PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/00 — A2

(11) International Publication Number: WO 00/67143

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/NL00/00278

(22) International Filing Date: 28 April 2000 (28.04.00)

(30) Priority Data:

99201334.2	28 April 1999 (28.04.99)	EP
09/543,602	5 April 2000 (05.04.00)	US

(71) Applicant *(for all designated States except US)*: UNICATE B.V. [NL/NL]; Gooimeer 3-15, NL-1411 DC Naarden (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: SIPMAN, Wilhelmus, Hendrikus, Maria [NL/NL]; Smidsweg 1A, NL-7433 BM Schalkhaar (NL). WARD, Scott, MacDonald [NL/NL]; Zuidlaan 31, NL-2111 GB Aerdenhout (NL).

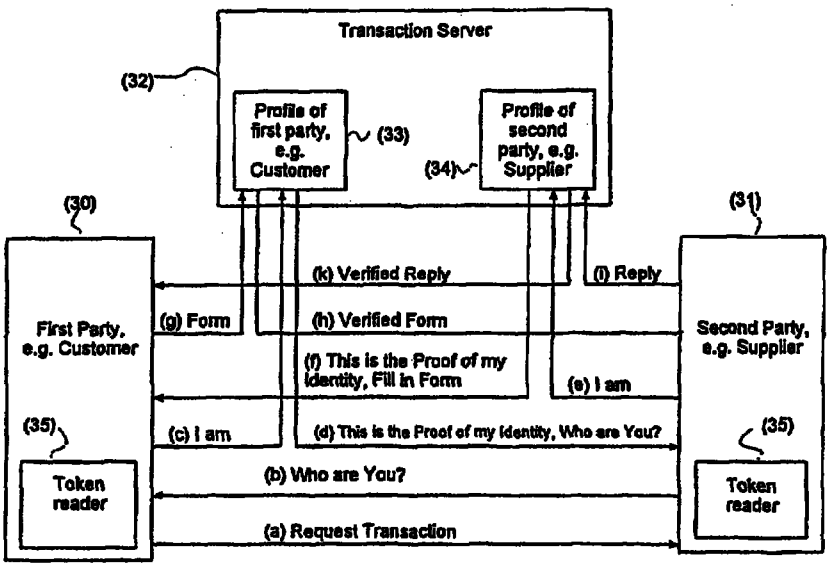
(74) Agent: H.V. MERTENS; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: TRANSACTION METHOD AND SYSTEM FOR DATA NETWORKS, LIKE INTERNET



(57) Abstract

A method and a system for performing a transaction between at least one first party and at least one second party are disclosed. A data network connects data input/output terminals of the parties. In the data network a secure and trusted transaction server is provided, in which a profile of the parties is registered, having a party identifier identifying a particular party, and authentication data for authenticating the party and data sent by the party. The parties communicate with each other through the transaction server by means of various transaction messages, which are digitally signed using a table of random numbers and a hashing operation, wherein the table of random numbers is generated by reading a token.