

(51) International Patent Classification:
G06F 15/16 (2006.01)(21) International Application Number:
PCT/US2012/058083(22) International Filing Date:
28 September 2012 (28.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/248,962 29 September 2011 (29.09.2011) US
13/248,953 29 September 2011 (29.09.2011) US
13/248,973 29 September 2011 (29.09.2011) US(71) Applicant (for all designated States except US):
AMAZON TECHNOLOGIES, INC. [US/US]; P.O. Box
8102, Reno, Nevada 89507 (US).

(72) Inventors; and

(71) Applicants (for US only): **ROTH, Gregory, B.** [US/US];
410 Terry Avenue North, Seattle, Washington 98109-5210
(US). **BEHM, Bradley, Jeffery** [CA/US]; 410 Terry Ave-
nue North, Seattle, Washington 98109-5210 (US). **CRA-
HEN, Eric, D.** [US/US]; 410 Terry Avenue North, Seattle,Washington 98109-5210 (US). **ILAC, Cristian, M.**
[US/US]; 410 Terry Avenue North, Seattle, Washington
98109-5110 (US). **FITCH, Nathan, R.** [US/US]; 410
Terry Avenue North, Seattle, Washington 98109-5210
(US). **BRANDWINE, Eric, Jason** [US/US]; 410 Terry
Avenue North, Seattle, Washington 98109-5210 (US).
O'NEILL, Kevin, Ross [CA/US]; 410 Terry Avenue
North, Seattle, Washington 98109-5210 (US).(74) Agents: **ADAMS, Scott, S.** et al.; Kilpatrick Townsend &
Stockton LLP, Two Embarcadero Center, 8th Floor, San
Francisco, California 94111 (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, 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, PA, 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.

[Continued on next page]

(54) Title: PARAMETER BASED KEY DERIVATION

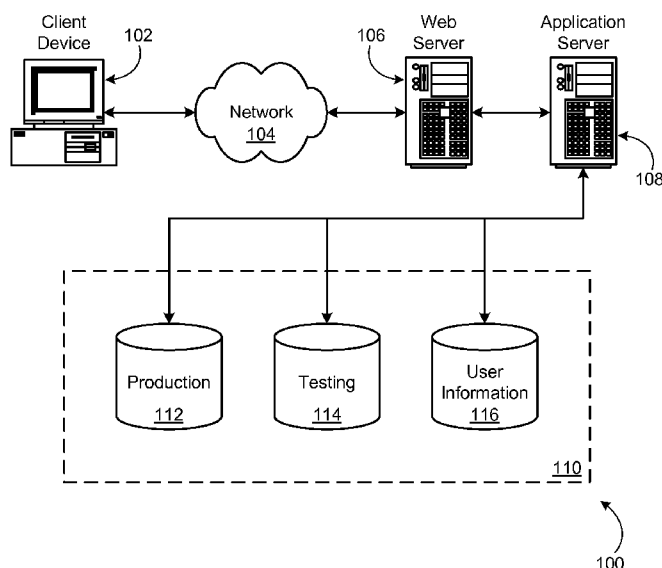


Figure 1

(57) Abstract: Systems and methods for authentication
generate keys from secret credentials shared
between authenticating parties and authenticators.
Generation of the keys may involve utilizing special-
ized information that, as a result of being used to
generate the keys, renders the generated keys usable
for a smaller scope of uses than the secret credential.
Further, key generation may involve multiple invoca-
tions of a function where each of at least a subset of
the invocations of the function results in a key that
has a smaller scope of permissible use than a key
produced from a previous invocation of the function.
Generated keys may be used as signing keys to sign
messages. One or more actions may be taken depend-
ing on whether a message and/or the manner in
which the message was submitted complies with re-
strictions of the key's use.



(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, 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))*