

14
CLAIMS

1.- Cryptographic equipment (10), comprising:

- an input interface (26), allowing to interact with the cryptographic equipment (10) and share sensitive or non-sensitive information sequentially,
- a red module (12), intended to process sensitive information,
- a cryptographic module (14), connected to the red module (12) by a first upstream internal link (16) and adapted to apply cryptographic functions,
- a black module (20), connected to the cryptographic module (14) by a first downstream internal link (22) and adapted to process non-sensitive information, and
- an output interface (38), connected to the black module (20) by a first interface link (40) and intended to manage information sharing from the cryptographic equipment (10),

characterized in that the cryptographic module (14) includes:

- a cryptographic unit (42), which interacts with the red module (12) through the first upstream internal link (16), and with the black module (20) through the first downstream internal link (22), and adapted to process the sensitive information using the cryptographic functions, and

- a management device (44), which interacts with the input interface (26) through at least one second interface link (30, 34, 36) and with either the red module (12) through a second upstream internal link (18), or the black module (20) through a second downstream internal link (24), but not with both simultaneously, and adapted to orient the sensitive information between the input interface (26) and the second upstream internal link (18), or the non-sensitive information between the input interface (26) and the second downstream internal link (24), without the non-sensitive information passing through the red module (12),

and in that the cryptographic unit (42) and the management device (44) are physically and logically separate from one another and independent, and have identical protection means, capable of protecting the integrity of the management device (44) so as to detect any tampering attempt.

2.- The cryptographic equipment (10) according to claim 1, characterized in that the cryptographic unit (42) and the management device (44) have separate physical resources.

3.- The cryptographic equipment (10) according to claim 1 or 2, characterized in that the management device (44) comprises:

- an orienting device (50) simultaneously connected to the second upstream internal link (18), the second downstream internal link (24), and at least one second interface link (30, 34, 36), the orienting device (50) being intended to link the input interface (26) either to the red module (12) or to the black module (20), but not both simultaneously; and

- verification means (58) of the orienting device connected simultaneously to:

- the orienting device (50), so as to control the link to be made, and

- the input interface (26), so as on the one hand to receive a selection instruction for the link to be made according to a selected operating mode, and on the other hand to inform the user of the current operating mode.

4.- The cryptographic equipment (10) according to claim 3, characterized in that the input interface (26) comprises:

- an external physical interface (28) connected to the orienting device (50) and intended to send the sensitive or non-sensitive information to the cryptographic equipment (10) and to receive the sensitive or non-sensitive information from the cryptographic equipment (10),

- an indicator (32) connected to the verification means (58) of the orienting device and intended to indicate the current operating mode, and

- selecting means (35) connected to the verification means (58) of the orienting device and intended to provide the selection instruction for the selected operating mode.

5.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the cryptographic equipment (10) comprises an additional external physical interface (46) connected to the red module (12) and intended to send and receive sensitive information, without passing through the management device (44).

6.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the red module (12) includes an element from the group consisting of: an audio encoding device, an audio retrieval device, an echo canceling device, an audio gain verification device, an error detection and correction device, an analog-digital converter, a digital-analog converter, a data packet classification device, a data routing device, and a data filtering device.

7.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the black module (20) includes an element from the group consisting of: an audio encoding device, an audio retrieval device, an analog-digital converter, a modulator/demodulator, a transmission error detection and correction device, a digital-analog converter, an electric, radiofrequency or optical emitter/receiver, an electrical, radiofrequency or optical power amplifier, a data routing device, a data filtering device, and a data packet classification device.

8.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the output interface (38) is an element from the group consisting of: an audio interface, a radiofrequency interface, a wired electrical interface, and an optical interface.

9.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the cryptographic equipment (10) is an element from the group consisting of: a radio set, a network encryptor, a feeder encryptor, an encrypting audio receiver, an encrypting terminal.

10.- The cryptographic equipment (10) according to any one of the preceding claims, characterized in that the management device (44) includes at least one of the elements from the group consisting of: an electromagnetic component, a discrete electronic component, a programmable logic circuit, and an integrated circuit.

1. Cryptographic equipment, comprising:
 - a first input interface configured to interact with the cryptographic equipment and share sensitive or non-sensitive information sequentially;
 - a red host domain configured to process sensitive information;
 - a cryptographic domain connected to the red host domain by a first upstream internal link and configured to apply cryptographic functions;
 - a black host domain connected to the cryptographic domain by a first downstream internal link and configured to process non-sensitive information;
 - an output interface connected to the black host domain by a first interface link and intended to manage information sharing from the cryptographic equipment; and
 - a second input interface connected to the red host domain,

wherein the first input interface is configured to form a first secured connection with the output interface,

wherein the second input interface is configured to form a second secured connection with the output interface,

wherein the first and second secured connections are different and are arranged in parallel,

wherein the cryptographic domain includes:

 - a cryptographic unit comprising a cryptographic processing circuit which interacts with the red host domain through the first upstream internal link, and with the black host domain through the first downstream internal link, and wherein the cryptographic processing circuit is configured to process the sensitive information using the cryptographic functions, and
 - a management device comprising a management processor configured to interact with the first input interface through at least one second interface link and with either the red host domain through a second upstream internal link, or the black host domain through a second downstream internal link, but not with both simultaneously,

wherein the management processor is further configured to orient the sensitive information between the first input interface and the second upstream internal link, or the non-sensitive information between the first input interface and the second downstream internal link, without the non-sensitive information passing through the red host domain,

wherein the cryptographic unit and the management device are physically and logically separate from one another and independent,

wherein the cryptographic unit and the management device include identical protective housings configured to: i) protect the integrity of the management device and ii) detect any tampering attempt, and

wherein the management device further comprises:

 - a bidirectional switch simultaneously connected to the second upstream internal link, the second downstream internal link, and at least one second interface

link, the bidirectional switch being configured to link the first input interface either to the red host domain or to the black host domain, but not both simultaneously, and
a bidirectional switch controller connected simultaneously to:

the bidirectional switch, and

the first input interface, wherein the bidirectional switch controller is configured to: i) receive a selection instruction for controlling the bidirectional switch according to a selected operating mode, and ii) inform the user of the current operating mode.

2. The cryptographic equipment according to claim 1, wherein the cryptographic unit and the management device have separate physical resources.

3. The cryptographic equipment according to claim 1, wherein the first input interface comprises:

an external physical interface connected to the bidirectional switch and configured to send the sensitive or non-sensitive information to the cryptographic equipment and to receive the sensitive or non-sensitive information from the cryptographic equipment,

an indicator connected to the bidirectional switch controller and configured to indicate the current operating mode, and

a selector connected to the bidirectional switch controller and configured to provide the selection instruction for the selected operating mode.

4. The cryptographic equipment according to claim 1, wherein the second input interface is configured to send and receive sensitive information, without passing through the management device.

5. The cryptographic equipment according to claim 1, wherein the red host domain includes an element from the group consisting of: an audio encoding device, an audio retrieval device, an echo canceling device, an audio gain verification device, an error detection and correction device, an analog-digital converter, a digital-analog converter, a data packet classification device, a data routing device, and a data filtering device.

6. The cryptographic equipment according to claim 1, wherein the black host domain includes an element from the group consisting of: an audio encoding device, an audio retrieval device, an analog-digital converter, a modulator/demodulator, a transmission error detection and correction device, a digital-analog converter, an electric, radiofrequency or optical emitter/receiver, an electrical, radiofrequency or optical power amplifier, a data routing device, a data filtering device, and a data packet classification device.

7. The cryptographic equipment according to claim 1, wherein the output interface is an element from the group consisting of: an audio interface, a radiofrequency interface, a wired electrical interface, and an optical interface.

8. The cryptographic equipment according to claim 1, wherein the cryptographic equipment is an element from the group consisting of: a radio set, a network encryptor, a feeder encryptor, an encrypting audio receiver, an encrypting terminal.

9. The cryptographic equipment according to claim 1, wherein the management device includes at least one of the elements from the group consisting of: an electromagnetic component, a discrete electronic component, a programmable logic circuit, and an integrated circuit.