

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
15 July 2004 (15.07.2004)

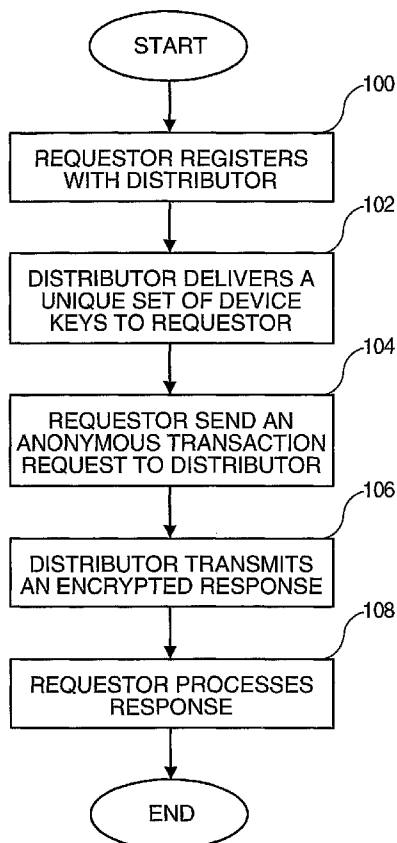
PCT

(10) International Publication Number
WO 2004/059588 A1

- (51) International Patent Classification⁷: **G07F 19/00**,
H04L 9/00, G07F 7/00
- (21) International Application Number:
PCT/EP2003/015040
- (22) International Filing Date:
19 December 2003 (19.12.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10/335,433 31 December 2002 (31.12.2002) US
- (71) Applicant (for MC only): **COMPAGNIE IBM FRANCE**
[FR/FR]; Tour Descartes- La Defense 5, 2, Avenue Gam-
betta, F-92400 Courbevoie (FR).
- (72) Inventors: **LOTSPIECH, Jeffrey, B.**; 2858 Hartwick
Pines Drive, Henderson, NV 89052 (US). **SRINIVASAN,**
Savitha; 7190 Silver Lode Lane, San Jose, CA 95120
(US). **SIGFREDO, Nin, I.**; 2150 Greenwood Avenue,
Morgan Hill, CA 95037 (US). **DALIT, Naor**; 4 Rosanes
Street, Tel-Aviv 69018 (US). **RAM, Reddy**; 89 Schreiner
Drive, North Wales, PA 19454 (US). **BLAKELEY, Bur-**
nette, D.; 205 Painted Fall Way, Cary, NC 27513-3529
(US).
- (74) Agent: **ZERBI, Guido**; Compagnie IBM France, Direc-
tion de la Propriété Intellectuelle, F-06610 La Gaude (FR).
- (71) Applicant (for all designated States except MC): **INTER-**
NATIONAL BUSINESS MACHINES CORPORA-
TION [US/US]; New Orchard Road, Armonk, NY 10504
(US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,

[Continued on next page]

(54) Title: METHOD FOR ENSURING PRIVACY IN ELECTRONIC TRANSACTIONS WITH SESSION KEY BLOCKS



(57) Abstract: A system, method, business method, and computer program product for conducting electronic transactions with a potentially untrusted server while maintaining user anonymity and transaction privacy, yet allowing the server to verify the user is a valid subscriber entitled to participate in the transaction. Anonymous service requests are sent to the server. The server transmits responses that have been encrypted such that only valid subscribers can decrypt them. Broadcast encryption schemes that enable selective revocation of misbehaving subscribers will tip off requestors that the server is trying to identify them. Transaction and content quantity can be monitored for usage-based billing while maintaining anonymity. Each content item may be uniquely encrypted with a content key that is then encrypted by a session key and included in encrypted form with a response, to reduce the computational workload.



LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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.