PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04K 3/00 | A1

(11) International Publication Number: **WO 00/56000**

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/SE00/00475

(22) International Filing Date: 10 March 2000 (10.03.00)

(30) Priority Data:
9900887-2 12 March 1999 (12.03.99) SE

(71) Applicant *(for all designated States except US)*: BUSINESS SECURITY [SE/SE]; Box 11065, S-220 11 Lund (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BOGARVE, Jens [SE/SE]; Åkershus 21b, S-245 37 Staffanstorp (SE). OLSSON, Jörgen [SE/SE]; Ehrensvärdsgatan 20, S-212 13 Malmö (SE). ERIKSSON, Roger [SE/SE]; Hjärupskroken 8, S-245 62 Hjärup (SE). LINDE, Ove [SE/SE]; Ringvägen 6, S-247 32 Södra Sandby (SE).

(74) Agents: STRÖM, Tore et al.; Ström & Gulliksson AB, P.O. Box 4188, S-203 13 Malmö (SE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, 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).

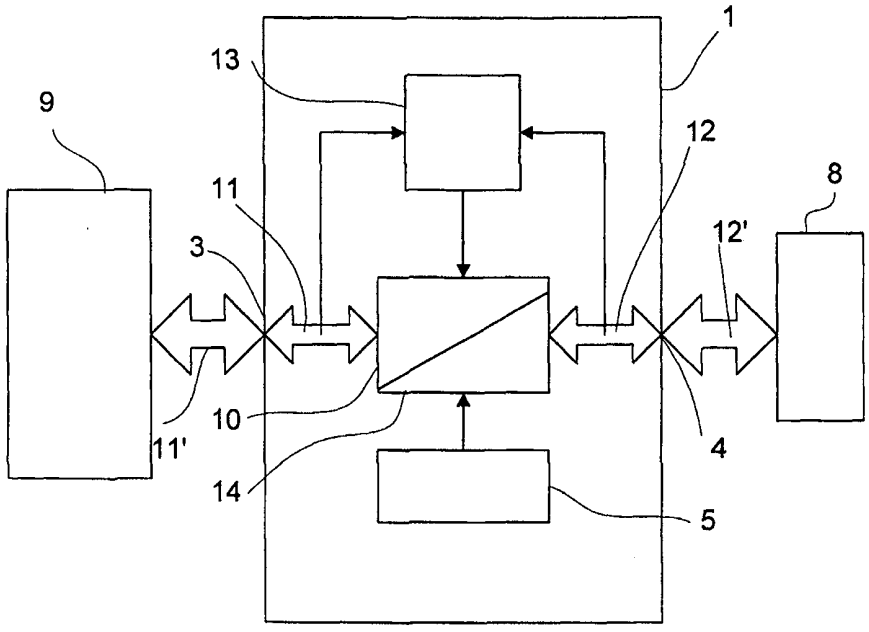
Published

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.

In English translation (filed in Swedish).

(54) Title: ENCRYPTION DEVICE



(57) Abstract

An encryption device for encryption of a data flow, comprising a PC-card part (2) having a data input (3) and a data output (4) for encrypted data. The PC-card part (2) comprises encryption means (10) for encryption of data on the PC-card bus (11, 12) and the data output (4) is operatively connected to a connection means for an external PC-card (8).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

TITLE: ENCRYPTION DEVICE

Technical Field

The present invention relates to an encryption device for encryption of a data flow, and more particularly to an encryption device comprising a PC-card, having a data input and a data output for encrypted data.

Prior Art

The increased use of computers in different networks for transmission of information involves at the same time an increased exposure of for example information of confidential nature, which the sender and receiver does not want to be available for unauthorized persons. This is a big problem, because it is relatively simple to tap data communication over different networks.

It is very difficult to keep unauthorized persons from tapping information being transmitted over the Internet, because the network is available for everyone, including persons acquiring secret information in an illegitimate way.

This problem can be solved by encryption of information, i.e. means for the sender and receiver to be able to transmit information over an insecure communication channel available for several users in a secure way. The security is achieved by means of a message en clair is translated into an encrypted text or a so-called cryptogram by means of a crypto and a key. The crypto can be an encryption algorithm known for a few or everyone while the key is known for authorized senders and receivers but unknown for other users, who have access to the same network. An unauthorized user encrypts a message with a key and then he transmits the encrypted message to an authorized receiver. In order to decode or decrypt the received message and

verify that the message is sent by an authorized sender, the user uses the current key. The encryption can be performed before the information is sent or in connection with the data stream passing the modem.

Laptop computers normally have card slots for connection to external hardware, such as different kinds of modems: analogue, ISDN, GSM; memory devices: hard disks, flash disks; or other kinds of interface cards for connection to the Ethernet, analogue or digital input and output signals. This kind of interface cards are called PC-cards or previously PCMCIA-cards.

During for example communication between a distance worker and his company network via the Internet or the public switched network, the transmitted information is internal and important information for the company. Often, it can be directly detrimental for the company if the information falls into wrong hands, and, therefore, it should be protected by encryption. A distance worker is often provided with a laptop computer, equipped with a modem to be able to work both at home and during business trips. For example, a modem can be a GSM or ISDN modem etc. on a PC-card for connection to a suitable network, for transmission of the information.

There are several prior art PC-cards with encryption functionality, which can be divided in two groups: PC-cards including only encryption functionality and PC-cards including encryption functionality and a modem. The main functionality of the first group can be described as a file and/or a hard disk encryption tool, and is not relevant for the present invention as it lacks communication possibilities via the modem. The integrated modem functionality of the latter group protects the calling modem connections in the first place.

Vkaart PCMCIA encryption card from Philips Crypto, Holland, is a PCMCIA-card providing a main functionality

for a modem crypto and PC-related security functions, such as access control to a PC or laptop computer, digital signatures in order to secure the authority of the user for what is communicated, and encryption of files on the computer, with optional smart card support.

The modem crypto from Philips Crypto and other prior art modem cryptos comprise a PC-card for encryption with an integrated modem. This delimits the possibilities for connection of the modem crypto, or the computer connected to the modem crypto, to a certain kind of network, determined by the kind of modem.

Summary of the Invention

The object of the present invention is to achieve an encryption device for encryption of a data flow between a computer and a PC-card, and decryption in the reverse direction, and to provide the possibility of connection of the encryption device to several kinds of networks in order to obtain a secure information transmission between a sender and a receiver over an insecure communication channel.

The object is achieved by an encryption device according to the present invention, comprising a PC-card part including encryption means/decryption means for encryption/decryption of data on the PC-card bus and a data output, which is operatively connected to connection means for an external PC-card.

An advantage of the encryption device according to the invention is that the communication between a computer, provided with the encryption device and a modem connected to its connection means for an external PC-card, and another computer, also provided with a corresponding encryption device in connection with the modem via the network, is encrypted in a simple and secure way.

Another advantage of the present invention is the possibility of changing the modem for other kinds of modems, for example for another communication medium.

The Drawings

The invention will be described in the following description with reference to the accompanying drawings, in which

FIG 1 is a schematic side view of an encryption device according to the present invention, and

FIG 2 is a block diagram illustrating the encryption device in FIG 1 connected to a computer and a PC-card modem.

Description

FIG 1 shows an encryption device 1 according to the present invention, including a PC-card or a PC-card part 2 having a data input 3 and a data output 4 for encrypted data, a reader/writer 5 for active cards 6 with an encryption key, wherein the reader/writer 5 is integrated with a keypad 7 for verification of a user of the active card 6. The encryption device 1 has a PC-card 2 such as a PCMCIA-card type II in this embodiment, which can be placed into a card slot of a computer for PC-cards with a corresponding terminal. The data output 4 is in turn operatively connected with a terminal in a card slot of the encryption device 1 for an external PC-card 8.

The block diagram in FIG 2 illustrates the encryption device 1 according to the invention connected to a computer 9, for example a laptop computer, and the external PC-card 8, a modem in the embodiment. The encryption device 1 has encryption means 10 for encryption of data, encrypting data by means of an encryption algorithm directly from the PC-card input bus 11, which is operatively connected to the data output 3. The encryption means 10 is connected to the

data output 4 through the output bus 12, said output being operatively connected to the connection means for an external PC-card. A filter 13 is operatively connected to the data input 3 via the input bus 11 of the PC-card 2 for wire tapping of the data flow, based on which the filter 13 activates and deactivates the encryption.

In order to obtain a required security in the encryption and the possibility for authorisation control, a key is required in addition to the crypto. The key is supplied from the active card 6 via the card reader/writer 5 in this embodiment to the encryption means 10, which is operatively connected to the card reader/writer 5.

Secret information to be securely transmitted from the computer 9 to a receiving computer is performed by the encryption device 1 according to the invention, connected to the PCMCIA-bus 11' of the computer 9, the PC-card modem connected to the encryption device 1, and an insecure communication channel available for several users and connected to the receiver. The security is obtained by means of the encryption device 1 being activated by a user, who put his active card 6 into the card reader/writer 5 and enters his authorisation code, a so-called PIN-code on the keypad 7. A correctly entered code results in the encryption key stored on the card 6 being read into the encryption device 10. A connection established by a call is initiated between the transmitter computer 9 and the receiver computer. The encryption device at the receiver computer automatically verifies that the key information of the calling computer 9 corresponds to the own information. If this verification is unsuccessful, the connection is interrupted and the line is automatically disconnected.

Regulation and control information for initialisation of the connection could usually not be encrypted. Therefore, the filter 13 taps the data flow and searches for known bit patterns for identification of regulation and

control information. Based on the identified information, the filter activates or deactivates the encryption function.

The information or the message from the computer is en clair and is translated in the encryption device 1 to a cryptogram by means of the crypto and a key in the encryption means. Then, the encrypted message is transmitted to the computer of the authorized receiver via the input bus 12, the data output 4, and the modem 8 placed in the card slot of the encryption device and its PCMCIA-bus 12'.

In order to decode or decrypt the received message and verify that the message is transmitted by an authorized sender, the user uses the current key.

Usually, the information transmission is duplex and the computer 9 therefore has to operate both as a transmitter and a receiver of encrypted information. Therefore, the encryption device 1 according to the invention also comprises decryption means 14 for decryption of received data from its external PC-card 8. During decryption, the data output 4 operates as input for encrypted input data and the data input 3 as output for decrypted data.

After a completed session, the user takes out his active card 6 from the card reader/writer 5. All secret information is stored on the card, and the encryption device 2 automatically deletes internal memory circuits in the encryption means 10 and the decryption means 14 after the card has been removed from the reader. This implies that the key always has to be loaded after the active card has been removed from the card reader/writer 5 or that the computer has been turned off. Since the encryption device 1 gets power supplied from the computer 9, it will be automatically turned off when the computer 9 is turned off.

Even though the invention has been described by way of an example thereof, it is apparent that the encryption device according to the present invention fulfils the aims

and advantages set forth above, and alternatives, modifications and variations of the invention are possible within the scope of the accompanying claims.

In alternative embodiments of the encryption device 1, the encryption key can be entered manually on the keypad 7, from a network through the connection means for the external PC-card 8, via the computer 9, or via an IR-connection.

Thus, the encryption device 1 according to the invention comprises a PC-card with a hardware based encryption. Encryption keys are supplied in several ways but preferably by a personal active card protected by a PIN-code. Additionally, the encryption device 1 provides functionality for encrypted information transmission through an analogue telecommunication network as well as GSM and ISDN. Examples of connectable external PC-cards 8 are the V90-, GSM-, ISDN-, XDSL- modem or a combination thereof. The flexibility of the construction facilitates a simple upgrade to future communication standards.

In another embodiment, the PC-card part 2 is provided with an interface terminal for connection to a serial port or a USB-port (Universal Serial Bus) of a desktop computer.

CLAIMS

1. An encryption device for encryption of a data flow, comprising a PC-card part (2) having a data input (3) and a data output (4) for encrypted data, **characterized** in that the PC-card part (2) comprises encryption means (10) for encryption of the data flow on the PC-card bus (11,12), and that the data output (4) is operatively connected to the connection means for transmission of encrypted data to an external PC-card (8).

2. A device according to claim 1, **characterized** in that a filter 13 is operatively connected to the data input (3) and the encryption device (10) for wire tapping of the data flow, based on which the filter (13) activates or deactivates the encryption.

3. A device according to claim 1 or 2, **characterized** in that a reader/writer (5) for active cards (6) with a encryption key is operatively connected to the PC-card part (2).

4. A device according to claim 3, **characterized** in that the reader/writer (5) is integrated with a keypad (7) for verification of the user of the active card (6).

5. A device according to any of the preceding claims, **characterized** in that a keypad (7) is operatively connected to the PC-card part (2) for manual input of the encryption key.

6. A device according to any of the preceding claims, **characterized** by means (1) for input of an encryption key from a network connectable to the external PC-card (8).

7. A device according to any of the preceding claims, **characterized** by means (1) for input of an encryption key from a computer (9) connectable to the PC-card part (2).

8. A device according to any of the preceding claims, **characterized** by means for input of a crypto key through an IR-connection at the encryption device (1), operatively connected to the encryption means (10).

9. A device according to any of the preceding claims, **characterized** in that the PC-card part (2) comprises decryption means (14) for decryption of an input data flow on the PC-card bus (11,12) from the connection means (4) for the external PC-card (8) for further transmission of a decrypted data flow to the data input (3).

10. A device according to any of the preceding claims, **characterized** in that the external PC-card (8) is a PCMCIA-modem.

11. A device according to claim 10, **characterized** in that the external PC-card (8) is a V90-, GSM-, ISDN-, or XDSL-modem or a combination thereof.

12. A device according to any of the claims 1-9, **characterized** in that the external PC-card (8) is a hard disk for storage of encrypted data.

13. A device according to any of the preceding claims, **characterized** in that the data input (3) is provided with an interface terminal for connection to a serial port or USB-port of a computer.

14. An encryption system for encryption of a data flow, comprising a computer (9) having a PC-card connection operatively connected to an encryption device, **characterized** by an encryption device (1) according to any of the preceding claims, and a PC-card (8) connected thereto.

1/1

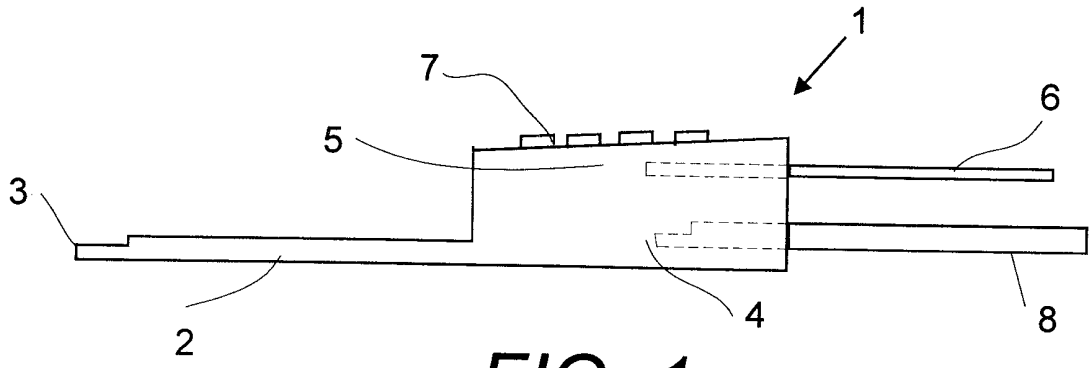


FIG. 1

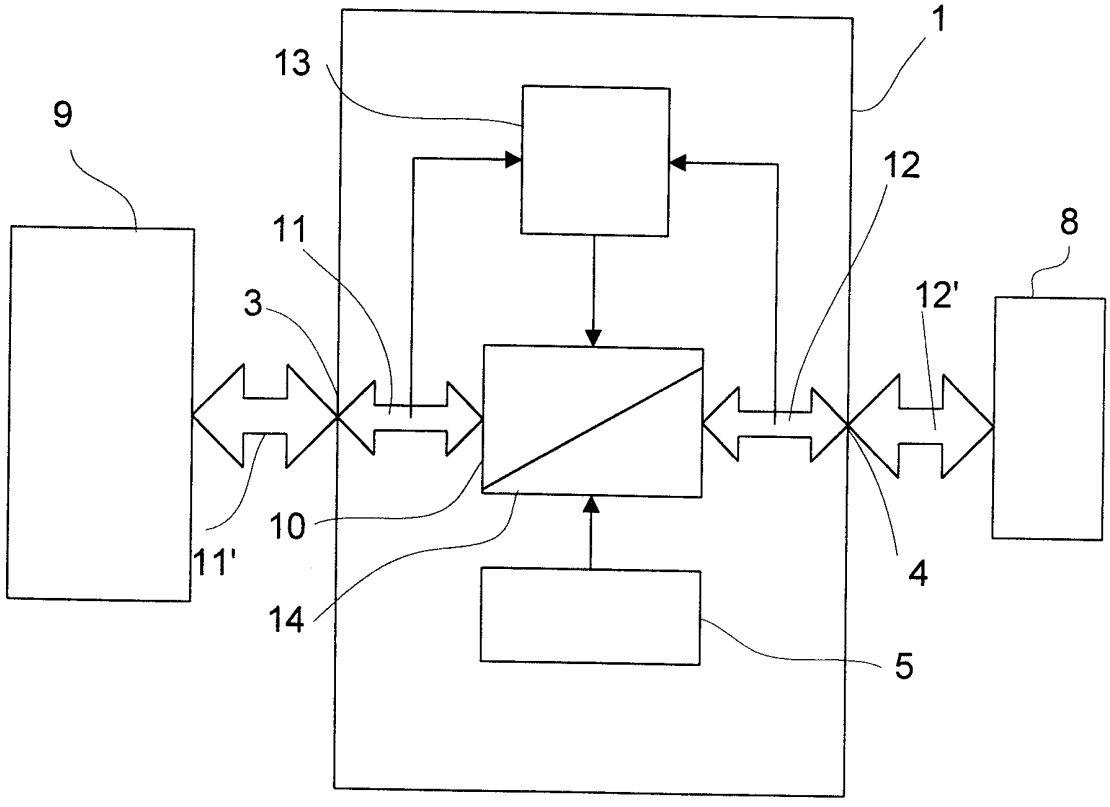


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/00475

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04K 3/00
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)

IPC7: H04K

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 29814427 U1 (SCM MICROSYSTEMS GMBH), 28 January 1999 (28.01.99), page 5, line 12 - line 32, figure 1	1
Y		2-14
	--	
X	WO 9820408 A1 (FOXBORO COMPANY), 14 May 1998 (14.05.98), claims, figures	1
Y		2-14
	--	
X	EP 0628908 A1 (AT & T CORP.), 14 December 1994 (14.12.94), abstract, figures	1
Y		2-14
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family 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" erlier 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 understanc 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
13 June 2000	19 -07- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer S-E Bergdahl / JA A Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/00475

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5671367 A (LE ROUX), 23 Sept 1997 (23.09.97), column 3, line 13 - line 57, abstract, figures	1
Y		2-14
	--	
X	US 5845114 A (CLOUD), 1 December 1998 (01.12.98), figure 1, abstract	1
Y		2-14
	--	
X	US 5857024 A (NISHINO ET AL), 5 January 1999 (05.01.99), column 4, line 49 - line 67, figures	1
Y		2-14
	--	
X	US 5867579 A (SAITO), 2 February 1999 (02.02.99), column 10, line 46 - column 11, line 20, abstract, figures	1
Y		2-14
	--	
X	US 5878142 A (CAPUTO ET AL), 2 March 1999 (02.03.99), column 4, line 66 - column 5, line 6, abstract, figures	1
Y		2-14
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 00/00475

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 29814427 U1	28/01/99	NONE	
WO 9820408 A1	14/05/98	AU 5167098 A	29/05/98
		US 5909586 A	01/06/99
EP 0628908 A1	14/12/94	CA 2123923 A	21/11/94
		JP 6348638 A	22/12/94
		JP 7089441 A	04/04/95
		US 5537654 A	16/07/96
US 5671367 A	23/09/97	DE 69208670 D,T	31/10/96
		DE 69326264 D	00/00/00
		EP 0552077 A,B	21/07/93
		EP 0600892 A,B	15/06/94
		SE 0600892 T3	
		FR 2686171 A,B	16/07/93
		GR 3020038 T	31/08/96
		JP 5324951 A	10/12/93
		JP 6506379 T	21/07/94
		SG 48206 A	17/04/98
		US 5406654 A	18/04/95
US 5845114 A	01/12/98	NONE	
US 5857024 A	05/01/99	JP 9114946 A	02/05/97
US 5867579 A	02/02/99	EP 0715241 A	05/06/96
		JP 8287014 A	01/11/96
US 5878142 A	02/03/99	US 5546463 A	13/08/96
		US 5778071 A	07/07/98