



PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶: H04L 9/32	A1	(11) International Publication Number: WO 97/43842 (43) International Publication Date: 20 November 1997 (20.11.97)
(21) International Application Number: PCT/US97/08134 (22) International Filing Date: 13 May 1997 (13.05.97) (30) Priority Data: 08/645,759 14 May 1996 (14.05.96) US (71) Applicant: INTEGRIS SECURITY, INC. [US/US]; Suite 208, 1230 Oakmead Parkway, Sunnyvale, CA 94086 (US). (72) Inventor: KOCHER, Paul, Carl; 2103 Menalto Avenue, Menlo Park, CA 94025 (US). (74) Agent: LAURIE, Ronald, S.; McCutchen, Doyle, Brown & Enersen, Three Embarcadero Center, San Francisco, CA 94111 (US).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, 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, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
(54) Title: APPARATUS AND METHOD FOR DEMONSTRATING AND CONFIRMING THE STATUS OF DIGITAL CERTIFICATES AND OTHER DATA		
(57) Abstract		
<p>Methods and apparatuses are disclosed for providing cryptographic assurance as to whether a particular data item is on a list. Typically the data item would be a digital certificate and the list would specify revoked certificates. The list of data items is typically converted into a set of ranges in which no data items exist, then the ranges are used as leaf nodes to construct a hash tree using a cryptographic hash function. The root node of the hash tree is digitally signed. A cryptographic confirmation whether a particular item is on the list consists of the range including the item in question, the hash tree nodes necessary to reconstruct the root from the range, and the digital signature on the root node. Verification of the confirmation involves testing the digital signature on the root node and checking that the root node can be constructed from a leaf node whose range includes the item in question.</p>		
<pre> graph TD Start([Start]) --> 1101[Obtain interval hash tree with digitally signed root] 1101 --> 1102[Receive candidate data item] 1102 --> 1103[If necessary, process into form required by interval hash tree] 1103 --> 1104[Locate leaf node in hash tree whose range includes the candidate data item] 1104 --> 1105[Construct path from leaf node of hash tree to the root] 1105 --> 1106[Construct confirmation by aggregating: 1. The leaf spanning the candidate data item 2. The number of the leaf node in the tree 3. Intermediate node values cryptographically linking the leaf node to the root node 4. The signature on the root node] 1106 --> 1107[Issue confirmation] 1107 --> Finish([Finish]) </pre>		