



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04K 1/00, H04L 9/00		A1	(11) International Publication Number: WO 99/57835
			(43) International Publication Date: 11 November 1999 (11.11.99)
(21) International Application Number: PCT/US99/09938 (22) International Filing Date: 5 May 1999 (05.05.99) (30) Priority Data: 60/084,257 5 May 1998 (05.05.98) US (71)(72) Applicant and Inventor: CHEN, Jay, C. [-/US]; 1335 Blackstone Road, San Marino, CA 91108 (US). (74) Agent: GELFOUND, Craig, A.; Christie, Parker & Hale, LLP, P.O. Box 7068, Pasadena, CA 91109-7068 (US).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, 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 With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.	
 *162162*		 *G00002*	

(54) Title: A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS

(57) Abstract

An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders (20), merchants (70), and service providers (SP) (60). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver's license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and random numbers are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP.

