

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/075339 A1

(51) International Patent Classification:

H04L 29/06 (2006.01) **G07F 7/10** (2006.01)
G06F 21/00 (2006.01)

LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, 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.

(21) International Application Number:

PCT/IN2006/000013

(22) International Filing Date: 17 January 2006 (17.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

105/Del/2005 17 January 2005 (17.01.2005) IN

(71) Applicant and

(72) Inventor: **MATHUR, Seemant, Shankar** [IN/IN]; c/o
Y.B. Lall, L-11, Kailash Colony, New Delhi 110 048 (IN).

(74) Agents: **ANAND, Pravin** et al.; Anand And Anand Advoca-
tates, B-41 Nizamuddin East, New Delhi 110 013 (IN).

(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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,

(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, HU, IE, IS, IT, LT, LU, LV, 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).

Declarations under Rule 4.17:

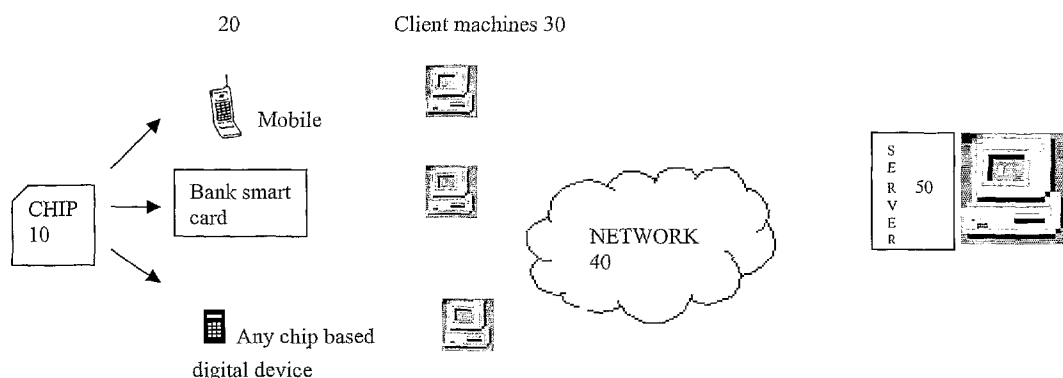
- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a
patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report
- 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 "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR SECURE AUTHENTICATION AND DATA EXCHANGE IN CLIENT SERVER AR-
CHITECTURE



(57) Abstract: The present invention relates to a method for secure authentication and data exchange, in client server architecture, comprising: registering a user and creating a first tabular data using the user's password for authentication of the user, at a server machine, deleting the password in its original form from the server, said server processing said first tabular data and generating a second tabular data to be sent to the client machine when said user logs in for a transaction at the client machine, said server initiating a communication session with the user using said second tabular data and generating a first set of numbers to be used for decryption by the server, encrypting and transferring said second tabular data to said user at the client machine, said client machine generating a second set of numbers to be used for encryption, using said second tabular data, said client encrypting the plain text using said second set of numbers, in a loop for a predetermined number of iterations, said client transmitting the encrypted data to the server, said server performing a decryption on the encrypted text using said first set of numbers, said server authenticating the user in the event correct plain text is generated, and said server completing the transaction.

WO 2006/075339 A1