

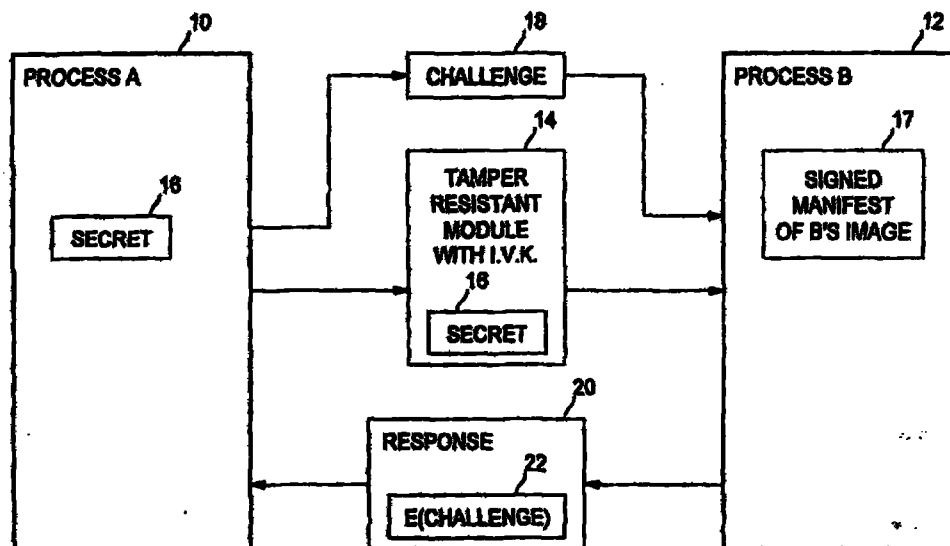


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/00, 9/14, 9/16, 9/28		A1	(11) International Publication Number: WO 99/31841
			(43) International Publication Date: 24 June 1999 (24.06.99)
(21) International Application Number: PCT/US98/25633 (22) International Filing Date: 12 December 1998 (12.12.98) (30) Priority Data: 08/989,615 12 December 1997 (12.12.97) US (71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US). (72) Inventor; and (75) Inventor/Applicant (for US only): MALISZEWSKI, Richard, L. [US/US]; 2218 12th Avenue, Forest Grove, OR 97116 (US). (74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).		(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), 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, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, 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.*

(54) Title: METHOD FOR STRONGLY AUTHENTICATING ANOTHER PROCESS IN A DIFFERENT ADDRESS SPACE



(57) Abstract

Authenticating a remote process (12) operating in an address space different than that of a local process (10) includes the steps of: creating, by the local process, a tamper resistant module (14) containing a temporary secret (16), sending the tamper resistant module and a challenge (18) from the local process to the remote process; executing the tamper resistant module by the remote process and recovering the secret when the integrity of the remote process is verified by the tamper resistant module; encoding the challenge using the secret to produce a response (20); sending the response to the local process; and decoding the response by the local process. Optionally, the tamper resistant module includes a request for information from the second process and the response includes the answer to the request for information.