

(19)



(11)

EP 1 391 073 B8

(12)

CORRECTED EUROPEAN PATENT SPECIFICATION

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 73

(51) Int Cl.:
H04L 29/06^(2006.01)

(86) International application number:
PCT/US2002/013521

(48) Corrigendum issued on:
05.09.2018 Bulletin 2018/36

(87) International publication number:
WO 2002/091662 (14.11.2002 Gazette 2002/46)

(45) Date of publication and mention
of the grant of the patent:
25.07.2018 Bulletin 2018/30

(21) Application number: **02729059.2**

(22) Date of filing: **30.04.2002**

(54) **METHOD AND SYSTEM FOR INCREASING SECURITY OF A SECURE CONNECTION**

VERFAHREN UND SYSTEM ZUR ERHÖHUNG DER SICHERHEIT EINER SICHEREN VERBINDUNG

PROCÉDÉ ET SYSTÈME D'AUGMENTATION DE LA SÉCURITÉ D'UNE CONNEXION SÉCURISÉE

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**

(30) Priority: **01.05.2001 US 287858 P**

(43) Date of publication of application:
25.02.2004 Bulletin 2004/09

(73) Proprietor: **OneSpan International GmbH
8152 Glattbrugg (CH)**

(72) Inventor: **COULIER, Frank
1850 Grimbergen (BE)**

(74) Representative: **Beck, Michaël Andries T. et al
IPLodge bvba
Technologielaan 9
3001 Heverlee (BE)**

(56) References cited:
**WO-A-00/07326 WO-A-98/25375
US-A- 5 602 918 US-B1- 6 173 400**

- **DIERKS CERTICOM C ALLEN CERTICOM T: "The TLS Protocol Version 1.0; rfc2246.txt" IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, 1 January 1999 (1999-01-01), XP015008030 ISSN: 0000-0003**
- **BOYEON SONG AND KWANG KIM: 'Comparison of existing key establishment protocols', 25 November 2000, CONFERNECE ON INFORMATION SECURITY & CRYPTOGRAPHY XP002954615 * page 1 - page 13 ***
- **MENEZES ALFRED, VAN OORSCHOT PAUL, VANSTONE SCOTT: 'Handbook of applied cryptography', 1997, CRC PRESS LLC XP002954614 * page 397 - page 405 ***
- **'Microsoft computer dictionary', 2002, MICROSOFT PRESS XP002954609 Fifth Edition, pages 93, 288, 429, 495, 522, 576**
- **"Upgrading to TLS within HTTP/1.1, R. KHARE, May 2000, XP002954612**
- **PERLMAN R., KAUFMAN C.: 'Analysis of the IPSec key exchange standard', June 2001, PROCEEDINGS TENTH IEEE INTERNATIONAL WORKSHOP ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES WET ICE 2001 XP002954613 * page 150 - page 156 ***

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 391 073 B8

- **ELTETO L., HUGHES J., CICOVIC N.: 'Token interoperability and portability', May 2002 XP002954608 * page 1 - page 21 ***
- **PARK J., SANDHU R.: 'Smart certificates: extending X.509 for secure attribute services on the web', October 1999, 22ND NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE XP002954616 * page 337 - page 348 ***
- **KAUFMAN C., PERLMAN R., SPECINER M.: 'Network security: private communication in a public world', 1995, PRENTICE-HALL INC. XP002954607 pages 223 and 249-253**

Remarks:

The file contains technical information submitted after the application was filed and not included in this specification