US008489868B2

(12) **United States Patent**
Yach et al.

(10) **Patent No.: US 8,489,868 B2**
(45) **Date of Patent: Jul. 16, 2013**

(54) **SOFTWARE CODE SIGNING SYSTEM AND METHOD**

(75) Inventors: **David P. Yach**, Waterloo (CA); **Michael S. Brown**, Waterloo (CA); **Herbert A. Little**, Waterloo (CA)

(73) Assignee: **Research In Motion Limited**, Waterloo, Ontario (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1974 days.

(21) Appl. No.: **10/381,219**

(22) PCT Filed: **Sep. 20, 2001**

(86) PCT No.: **PCT/CA01/01344**

§ 371 (c)(1),
(2), (4) Date: **Mar. 20, 2003**

(87) PCT Pub. No.: **WO02/25409**

PCT Pub. Date: **Mar. 28, 2002**

(65) **Prior Publication Data**

US 2004/0025022 A1 Feb. 5, 2004

Related U.S. Application Data

(60) Provisional application No. 60/234,152, filed on Sep. 21, 2000, provisional application No. 60/235,354, filed on Sep. 26, 2000, provisional application No. 60/270,663, filed on Feb. 20, 2001.

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.**
USPC **713/1**; 713/176; 713/187; 713/189; 719/328; 711/100

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,625,690 A 4/1997 Michel et al.
5,978,484 A 11/1999 Apperson et al.

(Continued)

FOREIGN PATENT DOCUMENTS

AU 9736815 2/1998
CN 1541350 10/2004

(Continued)

OTHER PUBLICATIONS

Adams, Carlisle. IDUP and SPKM: Developing Pubic-Key-Based APIs and Mechanisms for Communication Security Services. Proceedings of the Symposium on Network and Distributed System Security. Pub. Date: 1996. Relevant pp. 128-135. Found on the World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=492419.*

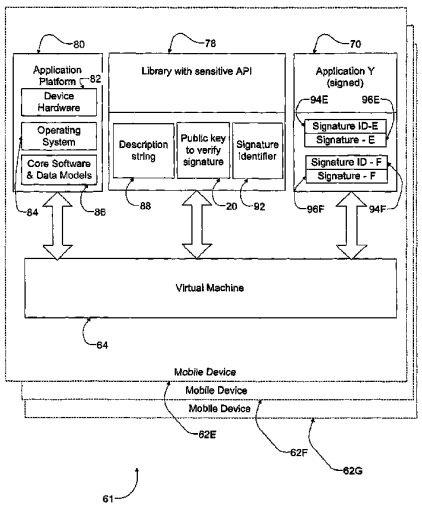
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Jon A. Gibbons; Fleit Gibbons Gutman Bongini & Bianco PL

(57) **ABSTRACT**

A code signing system and method is provided. The code signing system operates in conjunction with a signed software application having a digital signature and includes an application platform, an application programming interface (API), and a virtual machine. The API is configured to link the software application with the application platform. The virtual machine verifies the authenticity of the digital signature in order to control access to the API by the software application.

144 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

6,067,582	A	5/2000	Smith et al.	
6,157,721	A	12/2000	Shear et al.	
6,212,636	B1 *	4/2001	Boyle et al.	713/168
6,223,291	B1	4/2001	Puhl et al.	
6,233,683	B1 *	5/2001	Chan et al.	713/172
6,256,737	B1 *	7/2001	Bianco et al.	713/186
6,289,382	B1	9/2001	Bowman-Amuah	
6,324,650	B1 *	11/2001	Ogilvie	726/2
6,345,256	B1 *	2/2002	Milsted et al.	705/64
6,374,357	B1 *	4/2002	Mohammed et al.	726/5
6,390,374	B1 *	5/2002	Carper et al.	235/492
6,526,513	B1	2/2003	Shrader et al.	
6,574,609	B1 *	6/2003	Downs et al.	705/50
6,584,376	B1 *	6/2003	Van Kommer	700/245
6,587,837	B1 *	7/2003	Spagna et al.	705/52
6,697,948	B1 *	2/2004	Rabin et al.	726/30
6,748,541	B1 *	6/2004	Margalit et al.	726/9
6,766,353	B1	7/2004	Lin et al.	
6,795,919	B1 *	9/2004	Gibbs et al.	713/170
6,795,923	B1 *	9/2004	Stern et al.	726/12
6,895,507	B1 *	5/2005	Teppler	726/19
7,243,236	B1 *	7/2007	Sibert	713/179
2001/0044901	A1 *	11/2001	Grawrock	713/189
2002/0112078	A1	8/2002	Yach	
2002/0128036	A1	9/2002	Yach et al.	
2003/0026231	A1	2/2003	Lazaridis et al.	
2003/0159029	A1	8/2003	Brown et al.	
2004/0166834	A1	8/2004	Omar et al.	
2004/0170155	A1	9/2004	Omar et al.	
2004/0171369	A1	9/2004	Little et al.	
2004/0171374	A1	9/2004	Little et al.	
2004/0199665	A1	10/2004	Omar et al.	
2004/0202327	A1	10/2004	Little et al.	
2004/0205330	A1	10/2004	Godfrey et al.	
2005/0009502	A1	1/2005	Little et al.	

FOREIGN PATENT DOCUMENTS

CN	100573402	12/2009
CN	101694687	4/2010
CN	101694688	5/2010
CN	101714201	5/2011
EP	0930793	7/1999
EP	1320795	11/2005
EP	1626324	2/2006
EP	1626325	9/2010
EP	1626326	9/2010
EP	2278429	1/2011
EP	2284644	2/2011
EP	2306259	4/2011
EP	2306260	4/2011
HK	1055629	5/2006
HK	1091666	1/2007
HK	1091665	11/2010
HK	1091667	11/2010
WO	9905600	2/1999
WO	02/25409	3/2002

OTHER PUBLICATIONS

Communication of Notices of Opposition (R. 57(1) EPC) dated Sep. 26, 2006 and Working Translation, 16 pages.
ISO/IEC FCD 7816-9 "Identification cards . . . ", Part 9: Additional interindustry commands and security attributes, Jun. 17, 1999, S. 8 bis 13, 29 bis 31 (D5), 12 pages.
ISO/IEC FDIS 7816-8 "Identification cards . . . ", Part 8: Security related interindustry commands, Jun. 25, 1998, S. 2, 3, 6 bis 13 (D6), 13 pages.
ISO/IEC 7816-4 "Information Technology—Identification Cards . . . ", Part 4: Interindustry Commands for Interchange, 1995, S. 12 bis 16 (D7), 6 pages.
European Search Report issued on May 15, 2009 in connection with European Patent Application No. 05024662.8.
Rankl, Wolfgang, et al., Handbuch der Chipkarten, Aufbau—Funktionsweise—Einsatz von Smart Cards, Hanser, 1999—in German.
Notice of Abandonment. Canadian Application No. 2,422,917. Dated: Jun. 20, 2011.
First Office Action. Chinese Application No. 200910207911.0. Dated: Aug. 10, 2011.
Extended European Search Report. European Application No. 10186194.6. Dated: Jun. 22, 2011.
Communication Pursuant to Rules 70(2) and 70a(2) and Reference to Rule 39(1) EPC. European Application No. 10186194.6. Dated: Jul. 25, 2011.
Communication Pursuant to Article 94(3) EPC. European Application No. 10183655.9. Dated: Feb. 23, 2011.
Communication Pursuant to Article 94(3) EPC. European Application No. 10183655.9. Dated: Jul. 13, 2011.
Extended European Search Report (EESR). European Application No. 10183997.5. Dated: Dec. 12, 2010.
Communication Pursuant to Article 94(3) EPC. European Application No. 10183997.5. Dated: Feb. 23, 2011.
Communication Pursuant to Article 94(3) EPC. European Application No. 10183997.5. Dated: Jul. 14, 2011.
Extended European Search Report. European Application No. 10186296.9. Dated: Jun. 22, 2011.
Communication Pursuant to Rules 70(2) and 70a(2) and Reference to Rule 39(1) EPC. European Application No. 10186296.9. Dated: Jul. 25, 2011.
Invitation pursuant to Article 94(3) and Rule 71(1) EPC dated Sep. 28, 2011, European Patent Application No. 10186296.9.
First Office Action. Chinese Application No. 200910209311.8. Dated: Oct. 19, 2011.
Chinese Office Action dated Sep. 8, 2011, Chinese Patent Application No. 200910207912.5.
Notice of Abandonment. Canadian Application No. 2,422,917. Dated: Nov. 15, 2011.
Notice of Allowance. Canadian Application No. 2,422,917. Dated: Sep. 27, 2010.
Office Action. Canadian Application No. 2,422,917. Dated: Mar. 4, 2009.
Office Action. Canadian Application No. 2,422,917. Dated: Mar. 13, 2008.
Written Opinion. Application No. PCT/CA01/01344. Dated: May 28, 2002.
International Search Report. Application No. PCT/CA01/01344. Dated: Apr. 22, 2002.
Preliminary Examination Report. Application No. PCT/CA01/01344. Dated: Nov. 15, 2002.
Communication under Rule 51(4) EPC. European Application No. 01973901.0. Dated: May 6, 2005.
Communication of a notice of opposition. European Application No. 01973901.0. Dated: Aug. 21, 2006.
Observations to opposition. European Application No. 01973901.0. Dated: May 7, 2007.
Handbuch Der Chipkarten, "Sicherung der Datenubertragung".
Summons to attend oral proceedings pursuant to Rule 115(1) EPC. European Application No. 01973901.0. Dated: Mar. 20, 2008.
Provision of the minutes in accordance with Rule 124(4) EPC. European Application No. 01973901.0. Dated: Dec. 22, 2008.
Interlocutory decision in Opposition proceedings (Art. 101(3)(a) and 106(2) EPC). European Application No. 01973901.0. Dated: Dec. 22, 2008.
First Office Action (English translation). Chinese Application No. 01819200.9. Dated: Aug. 26, 2005.
Second Office Action (English translation). Chinese Application No. 01819200.9. Dated: May 30, 2008.
Rejection Decision (English translation). Chinese Application No. 01819200.9. Dated: Sep. 26, 2008.
Request for Reexamination. Chinese Application No. 01819200.9. Dated: Dec. 24, 2008.
Third Office Action (English translation). Chinese Application No. 01819200.9. Dated: Apr. 17, 2009.
Certificate of Invention Patent (English translation). Chinese Application No. 01819200.9. Dated: Dec. 23, 2009.
Noting of loss of rights pursuant to Rule 112(1) EPC. European Application No. 05024661.0. Dated: Dec. 16, 2011.
Communication under Rule 71(3) EPC. European Application No. 05024661.0. Dated: Jun. 29, 2011.

Extended European Search Report (EESR). European Application No. 05024661.0. Dated: May 15, 2009.
Communication under Rule 71(3) EPC. European Application No. 05024662.8. Dated: Feb. 10, 2010.
Extended European Search Report (EESR). European Application No. 05024663.6. Dated: May 15, 2009.
Communication under Rule 71(3) EPC. European Application No. 05024663.6. Dated: Feb. 10, 2010.
Extended European Search Report (EESR). European Application No. 10183655.9. Dated: Dec. 30, 2010.
Extended European Search Report (EESR). European Application No. 10183997.5. Dated: Dec. 21, 2010.
ISO/IEC 7816-4 Part 4: "Interindustry commands for interchange" XP002269400.
Office Action dated May 11, 2012 for U.S. Appl. No. 13/413,173.
Office Action dated Nov. 30, 2012 for U.S. Appl. No. 13/413,173.
Java Platform Standard Ed. 6, http://docs.oracle.com/javase/6/docs/apl/java/lang/reflect/Method_html (last visited Nov. 3, 2012).
Application programming interface, http://en.wikipedia.org/windex.php?title=Application_programming_interface&oldid=520968418 (last visited Nov. 3, 2012).
ETSI TS 123 057 v3.3.0 (Oct. 16, 2000).
Devanbu, P.T., et al., "Techniques for trusted software engineering." Proceedings of the 20th International Conference on Software Engineering, p. 126-135. Apr. 19-25, Kyoto, Japan.
ETSI TA 123 057 v3.2.0 (Jun. 23, 2000).

* cited by examiner

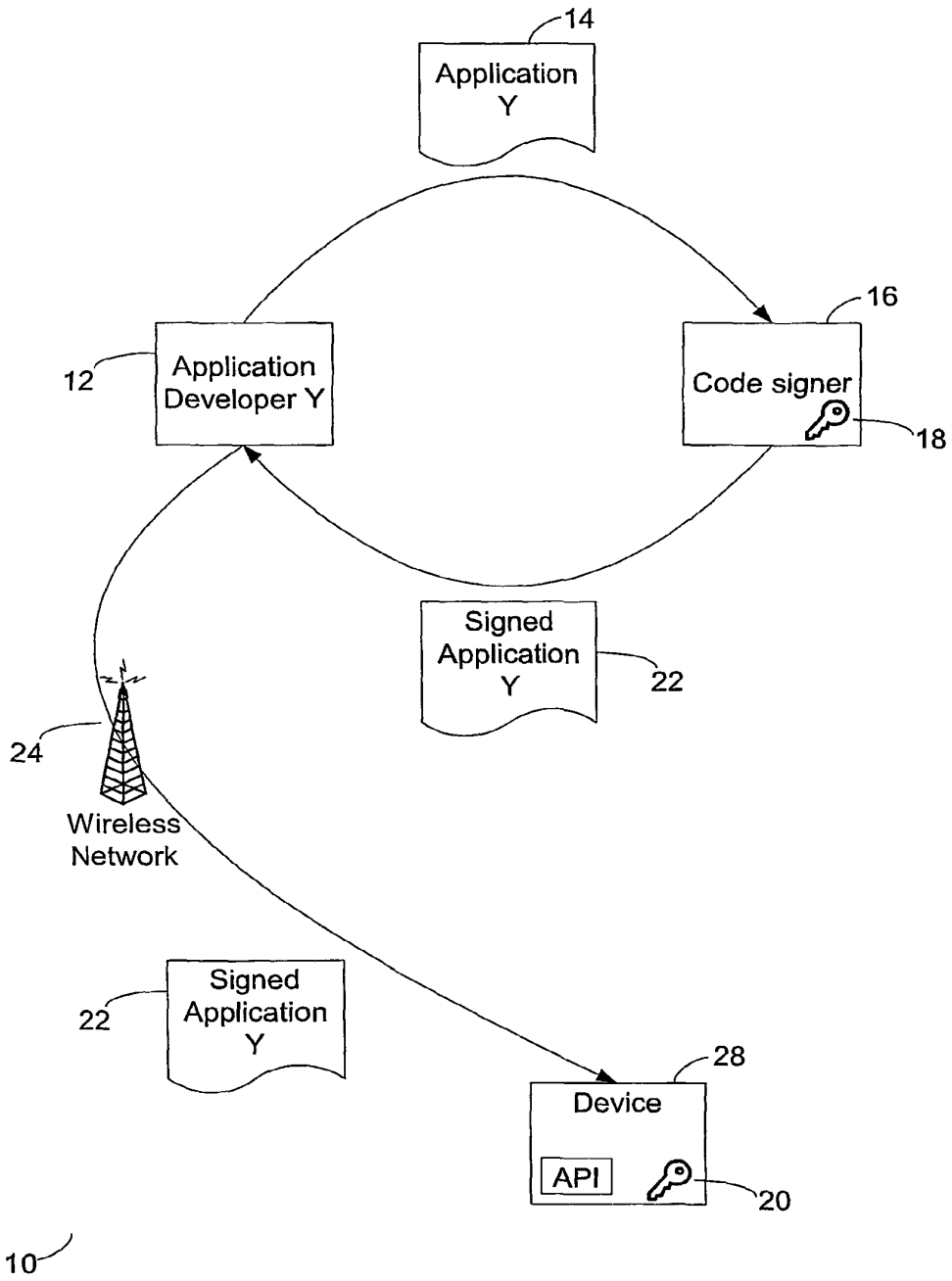
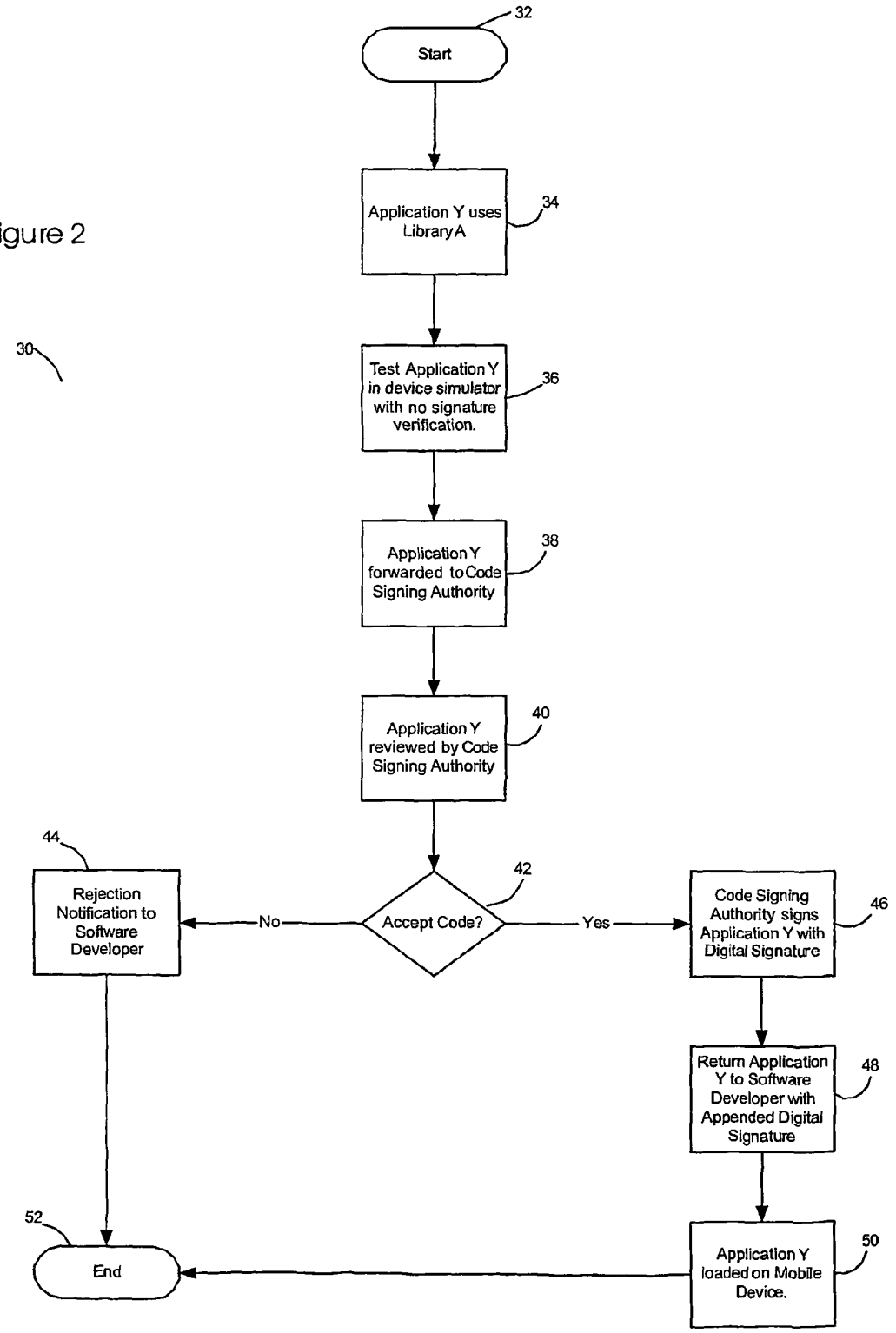


Figure 1

Figure 2



DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.