

(51) International Patent Classification:
G06F 12/14 (2006.01)(21) International Application Number:
PCT/US2014/012605(22) International Filing Date:
22 January 2014 (22.01.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/746,780 22 January 2013 (22.01.2013) US(71) Applicant: **AMAZON TECHNOLOGIES, INC.**
[US/US]; P.O.Box 8102, Reno, Nevada 89507 (US).(72) Inventors: **BRANDWINE, Eric Jason**; 410 Terry Ave.
North, Seattle, Washington 98109-5210 (US). **WILSON,
Matthew Shawn**; 410 Terry Ave. North, Seattle, Washing-
ton 98109-5210 (US).(74) Agents: **LOHR, Jason D.** et al.; Novak Druce Connolly
Bove + Quigg LLP, 1000 Louisiana Street, Fifty-Third
Floor, Houston, TX 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))
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))

(54) Title: SECURING RESULTS OF PRIVILEGED COMPUTING OPERATIONS

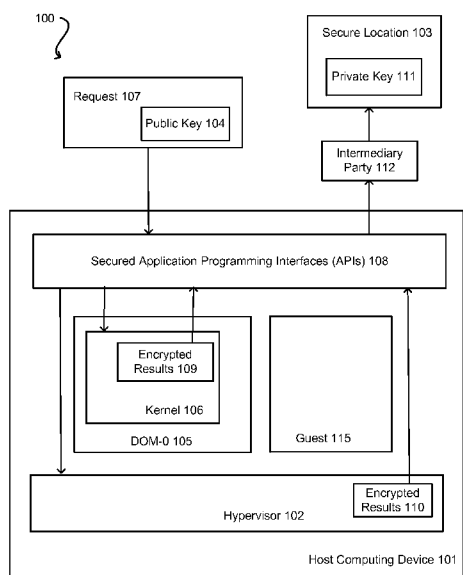


FIGURE 1

(57) **Abstract:** A formalized set of interfaces (e.g., application programming interfaces (APIs)) is described, that uses a security scheme, such as asymmetric (or symmetric) cryptography, in order to secure the results of privileged operations on systems such as the operating system (OS) kernel and/or the hypervisor. The interface allows a public key to be included into a request to perform a privileged operation on a hypervisor and/or kernel. The kernel and/or hypervisor use the key included in the request to encrypt the results of the privileged operation. In some embodiments, the request itself can also be encrypted, such that any intermediate parties are not able to read the parameters and other information of the request.