(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 December 2003 (11.12.2003)

PCT

(10) International Publication Number
WO 03/103251 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/IE03/00087

(22) International Filing Date: 30 May 2003 (30.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/384,083 31 May 2002 (31.05.2002) US

(71) Applicant *(for all designated States except US)*: **AEP SYSTEMS LIMITED** [IE/IE]; Bray Business Park, Southern Cross Route, Bray, County Wicklow, Ireland (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DO AMARAL CID, Carlos, Frederico** [BR/IE]; 52 Hampton Square, Navan Road, Dublin 7, Ireland (IE). **RYAN, Michael** [IE/IE]; Verbena House, Upper St. Columba's Road, Dublin 9 (IE). **MAHER, Thomas** [IE/IE]; 4 Glencairn Chase, Dublin 18 (IE).

(74) Agents: **O'BRIEN, John, A.** et al.; John A. O'Brien & Associates, Third Floor, Duncairn House, 14 Carysfort Avenue, Blackrock, County Dublin (IE).

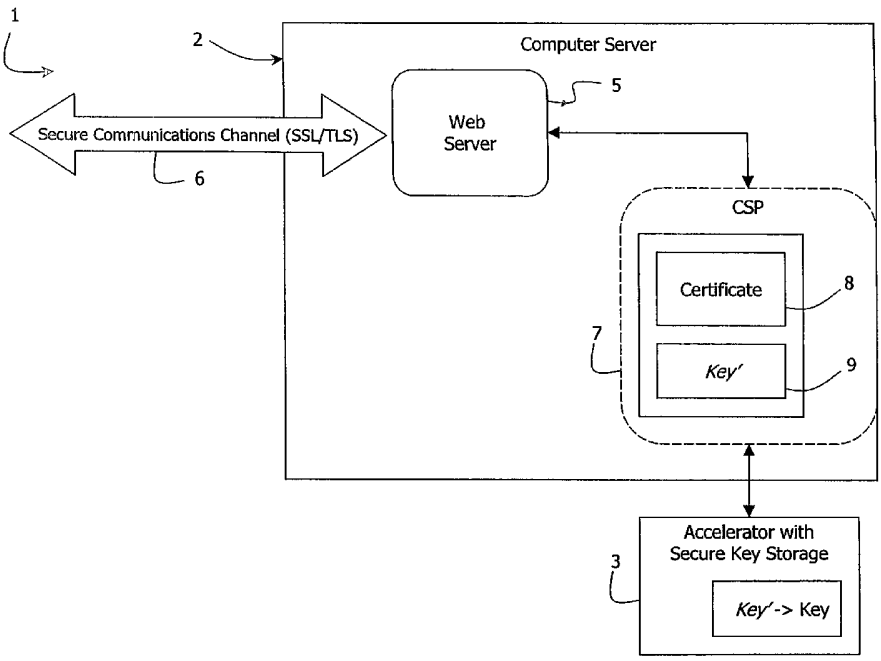
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

*[Continued on next page]*

(54) Title: CRYPTOGRAPHY KEY STORAGE




(57) Abstract: A computer server system has a server (2) and a separate accelerator (3). A cryptographic service provider (CSP, 8) within the server (2) performs all cryptography operations except those requiring use of a real cryptography key. For the latter, it passes a request to the accelerator (3) together with a pseudo key, which it stores in a manner similar to what is conventional for a real key. The accelerator (3) uses the pseudo key to retrieve the real key and perform the operation and return the result.

WO 03/103251 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

"Cryptography Key Storage"

## INTRODUCTION

### Field of the Invention

The invention relates to storage of cryptography keys.

### Prior Art Discussion

In one example, a server system has a Web server for communicating via the Internet on a secure communications channel (for example SSL/TLS) and uses a cryptographic service provider (CSP) to perform cryptographic operations. Implementation of a cryptography scheme by a system such as this requires storage of a private key. Heretofore, the private key has in many instances been stored on the computer's primary or secondary memory, either in plaintext or encrypted. In this situation the key is vulnerable to access by an attacker. Even if the key is encrypted, it may be decrypted off-line using brute-force or another method.

The invention is therefore directed towards providing improved cryptographic key storage and private key operations.

## SUMMARY OF THE INVENTION

According to the invention, there is provided a computer server system comprising:

a host server comprising an interface for communicating with external systems, and a cryptography system for performing cryptographic operations; and

a physically separate security device for storing a real cryptography key and for performing cryptographic operations with said real key in response to requests from the host server.

In one embodiment, the cryptography system of the host server performs all cryptography operations except those requiring use of the real key.

In another embodiment, the cryptography system stores a pseudo key and passes said pseudo key to the security device in a request for the security device to perform an operation with the real key.

In another embodiment, the cryptography system is not aware at the application level that the key it stores is a real key and the request to the security is made by a lower-level function.

In a further embodiment, the pseudo key has the same format as the real key.

In one embodiment, the cryptography system stores the pseudo key in a manner similar to that for a real key.

In another embodiment, the security device uses the received pseudo key to identify the real key.

In one embodiment, the security device processes the pseudo key to generate an address for the real key.

In another embodiment, security device hashes the pseudo key.

In a further embodiment, the security device is an exponentiation accelerator.

In another aspect, the invention provides a host server comprising a cryptography system for storing a pseudo cryptography key, and for passing a request to a physically separate security device for performance of a cryptography operation requiring use of a real cryptography key.

## DETAILED DESCRIPTION OF THE INVENTION

### Brief Description of the Drawings

The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only with reference to the accompanying drawing, Fig. 1, which is a diagram showing a computer server system of the invention.

### Description of the Embodiments

Referring to Fig. 1 a computer server system 1 comprises a server 2 linked to a separate key storage accelerator 3.

The server 2 comprises a Web server 5 which communicates on a secure SSL/TLS communications channel 6. The server 1 also comprises an internal cryptographic service provider (CSP) 7 which stores a certificate 8 and a pseudo key, *key'* 9. The pseudo key 9 is stored in the same manner as is conventional for a real key, and it has a similar format. However, the pseudo key 9 can not be used in valid cryptographic operations because it is not the real key. At the application level the CSP 7 is not aware that the pseudo key can not be used for cryptographic operations requiring a private key.

The accelerator 3 may be of the type described in our prior published PCT Patent Specification No. WO01/29652.

The accelerator 3 stores the real key, and also the pseudo key for addressing/identification purposes. All cryptography operations requiring use of the real key are performed by the accelerator 3, after requests incorporating the pseudo key are passed to it. These requests are generated at a low level in the CSP without application-level "knowledge". The server 1 also user the CSP 7 hosted internally to perform a large range of cryptographic operations which do not require use of the real key.

The accelerator 3 uses the received pseudo key to locate the real key by hashing the pseudo key to bring it down from say 1024 bits to 12 bits. The hash result is then used as an address for a look-up table to retrieve the real key. While not mentioned above the CSP 7 has a number of pseudo keys and the accelerator 3 has a number of corresponding real keys. Each key is for a different type of operation such as signing, encryption and decryption with different levels of security. The hash result provides access to the relevant real key.

It will be appreciated that the invention provides for a large range of cryptographic operations while at the same time allowing secure key storage. Unauthorised accesses only have access to the server 2, and if such an access retrieves the "key" it is only the pseudo key and so it is of no benefit to the hacker. The invention achieves major security benefits, while allowing a conventional crypto system to be used internally on the server, without it even needing to be aware at the application level that the keys it stores are only pseudo keys.

The invention is not limited to the embodiments described but may be varied in construction and detail. For example, the cryptography server 7 may store multiple certificates and keys.

Claims

1. A computer server system comprising:

a host server comprising an interface for communicating with external systems, and a cryptography system for performing cryptographic operations; and

a physically separate security device for storing a real cryptography key and for performing cryptographic operations with said real key in response to requests from the host server.

2. A computer server system as claimed in claim 1, wherein the cryptography system of the host server performs all cryptography operations except those requiring use of the real key.

3. A computer server system as claimed in claims 1 or 2, wherein the cryptography system stores a pseudo key and passes said pseudo key to the security device in a request for the security device to perform an operation with the real key.

4. A computer server system as claimed in claim 3 wherein the cryptography system is not aware at the application level that the key it stores is a pseudo key and the request to the security device is made by a lower-level function.

5. A computer server system as claimed in claims 3 or 4, wherein the pseudo key has the same format as the real key.

6. A computer server system as claimed in claims 4 or 5, wherein the cryptography system stores the pseudo key in a manner similar to that for a real key.

7. A computer server system as claimed in claims 3 to 6, wherein the security device uses the received pseudo key to identify the real key.

8. A computer server system as claimed in claim 7, wherein the security device processes the pseudo key to generate an address for the real key.

9. A computer server system as claimed in claim 8, wherein the security device hashes the pseudo key.

10. A computer server system as claimed in any preceding claim, wherein the security device is an exponentiation accelerator.

11. A computer server system substantially as described with reference to the drawing.

12. A host server comprising a cryptography system for storing a pseudo cryptography key, and for passing a request to a physically separate security device for performance of a cryptography operation requiring use of a real cryptography key.

1/1

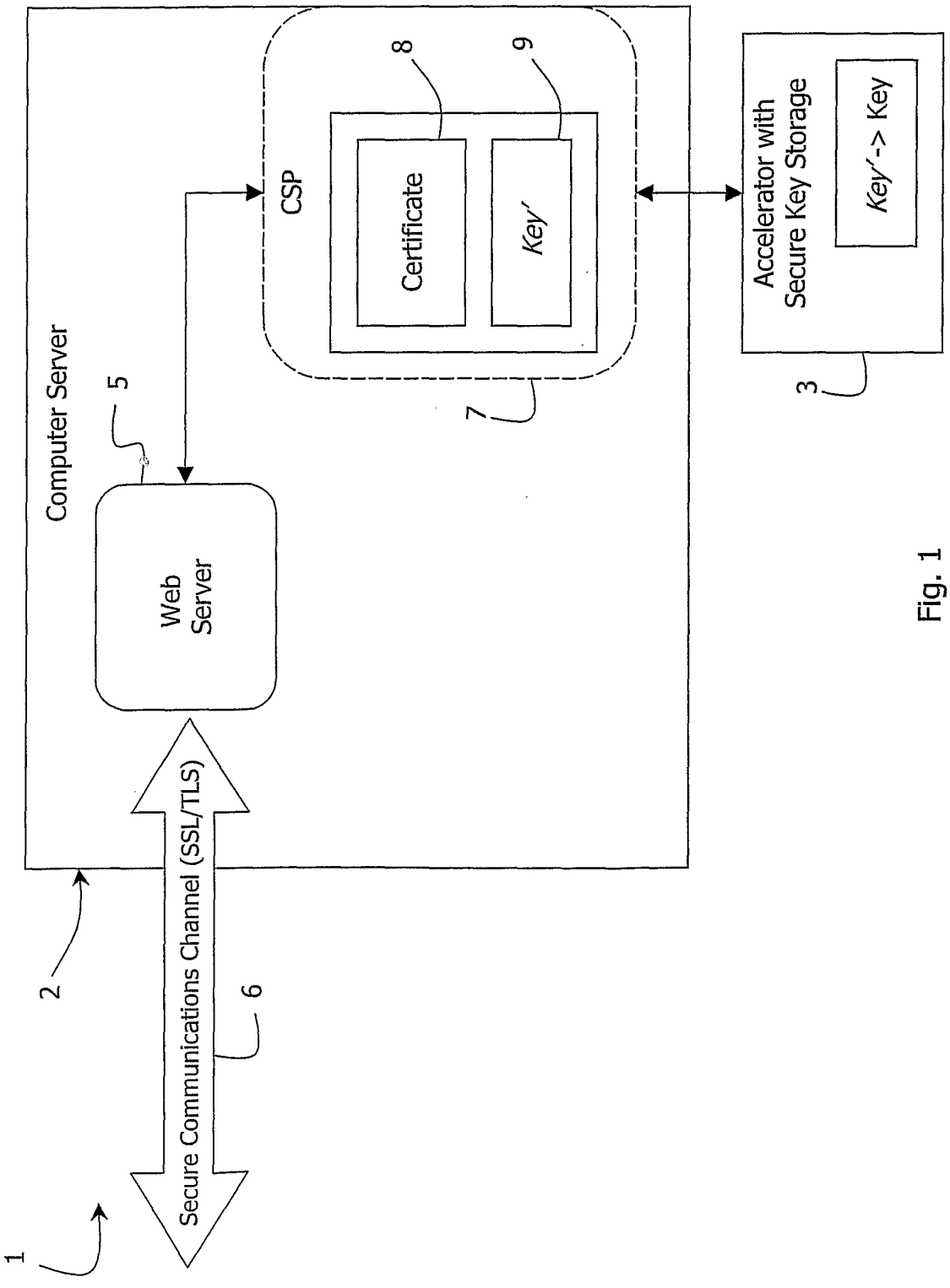

1
Secure Communications Channel (SSL/TLS)
2
6
Computer Server
5
Web Server
CSP
8
Certificate
9
Key'
7
Accelerator with Secure Key Storage
Key'-> Key
3

Fig. 1

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IE 03/00087

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 886 409 A (DIGITAL VISION LAB CORP)<br>23 December 1998 (1998-12-23)<br>column 3, line 36 -column 4, line 1<br>column 4, line 34 - line 40<br>column 7, line 33 -column 8, line 57 | 1-12 |
| A | US 5 940 510 A (BOLAN MICHAEL L ET AL)<br>17 August 1999 (1999-08-17)<br>column 5, line 38 - line 62 | 10 |
| A | US 5 764 766 A (SPRATTE MICHAEL)<br>9 June 1998 (1998-06-09)<br>abstract | 9 |

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 28 October 2003 | 05/11/2003 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Veen, G |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

**Information on patent family members**

International Application No
PCT/IE 03/00087

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0886409 A | 23-12-1998 | JP 10303880 A | 13-11-1998 |
| | | EP 0886409 A2 | 23-12-1998 |
| US 5940510 A | 17-08-1999 | US 5949880 A | 07-09-1999 |
| US 5764766 A | 09-06-1998 | NONE | |