

(51) International Patent Classification:
G06F 21/00 (2006.01)(21) International Application Number:
PCT/US2011/032036(22) International Filing Date:
12 April 2011 (12.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/323,248 12 April 2010 (12.04.2010) US
61/357,474 22 June 2010 (22.06.2010) US(71) Applicant (for all designated States except US): **INTER-DIGITAL PATENT HOLDINGS, INC.** [US/US]; 3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, DE 19810 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **CHA, Inhyok** [US/US]; 510 Southridge Circle, Yardley, PA 19067 (US). **SHAH, Yogendra, C.** [GB/US]; 10 Regency Court, Ex-ton, PA 19341 (US). **CASE, Lawrence** [US/US]; 5002 Timothy Circle, Austin, TX 78734 (US).(74) Agents: **SAMUELS, Steven, B.** et al.; WOODCOCK WASHBURN LLP, Cira Centre, 12th Floor, 2929 Arch Street, Philadelphia, PA 19104-2891 (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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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,

[Continued on next page]

(54) Title: STAGED CONTROL RELEASE IN BOOT PROCESS

(57) Abstract: Integrity validation of a network device may be performed. A network device comprising a secure hardware module, may receive a root key. The secure hardware module may also receive a first code measurement. The secure hardware module may provide a first key based on the root key and the first code measurement. The secure hardware module may receive a second code measurement and provide a second key based on the first key and the second code measurement. The release of keys based on code measurements may provide authentication in stages.

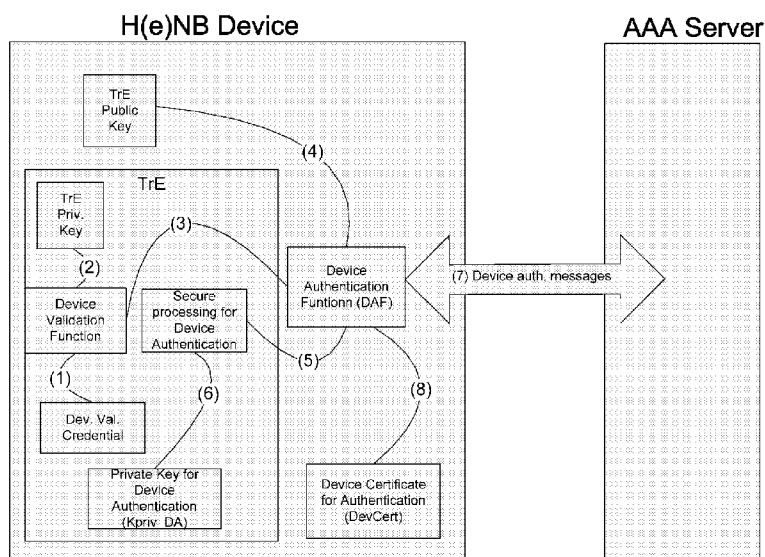


Figure 8. Binding between Validation and Certificate based Device Authentication for H(e)NB Device



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, —
GW, ML, MR, NE, SN, TD, TG).

*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))*

Published:

— *with international search report (Art. 21(3))*