

Description

Method for activating and carrying out secure functions in a communications system

5 The invention relates to a method for activating secure functions in a communications system by means of a peripheral device which is connected to the communications system.

10 Peripheral devices, for example servers, which are connected to communications systems, are provided for convenient switching of incoming calls to communications systems of a communications network, for connected communications terminals and for the activation of performance features. The communications interchange between the communications system and the peripheral
15 device is controlled, for example, by an ACL interface (Application Connectivity Link) which is implemented in both devices. In the communications system, a central controller has a program structure using which not only are the switching events for the incoming calls reported
20 by event messages to the peripheral device, but also switching and operating instructions, which are transmitted from this peripheral device via the ACL interface, are caused to be carried out. The switching and operating instructions initialize and control the functions and
25 performance features in a communications system.

Furthermore, communications systems have functions and performance features whose activation and execution may be carried out only by authorized personnel, for example monitoring of existing communications
30 links or recording, that is to say recording of information transmitted via a communications link. The activation and control of the execution are in this case carried out by the peripheral device, via the ACL interface.

35 The object on which the invention is based is to prevent non-authorized activation and execution of specific functions and performance features of a communi-

cations system by the peripheral device via the ACL interface. The object is achieved on the basis of a method for activating secure functions in a communications system in accordance with the features of the precharacterizing clause of Patent Claim 1 by the characterizing features in said claim.

The essential aspect of the method according to the invention may be regarded as being that function-dependent encryption algorithms are stored in an additional encryption unit which is assigned to the communications system, and a secure function and a security routine are activated in the communications system by means of one operating instruction which is transmitted from the peripheral device. Interrogation information which is encrypted in a functionally specific manner is transmitted to the encryption unit by the activated security routine at least temporarily and advantageously periodically - Claim 5 -, and the secure function is initiated or continues to be carried out provided response information, which is additionally encrypted in a functionally specific manner, is received by the encryption unit, in the security routine, within a predetermined time interval after each transmission of the interrogation information. This at least temporary, advantageously periodic transmission of encrypted interrogation information and the reception of additionally encrypted response information within a predetermined time interval after the transmission of the interrogation information ensure that a secure function and/or a secure performance feature can be activated and executed only by authorized peripheral devices and/or authorized personnel. The operating instruction which activates a secure function is formed - is stored there and is called up - in a secure application implemented in the peripheral device, or is input in an input device of the peripheral device - Claim 2.

During the setting up, which is linked to the activation, of a secure function, the operating instruction advantageously and additionally comprises

operating information by means of which subfunctions which are implemented in a program in the communications system are linked in the program for the purpose of setting up the secure function - Claim 3. In this case, the secure function and/or the secure performance feature are set up first, in the case of their activation, by the program linking of subfunctions which already exist in the communications system, that is to say the secure function and/or the secure performance feature cannot be used before this secure setting up procedure. This achieves further security of functions and performance features which must not be used by unauthorized personnel.

The predetermined time interval can be matched to the processing and transmission times of the communications system, of the peripheral device and of the encryption unit - Claim 6. On the one hand, the predetermined time interval must not be shorter than the total of all the processing and transmission times for the transmission of the interrogation information and the formation and transmission of the response information while, on the other hand, it should not exceed a chosen, maximum time interval.

According to a further advantageous refinement, the encryption programs which implement the determination of the function-specific codes and the formation of the response information can be activated in the encryption unit only by a circuitry program running protection - Claim 8. The circuitry program running protection is advantageously connected to an interface of the encryption unit and causes the encryption programs to be activated by means of an interface routine connected to the interface - Claim 8, 9. This circuitry program running protection - also known as a hardware dongle in the specialist world - additionally enhances security with respect to unauthorized use of specific functions and performance features.

The peripheral device is advantageously connected to the communications system via an ACL interface - Claim

10 - and the encryption unit is advantageously integrated in the peripheral device - Claim 11. The encryption unit is advantageously implemented - integrated in the peripheral device, for example, by means of a personal computer, it being possible to use one of the existing
5 interfaces on the personal computer for the connection of the circuitry program running protection.

The method according to the invention will be explained in more detail in the following text with
10 reference to a block diagram. The block diagram shows a communications system KS to which the communications terminals KE are connected. Two communications terminals KE are illustrated by way of example, which are connected via a switching matrix KF, which is arranged in the
15 communications system KS - indicated by dashed lines in the switching matrix KF. The link between the communications terminals KE shown is set up in accordance with a signalling procedure, for example the ISDN signalling procedure, using a central controller ST which is pre-
20 dominantly implemented as a program.

The communications system comprises a coordinating central control device ST which controls the switching, and an ACL routine ACLR which implements an ACL interface (Application Connectivity Link). The
25 switching matrix KF and the ACL routine ACLR are each connected to the central controller ST. The ACL interface of the ACL routine ACLR is in each case connected to an identically implemented ACL interface ACL of a personal computer PC and to an encryption unit SE. The personal
30 computer PC represents a peripheral device of the communications system KS in which application programs APP for controlling additional functions and performance features of the communications system, for example ACD (Automatic Call Distribution) - functions, are stored.
35 The functions and performance features implemented in the communications systems KS are activated, and their execution is initiated, by the respective application programs APP, by means of switching and operating instructions amo. A program structure - a monitoring

program which is not illustrated - is provided in the central controller ST for indicating switching events and information sp transmitted via the link, by means of which program structure all the switching events and, if
5 required, transmitted information sp are detected and transmitted to the personal computer PC.

For the exemplary embodiment, it is assumed that a secure^a function FAA, in the exemplary embodiment monitoring a connection between the two communications
10 terminals KE and recording the transmitted information sp, is intended to be activated and carried out by means of an application program SAPP. This is done by an operating instruction amo, having information faa indicating the secure^a function FAA to be activated, being
15 transmitted by the application program SAPP via the ACL interface ACL to the central controller ST, which results in a recording routine RER being caused to be set up in said central controller ST. The recording routine RER is set up in the central controller ST in accordance with
20 the statements, which are additionally transmitted in the operating instruction amo, relating to subfunctions tfl...n and linking information vl...n. This additional information tfl...n, vl...n indicates the subfunctions already implemented in the communications system KS and
25 their linkage to one another. This information tfl...n, vl...n can advantageously be indicated in a table in the operating instruction amo.

After setting up the recording routine RER, a start information item si is transmitted to a security
30 routine SIS implemented in the central control unit ST. Encrypted interrogation information afi is formed in this security routine SIS depending on the function and/or performance feature to be activated. In this case, a separate code is stored - not illustrated - in each case
35 for each function to be secured and for each performance feature to be secured. With respect to the exemplary embodiment, the code SRER, which is stored in the security routine SIS and is intended for the performance feature of monitoring and recording is used for the

recording routine RER, which implements the performance feature FAA, monitoring and recording. The interrogation information afi which is encrypted using the function-specific code SRER, is transmitted via the ACL interface

5 ACL to the encryption module SM implemented in the encryption unit SE. In this encryption module SM, the transmitted interrogation information afi is once again encrypted using a function-specific code ARER and is sent back to the security routine SIS as response information

10 ai. The function-specific code ARER differs for the respective functions and/or performance features to be secured and is incorporated in the encryption unit SE by means of circuitry running protection, DONGLE. This inputting is carried out by connecting the circuitry

15 program running protection DONGLE to an interface SST of the interface unit SE. The interface SST, which is implemented by an interface routine SSR, is connected to the encryption module SM. The code ARER is interrogated from the circuitry program running protection DONGLE and

20 is passed to the encryption module SM with the aid of the interface routine SSR, for each incoming interrogation information item afi. Using this function-specific code ARER, the transmitted interrogation information afi is encrypted once again and is sent back to the security

25 routine SIS as response information ai. If the circuitry program running protection DONGLE has not been connected or has been removed, initial or further encryption of the received interrogation information afi is no longer possible. The interrogation information afi is thus sent

30 back without being encrypted - this being assumed in the following text for the exemplary embodiment - or, alternatively, is no longer sent back.

In the security routine SIS of the communications system KS, the transmitted response information ai is

35 checked to determine whether the emitted interrogation information afi is correct, that is to say has been encrypted using the corresponding function-specific code ARER - for the performance feature FAA monitoring and recording in the exemplary embodiment. If the response

information ai has been correctly transmitted, a confirmation information item bi is formed and is transmitted to the recording routine RER which has been set up. A setting command eb is formed by the recording routine RER on the basis of the received confirmation information bi, and is transmitted to the switching matrix KF. The switching matrix causes an additional subscriber connection A to be connected to the already existing link V between the communications terminals KE - indicated by dashed lines. A recording device REC, for example, which automatically records information sp once said information sp is present, is connected to this additional subscriber connection A. Alternatively, the recording device REC is connected to an interface SC of the personal computer PC. In this case, the information sp transmitted between the two communications terminals KE is transmitted via the recording routine RER and the ACL interface ACL, as well as the relevant application program SAPP, and via the interface SC to the recording device REC. The recording device REC can alternatively be integrated in the personal computer PC - indicated by dashed lines -, it also being possible to use existing memory devices in the personal computer PC.

Particularly when using the personal computer PC to record the transmitted information sp, it is necessary to prevent unallowed access or unauthorized access to the ACL interface ACL during recording, that is to say during operation. To this end, the security routine SIS periodically, that is to say at predetermined time intervals of, for example, five seconds, forms and transmits an interrogation information item afi and, at a predetermined time interval, for example 3 seconds, waits for a correctly encrypted response information item ai. If this additionally encrypted response information item ai does not occur, the recording process is interrupted immediately and the recording routine RER which has been set up is erased. The period duration, that is to say the time duration between the respective transmission of interrogation information afi [lacuna], and the response

duration, that is to say the duration in which an additionally encrypted response information item ai must be received after the transmission of an interrogation information item afi, must be matched to the respective
5 processing and transmission times in the communications system KS, the encryption unit SE and the connecting lines between the ACL interfaces ACL.

The operating instruction amo for activating and setting up a secure^a function and/or a secure feature can
10 alternatively be formed by an input device EE, for example a keyboard, of the personal computer PC and is subsequently transmitted via the ACL interface ACL to the communications system. Considerable security against
15 unallowed activation of secure functions and performance features is achieved both by the special, that is to say user-specific, inputting on the input device EE of the personal computer PC and by the circuit program running protection DONGLE.

Additional security is achieved in that the
20 encryption unit SC is connected to the ACL interface ACL, that is to say, for example, is plugged in, by an authorized person shortly before activation and execution of secure functions and/or performance features. The encryption unit SE can also be connected to a connecting
25 unit, for example an existing plug device of the personal computer, this connection in the personal computer PC being dependent on integration of an additional ACL interface ACL. The encryption unit SE can also be permanently inserted between the two ACL interfaces ACL of the
30 personal computer PC and of the communications system KS, security being achieved, for example, by means of plug-in circuitry program running protection DONGLE.

Patent Claims

1. Method for activating secure functions (FAA) in a communications system (KS) by means of a peripheral device (PC) which is connected to the communications system (KS),
5 characterized
- in that function-dependent encryption algorithms (SRER) are provided in an additional encryption unit (SE) which is assigned to the communications system (KS),
10 - in that a secure function (FAA) and a security routine (SIS) are activated in the communications system (KS) by means of at least one operating instruction (amo) which is transmitted from the peripheral device (PC),
- in that interrogation information (afi) which is
15 encrypted in a functionally specific manner at least temporarily by the activated security routine (SIS) is transmitted to the encryption unit (SE), and
- in that the secure function (FAA) is initiated or continues to be carried out providing response information
20 (ai), which is additionally encrypted in a functionally specific manner, is received by the encryption unit (SE), in the security routine (SIS), within a predetermined time interval after each transmission of the interrogation information (afi).
- 25 2. Method according to Claim 1, characterized in that the at least one operating instruction (amo) is formed in a secure application (SAPP) which is provided in the peripheral device (PC), or in an input device (EE) of the peripheral device (PC).
- 30 3. Method according to Claim 1, characterized in that, during the period in which the secure function (FAA) is being set up, this process being linked to activation, the operating instruction (amo) additionally comprises operating information (tfl..n, vl..n) by means
35 of which subfunctions which are implemented in a program in the communications system (KS) are linked in the program for the purpose of setting up the secure function (FAA).



4. Method according to Claim 3, characterized in that the additional operating information (tfl..n,vl..n) which is formed by the secure^a application (SAPP) is entered in a logic table using which the subfunctions
5 which implement the specified secure^a function (FAA) are linked in the program.

5. Method according to one of the preceding claims, characterized in that the interrogation information (afi) which is encrypted in a functionally specific manner is
10 transmitted periodically to the encryption unit (SE).

6. Method according to one of the preceding claims, characterized in that the predetermined time interval is matched to the processing and transmission times of the communications system (KS), of the peripheral device (PC)
15 and of the encryption unit (SE).

7. Method according to one of the preceding claims, characterized in that the secure^a functions (FAA) are represented by secure^a switching functions and by secure^a performance features.

8. Method according to one of the preceding claims, characterized in that the encryption programs (SM) which implement the determination of the function-specific codes (ARER) and the formation of the response information (ai) can be activated in the encryption unit (SE) by
25 a circuitry program running protection (DONGLE).

9. Method according to Claim 6, characterized in that the circuitry program running protection (DONGLE) is connected to an interface (SST) of the encryption unit (SE), and in that the activation of the encryption
30 program (SM) is brought about by means of an interface routine (SSR) which is connected to the interface (SST).

10. Method according to one of the preceding claims, characterized in that the peripheral device (PC) is connected to the communications system (KS) via an ACL
35 interface (ACL).

11. Method according to one of the preceding claims, characterized in that the encryption unit (SE) is integrated in the peripheral device (PC).

