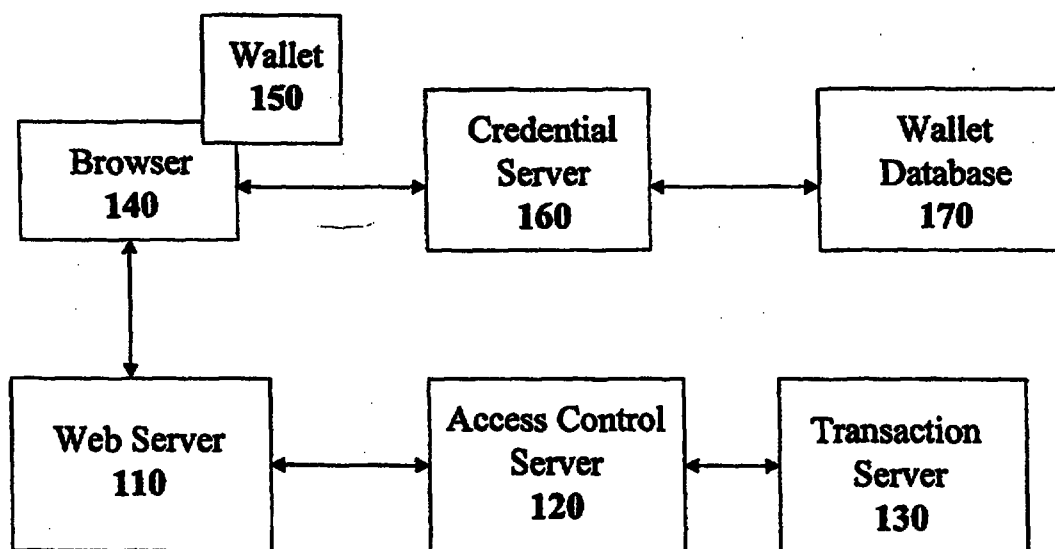




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04K 1/00	A1	(11) International Publication Number: WO 00/30285 (43) International Publication Date: 25 May 2000 (25.05.00)
<p>(21) International Application Number: PCT/US99/27621</p> <p>(22) International Filing Date: 19 November 1999 (19.11.99)</p> <p>(30) Priority Data: 09/196,430 19 November 1998 (19.11.98) US</p> <p>(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 08/996,758 (CIP) Filed on 23 December 1997 (23.12.97)</p> <p>(71) Applicant (for all designated States except US): ARCOT SYSTEMS, INC. [US/US]; 811 Hansen Way, Palo Alto, CA 94304-1023 (US).</p> <p>(72) Inventors; and (75) Inventors/Applicants (for US only): KAUSIK, Balas, Natara- jan [US/US]; 18079 Reed Knoll Road, Los Gatos, CA 95030 (US). VARADARAJAN, Rammohan [-/US]; 11674 Seven Springs Drive, Cupertino, CA 95014 (US).</p> <p>(74) Agents: LAURIE, Ronald, S. et al.; Skadden, Arps, Slate, Meagher & Flom LLP, 525 University Avenue, Palo Alto, CA 94301-1916 (US).</p>		<p>(81) Designated States: AU, CA, JP, NO, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Published <i>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.</i></p>

(54) Title: **METHOD AND APPARATUS FOR SECURE DISTRIBUTION OF AUTHENTICATION CREDENTIALS TO ROAMING USERS**



(57) Abstract

A roaming user (150) needing an authentication credential (e.g., private key) (230) to access a computer server (110) to perform an electronic transaction may obtain the authentication credential (230) in an on-demand fashion from a credential server (160) accessible to the user over a computer network. In this way, the user is free to roam on the network without having to physically carry his authentication credential (230). Access to the credential (230) may be protected by one or more challenge-response protocols involving simple shared secrets, shared secrets with one-to-one hashing (210), or biometric methods such as fingerprint recognition. If camouflaging is used to protect the authentication credential (230), decamouflaging may be performed either at the server (160) or at the user's computer (160).