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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 September 2005 (29.09.2005)

PCT

(10) International Publication Number
WO 2005/091551 A1

(51) International Patent Classification[7]: H04L 9/30

(21) International Application Number:
PCT/KR2005/000522

(22) International Filing Date: 25 February 2005 (25.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10-2004-0019446	22 March 2004 (22.03.2004)	KR
10-2004-0039382	31 May 2004 (31.05.2004)	KR
60/575,757	1 June 2004 (01.06.2004)	US

(71) Applicant *(for all designated States except US)*: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEE, Byung-rae** [KR/KR]; #306-104 Seongwon Santevill, Manhyun Maeul, Sanghyun-ri, Suji-eup, Yongin-si, Gyeonggi-do 449-130 (KR). **KIM, Tae-sung** [KR/KR]; #202 Goi Villat, 215-1, Sangdo 1-dong, Dongjak-gu, Seoul 156-031 (KR). **YOON, Joong-chul** [KR/KR]; 372-9, Suyu 2-dong, Gangbuk-gu, Seoul 142-877 (KR). **JUNG, Kyung-im** [KR/KR]; #310-2402 Jugong 3-danji, Neuti-maeul, 88, Jeongja-dong, Bundang-gu, Seongnam-si, Gyeonggi-do 463-744 (KR).

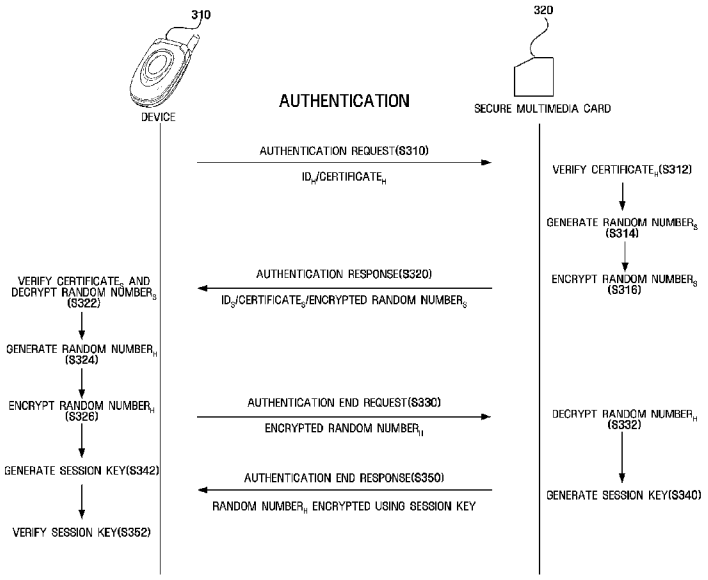
(74) Agents: **KIM, Dong-jin** et al.; 6th Fl. Youngpoong Bldg., 142, Nonhyun-dong, Gangnam-gu, Seoul 135-749 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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,

[Continued on next page]

(54) Title: AUTHENTICATION BETWEEN DEVICE AND PORTABLE STORAGE



(57) Abstract: For digital rights management (DRM), a method for performing authentication between a device and a portable storage, which is performed by the device, includes transmitting a first key to the portable storage, receiving a third key and a first encrypted random number obtained by encrypting a first random number using the first key from the portable storage and decrypting the first encrypted random number using a second key related with the first key, generating a second encrypted random number by encrypting a second random number using the third key and transmitting the second encrypted random number to the portable storage, and generating a session key using the first random number and the second random number. The technique guarantees secure authentication between the device and the portable storage for DRM.

WO 2005/091551 A1

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, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— *with international search report*