



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04W 12/02* (2009.01)
- (21) **International Application Number:**
PCT/EP2008/005960
- (22) **International Filing Date:**
21 July 2008 (21.07.2008)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/059,386 6 June 2008 (06.06.2008) US
- (71) **Applicant (for all designated States except US):** TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** NORRMAN, Karl [SE/SE]; Stigbergsgatan 32A, S-116 28 Stockholm (SE). NÄSLUND, Mats [SE/SE]; Stopvägen 95, S-168 36 Bromma (SE).
- (74) **Agent:** RÖTHINGER, Rainer; WUESTHOFF & WUESTHOFF, Schweigerstrasse 2, 81541 München (DE).
- (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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))

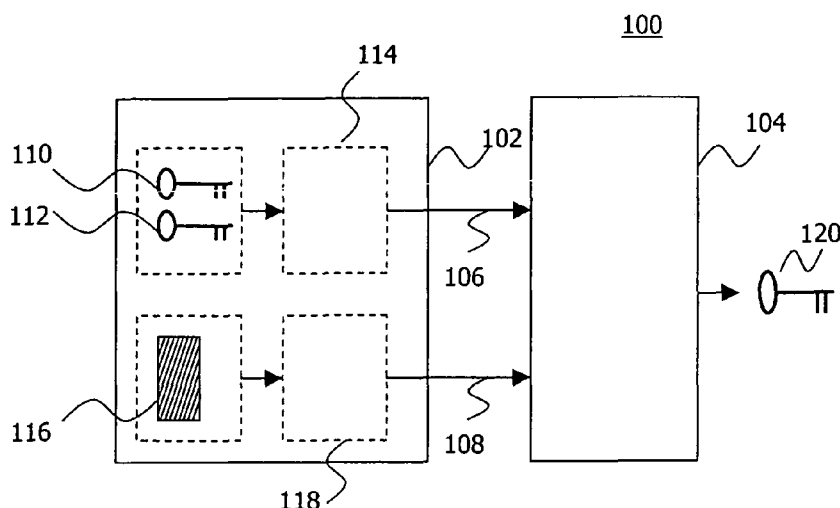
(54) **Title:** CRYPTOGRAPHIC KEY GENERATION

Fig. 3

(57) **Abstract:** A technique for generating a cryptographic key (120) is provided. The technique is particularly useful for protecting the communication between two entities (202, 302; 204, 304) cooperatively running a distributed security operation. The technique comprises providing at least two parameters (106, 108), the first parameter (106) comprising or deriving from some cryptographic keys (110, 112) which have been computed by the first entity (202, 302) by running the security operation; and the second parameter (108) comprising or deriving from a token (116) having a different value each time the security (114) operation is initiated by the second entity (204, 304) for the first entity (202, 302). A key derivation function is applied to the provided parameters (106, 108) to generate the desired cryptographic key (120).