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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2014 (31.07.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/116740 A3

(51) **International Patent Classification**:
H04L 9/32 (2006.01)

(21) **International Application Number**:
PCT/US2014/012600

(22) **International Filing Date**:
22 January 2014 (22.01.2014)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
13/746,924 22 January 2013 (22.01.2013) US

(71) **Applicant**: **AMAZON TECHNOLOGIES, INC.** [US/US]; P.O. Box 8102, Reno, Nevada 89507 (US).

(72) **Inventors**: **ROTH, Gregory Branchek**; 410 Terry Ave. North, Seattle, Washington 98109-5210 (US). **POTLAPALLY, Nachiketh Rao**; 410 Terry Ave. North, Seattle, Washington 98109-5210 (US).

(74) **Agents**: **LOHR, Jason D.** et al.; Novak Druce Connolly Bove + Quigg LLP, 1000 Louisiana Street, Fifty-Third Floor, Houston, Texas 77002 (US).

(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))*

[Continued on next page]

(54) **Title**: PRIVILEGED CRYPTOGRAPHIC SERVICES IN A VIRTUALIZED ENVIRONMENT

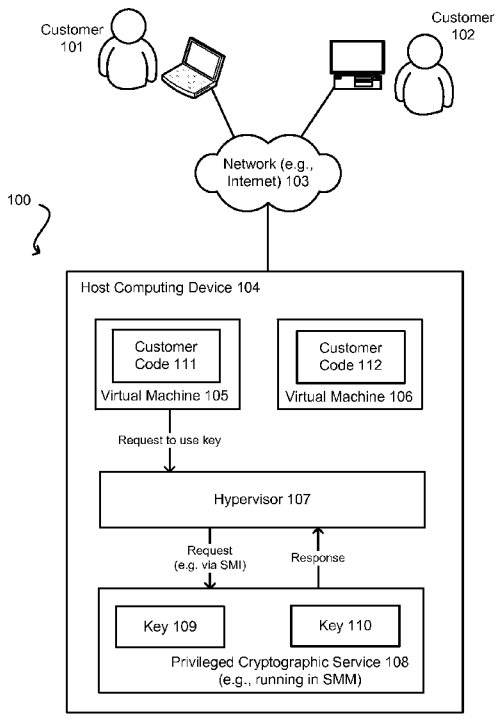

FIGURE 1

(57) **Abstract**: A privileged cryptographic service is described, such as a service running in system management mode (SMM). The privileged service is operable to store and manage cryptographic keys and/or other security resources in a multitenant remote program execution environment. The privileged service can receive requests to use the cryptographic keys and issue responses to these requests. In addition, the privileged service can measure the hypervisor at runtime (e.g., either periodically or in response to the requests) in an attempt to detect evidence of tampering with the hypervisor. Because the privileged service is operating in system management mode that is more privileged than the hypervisor, the privileged service can be robust against virtual machine escape and other hypervisor attacks.

WO 2014/116740 A3

WO 2014/116740 A3

(88) Date of publication of the international search report:
9 October 2014