed to the one or more users for signing, the document file displaying form fields configured to receive input information from the one or more users and an activatable control *embedded in the document file and comprising second information indicating the signing template, the activatable control being* configured to initiate an upload, over a network *and using the second information indicating the signing template*, of the input information to the signing template stored on the server, the content specified by the signing template not being modifiable by the one or more users through the generated document file;

emailing the document file to the one or users over the network;

receiving, from a client device of one of the one or more users, input information input into the form fields of the document file; and

[executing,] in response to activation of the activatable control by the client device, *causing* an electronic signing process defined by the signing template stored on the server *to be executed, wherein the electronic signing process comprises merging, with the signing template, the input information uploaded from the client device through activation of the activatable control of the document file.*

[10. The system of claim 9, wherein executing the electronic signing process comprises:

merging, with the signing template, the input information uploaded from the client device through the activation of activatable control of the document file.]

11. The system of claim [10] 9, wherein [executing] the electronic signing process comprises:

7

causing presentation, on the client device, of a web browser displaying a modified version of the document file created from the merged signing template, and wherein

the document file is a PDF (Portable Document Format) file, and wherein the [activatable control] *second information indicating the signing template* is a network link.

12. The system of claim 9, the operations further comprising:

responsive to activation of the activatable control displayed in the document file, [casing] *causing* presentation, on the client device, of a login web interface; and

authenticating a user from *input* information input into the login web interface.

13. The system of claim 9, the operations further comprising:

validating the document file to ensure the content of the document file is not modified.

14. A non-transitory computer readable storage device storing instructions that, when executed by a machine, cause the machine to perform operations comprising:

generating a signing template [that contains] *specifying first* information about how a document file is to be signed, the *first* information [further] specifying locations within the document file for signatures of one or more users, the *first* information further specifying content the document file that is not modifiable the one or more users;

[storing] *causing* the signing template *to be stored* on a server;

generating a document file to be emailed to the one or more users for signing, the document file displaying form fields configured to receive input information from the one or more users and an activatable control *embedded in the document file and comprising second information indicating the signing template, the activatable control being* configured to initiate an upload, over a network *and using the second information indicating the signing template*, of the input information to the signing template stored on the server, the content specified by the signing template not being modifiable by the one or more users through the generated document file;

8

emailing the document file to the one or users over the network;

receiving, from a client device of one of the one or more users, input information input into the form fields of the document file; and

[executing,] in response to activation of the activatable control by the client device, *causing* an electronic signing process defined by the signing template stored on the server *to be executed, wherein the electronic signing process comprises merging, with the signing template, the input information uploaded from the client device through activation of the activatable control of the document file.*

[15. The non-transitory computer readable storage device of claim 14, wherein executing the electronic signing process comprises:

merging, with the signing template, the input information uploaded from the client device through activation of the activatable control of the document file.]

16. The non-transitory computer readable storage device of claim [15] 14, wherein [executing] the electronic signing process comprises:

causing presentation, on the client device, of a web browser displaying a modified version of the document file created from the merged signing template.

17. The non-transitory computer readable storage device of claim 14, the operations further comprising:

responsive to activation of the activatable control displayed in the document file, causing presentation, on the client device, of a login web [interfact] *interface*; and

authenticating a user from *input* information input into the login web interface.

18. The non-transitory computer readable storage device of claim 14, wherein the document file is a PDF (Portable Document Format) file, and wherein the [activatable control contains] *second information indicating the signing template specifies* a network link.

19. The *non-transitory* computer readable storage device of claim 14, the operations further comprising:

in response to receiving a signature from the client device, automatically emailing the document file to an additional client device for an additional signature, the additional client device specified by a signing order in the signing template.

* * * * *