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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 September 2009 (24.09.2009)

PCT

(10) International Publication Number
WO 2009/115997 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2009/051145

(22) International Filing Date:
18 March 2009 (18.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08102759.1 19 March 2008 (19.03.2008) EP

(71) Applicant *(for all designated States except US)*: **NXP B.V.** [NL/NL]; High Tech Campus 60, NL-5656 AG Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MARX, Felix** [AT/AT]; c/o Nxp Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(74) Agent: **ROEGGLA, Harald**; c/o Nxp Semiconductors Austria Gmbh, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR ENSURING INTEGRITY OF A CONTACTLESS CARD EMULATING DEVICE

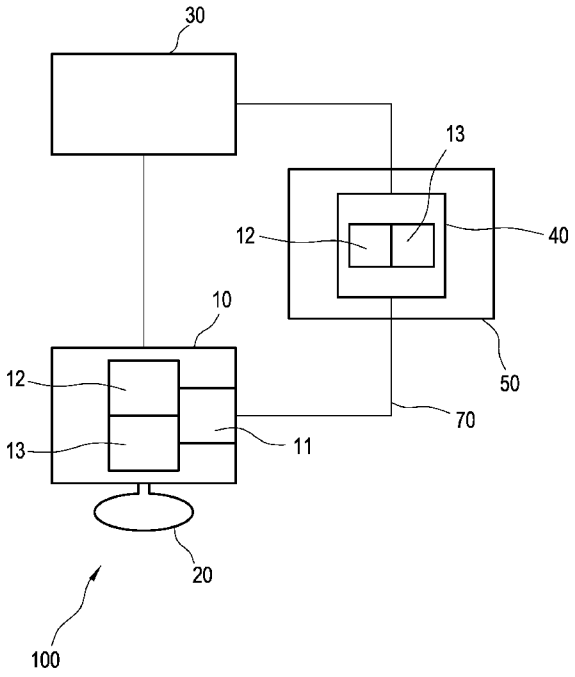

Fig. 3

(57) Abstract: Method for ensuring an integrity of a contactless card emulating device (12), wherein the card emulating device (12) is arranged in an NFC frontend device (10) and/or in a secure element (40),wherein the secure element (40) is galvanically connected to the NFC frontend device (10), and wherein an authenticating procedure for the contactless card emulating device (12) is performed between the NFC frontend device (10) and the secure element (40).

WO 2009/115997 A2

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

Method and system for ensuring integrity of a contactless card emulating device

FIELD OF THE INVENTION

The invention relates to a method for ensuring integrity of a contactless card emulating device.

The invention further relates to a system for ensuring integrity of a contactless card emulating device.

BACKGROUND OF THE INVENTION

Nowadays, contactless card emulating functionality is increasingly implemented into mobile electronic devices (e.g. mobile phones, PDAs, etc.). Said contactless card emulating functionality can e.g. integrated by means of contactless card emulating devices in a well known Near Field Communication (NFC) frontend device of the mobile electronic devices. Usually, the contactless card emulating functionality is implemented by means of so called "secure elements" which are also used for encryption purposes of the contactless card emulating devices. Said secure elements can be integrated e.g. in a SIM-card, an SD-card or other electronic memory devices. A legitimation problem can arise in that said contactless card emulating devices are not legitimated, e.g. clones which are not allowed to be operated without an expressive permission of a licensor or licensee.

OBJECT AND SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide a method and a system for an enhanced security level of contactless card emulating devices.

In order to achieve the object defined above, a method for ensuring the integrity of a contactless card emulating deivices is provided wherein the card emulating device is arranged in an NFC frontend device and/or in a secure element, wherein the secure element is galvanically connected to the NFC frontend device and wherein an authenticating procedure for the contactless card emulating device is performed between the NFC frontend device and the secure element. Thus, it can advantageously be verified that the contactless card emulating device is a certified and not a cloned one. In a case that the contactless card emulating device is a cloned one, the contactless card emulating procedure by means of said cloned device is disabled. A user or distributor of cloned contactless card emulating devices

derives thus no benefit from the usage or distribution of said unlegitimated devices.

In a preferred embodiment of the inventive method, the authenticating procedure is performed between specific authenticating means which are arranged on the NFC frontend device and/or on the secure element. Thus, by implementing specific authenticating means which are as such well known in the art, a very comfortable way of ensuring the integrity of a contactless card emulating device is provided.

A preferred embodiment of the inventive method provides, that in a case, that no authenticating means is assigned to the contactless card emulating device, the contactless card emulating device is disabled from performing the contactless card emulating procedure. Thus, an easy implementable method for disabling not allowed card emulating devices is provided.

In a further preferred embodiment of the method according to the invention, the authenticating means are based on a comparison of unique identifier ranges which are able to be handled by the NFC frontend device. Thus, a legalized owner of rights on the contactless card emulating devices (e.g. licensor) is able to control a supply chain of the contactless card emulating devices in the market.

In a further preferred embodiment of the method according to the invention, the authenticating procedure uses not standardized, proprietary data. Thus, it is advantageously complicated for imitators of the contactless card emulating devices to place their unlegitimated devices in the market.

The object of the invention is further solved by a system for ensuring integrity of a contactless card emulating device comprising an NFC frontend device and a secure element, wherein the contactless card emulating device is arranged in the NFC frontend device and/or in the secure element, wherein the secure element is galvanically connected to the NFC frontend device, and wherein an authenticating procedure is performable between the NFC frontend device and the secure element.

The aspects defined above and further aspects of the invention are apparent from exemplary embodiments to be described hereinafter and are explained with reference to these exemplary embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in more detail hereinafter with reference to exemplary embodiments. However, the invention is not limited to these exemplary embodiments.

Figure 1 shows in principle a mobile phone with different possibilities to integrate contactless card functionality into the mobile phone;

Figure 2 shows in principle an embodiment of the invention; and

Figure 3 shows in principle a use case of the invention.

DESCRIPTION OF EMBODIMENTS

Figure 1 shows in principle a mobile phone 100 with well known Near Field Communication (NFC) functionality. To provide said functionality, the mobile phone 100 comprises an NFC frontend device 10 and a host controller 30 for controlling the NFC frontend device 10. An antenna 20 is galvanically connected to the NFC frontend device 10 in order to provide an air interface to another NFC- or RFID device. Furthermore, the mobile phone 100 comprises contactless card emulating functionality. Contactless card emulating functionality means that a device can emulate a contactless smart card functionality (e.g. payment and/or ticketing applications). The contactless card emulating functionality requires dedicated encryption algorithms to ensure an integrity of the data. In the mobile environment, the contactless card emulating and the encryption functionalities are handled in a so called "secure element" 40. Said secure element 40 is an integrated electronic circuitry which is especially safe against cloning and counterfeiting.

Figure 1 shows different possibilities to implement the contactless card emulating functionality into the mobile phone 100, indicated via dotted lines to the NFC frontend device 10. Figure 1 shows a SIM module 50, which is connectable to the NFC frontend device 10 and into which the contactless card emulating functionality can be integrated by means of the secure element 40. Alternatively, the secure element 40 can also be integrated into an SD card 60 which is also connectable to the NFC frontend device 10.

Legitimation problems could arise when the devices for performing the contactless card emulating functionality are counterfeited and/or cloned.

Figure 2 shows in principle an embodiment of a system according to the invention. The figure shows in principle a galvanic connection 70 between the NFC frontend device 10 and the secure element 40, the secure element 40 being integrated into a SIM module 50. The galvanic connection between the NFC frontend device 10 and the secure element 40 can e.g. be formed as a single wire connection 70. Needless to say, that also alternative kinds of galvanic connections between the NFC frontend device 10 and the secure element 40 are imaginable. Both the NFC frontend device 10 and the secure element 40 have card emulating devices 12 implemented. Both card emulating devices 12 have dedicated

corresponding encrypting devices 13. The card emulating devices 12 on the NFC frontend device 10 and on the SIM module 50 have authenticating means 11, 41. In more detail, first authenticating means 11 are assigned to the card emulating means 12 on the NFC frontend device 10 and second authenticating means 41 are assigned to the card emulating device 12 on the SIM module 50.

Now, in order to verify an integrity of the card emulating devices 12, an authenticating procedure takes place between the first and second authenticating means 11, 41 via the single wire connection 70. To this end, the first and second authenticating means 11, 41 can be based on a simple comparison of unique identifier (UID) ranges which are processable by the NFC frontend device 10. An alternative option is a dedicated secret authentication method using proprietary, e.g. not standardized commands/information. Alternatively, also an authentication method based on symmetric or asymmetric encryption algorithms is possible. Said mentioned methods as such are numerous and are well known in the art and are therefore not further described hereinafter. After having performed the authentication, the first and second authentication means 11, 41 decide which of the card emulating devices 12 are to be used for the performance of the contactless card emulating functionality of the mobile phone 100.

Figure 3 shows in principle a use case of the invention. In this use case, the SIM module 50 contains a card emulating device 12 and an assigned corresponding encrypting device 13 but no assigned corresponding second authenticating means 41. As a result of the absence of the second authenticating means 41, the authenticating procedure as described above on the basis of figure 2 will fail. Therefore, the card emulating device 12 on the SIM module 50 is identified as a not legitimated card emulating device 12 (e.g. a clone) and will therefore be disabled from performing the contactless card emulating functionality on the mobile phone 100. It is thus advantageously very comfortable to exclude not legitimated entities of the card emulating devices 12 from performing the contactless card emulating functionality on the mobile phone 100. An enhanced security level of the contactless card emulating devices 12 results by performing the inventive method with the inventive system.

Summarizing, the invention is based on a trust logic which ensures that the entities containing the contactless card emulating functionality are provided by trusted partners and/or licensers.

It has to be mentioned that the invention is not limited to a single card emulating device 12 on a single secure element 40. Rather, the invention can also be

performed with several secure elements 40, wherein all or several of the secure elements 40 contain card emulating devices 12. By means of the method according to the invention, all card emulating devices 12 which do not comply with the authenticating method can be disabled from performing the contactless card emulating functionality.

Although exemplary embodiments of the invention have been disclosed, it will be apparent to those skilled in the art that various changes and modifications can be made which will achieve some of the advantages of the invention without departing from the spirit and scope of the invention. Such modifications to the inventive concept are intended to be covered by the appended claims in which the reference signs shall not be construed as limiting the scope of the invention. Further, in the description and the appended claims the meaning of "comprising" is not to be understood as excluding other elements or steps. Furthermore, "a" or "an" does not exclude a plurality, and a single device or other units may fulfill the functions of several means recited in the claims.

CLAIMS

1. Method for ensuring an integrity of a contactless card emulating device (12), wherein the card emulating device (12) is arranged in an NFC frontend device (10) and/or in a secure element (40), wherein the secure element (40) is galvanically connected to the NFC frontend device (10), and wherein an authenticating procedure for the contactless card emulating device (12) is performed between the NFC frontend device (10) and the secure element (40).

2. Method according to claim 1, wherein the authenticating procedure is performed between authenticating means (11, 41) being arranged on the NFC frontend device (10) and/or on the secure element (40).

3. Method according to claim 2, wherein in a case, that no authenticating means (11, 41) is assigned to the contactless card emulating device (12), the contactless card emulating device (12) is disabled from performing the contactless card emulating procedure.

4. Method according to claim 3, wherein the authenticating means (11, 41) are based on a comparison of unique identifier ranges which are able to be handled by the NFC frontend device (10).

5. Method according to any of the claims 1 to 4, wherein the authenticating procedure is based on symmetric or asymmetric encryption algorithms.

6. Method according to any of the claims 1 to 5, wherein the authenticating procedure uses not standardized, proprietary data.

7. System for ensuring an integrity of a contactless card emulating device (12) comprising an NFC frontend device (10) and a secure element (40), wherein the contactless card emulating device (12) is arranged in the NFC frontend device (10) and/or in the secure element (40), wherein the secure element (40) is galvanically connected to the NFC frontend

device (10), and wherein an authenticating procedure is performable between the NFC frontend device (10) and the secure element (40).

8. System according to claim 7, wherein the authenticating procedure is performable with authenticating means (11, 41), the authenticating means (11, 41) being arrangeable in the NFC frontend device (10) and/or in the secure element (40).

9. System according to claim 8, wherein the galvanic connection between the NFC frontend device (10) and the secure element (40) is formed as a single wire connection (70).

10. System according to claim 9, wherein the authenticating procedure is performable via the single wire connection (70).

11. System according to any of the claims 7 to 10, wherein the secure element (40) is arrangeable in a SIM card (50) or in a SD card (60).

12. System according to any of the claims 7 to 11, wherein the system comprises a multiplicity of secure elements (40), wherein the authenticating procedure is performable between the NFC frontend device (10) and at least one of the multiplicity of the secure elements (40).

13. Mobile phone (100), comprising a system according to any of the claims 7 to 12.

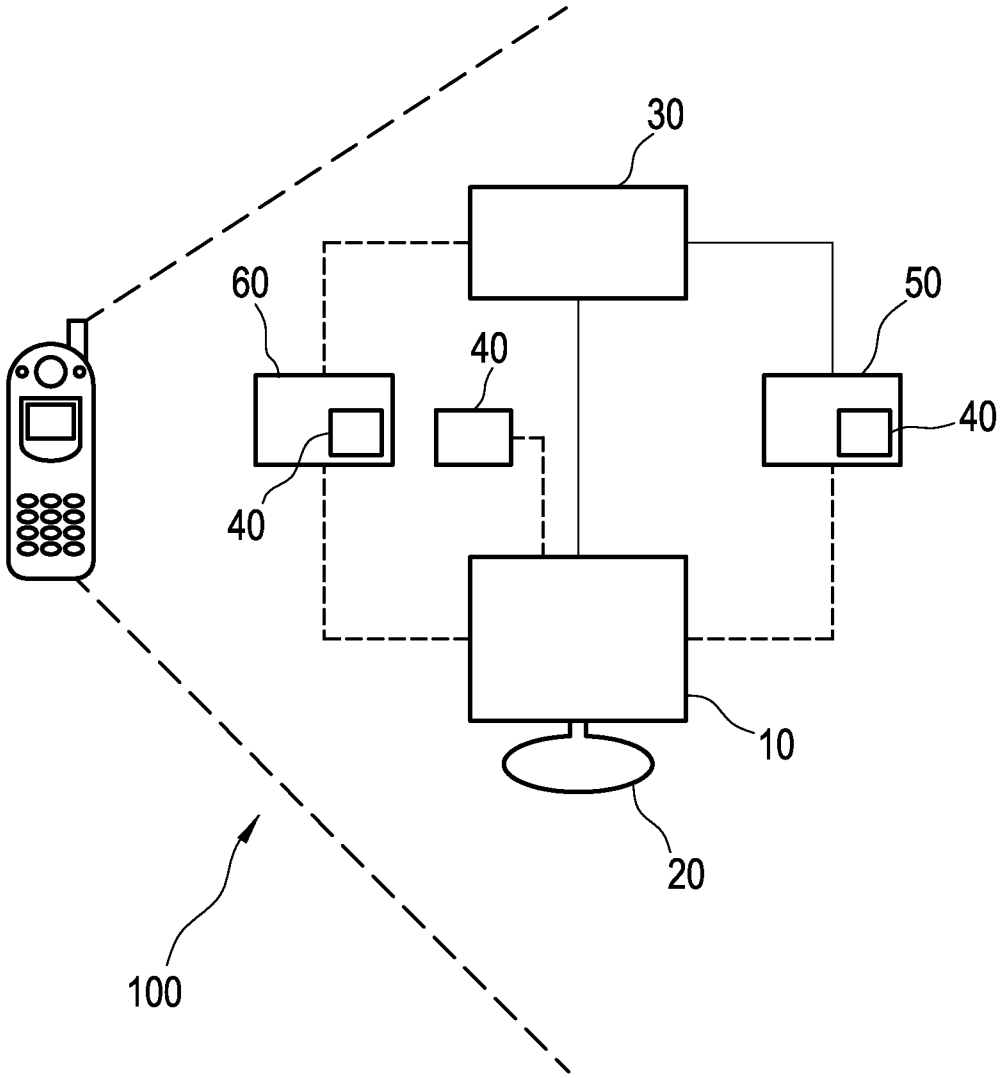

Fig. 1

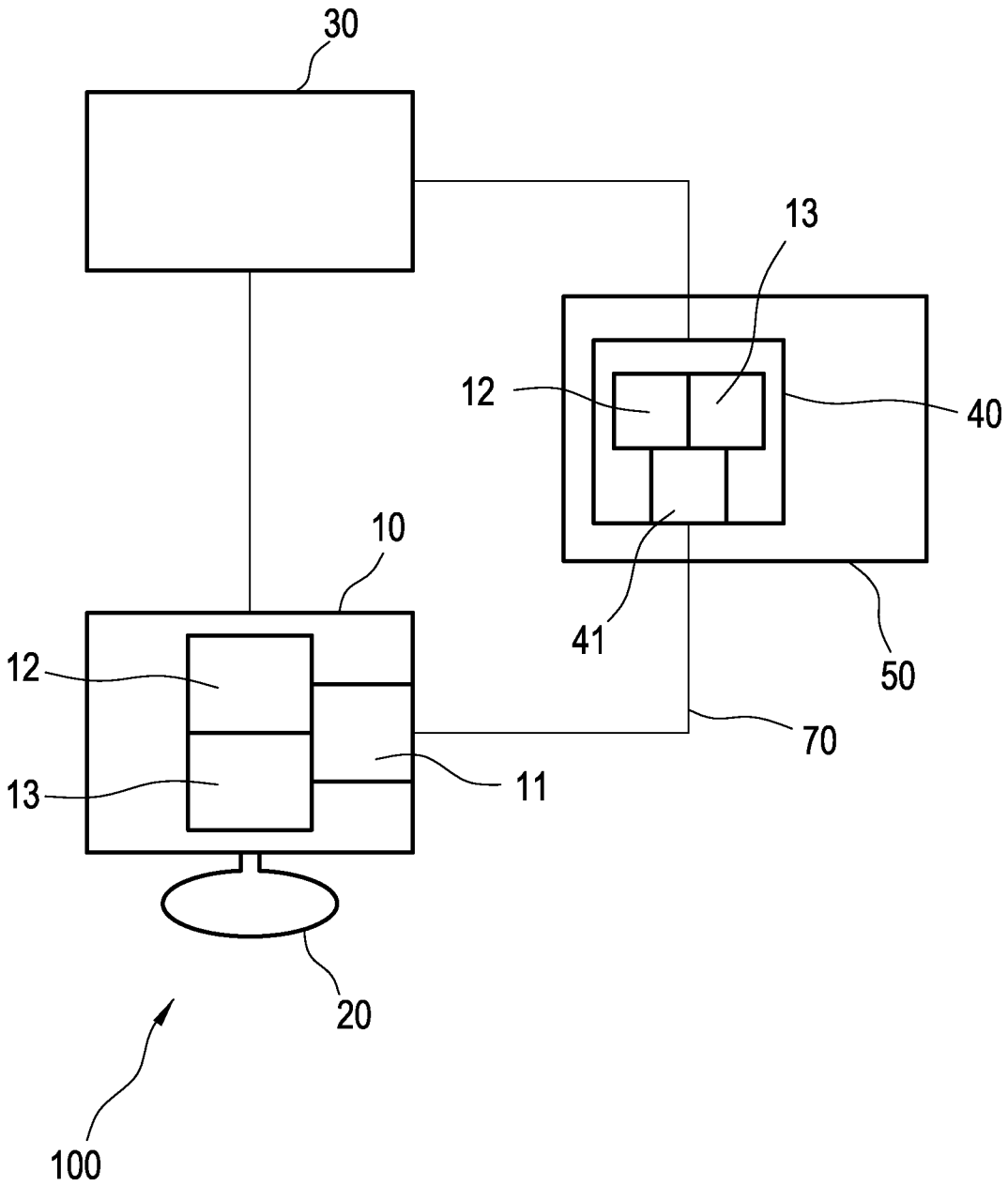

Fig. 2

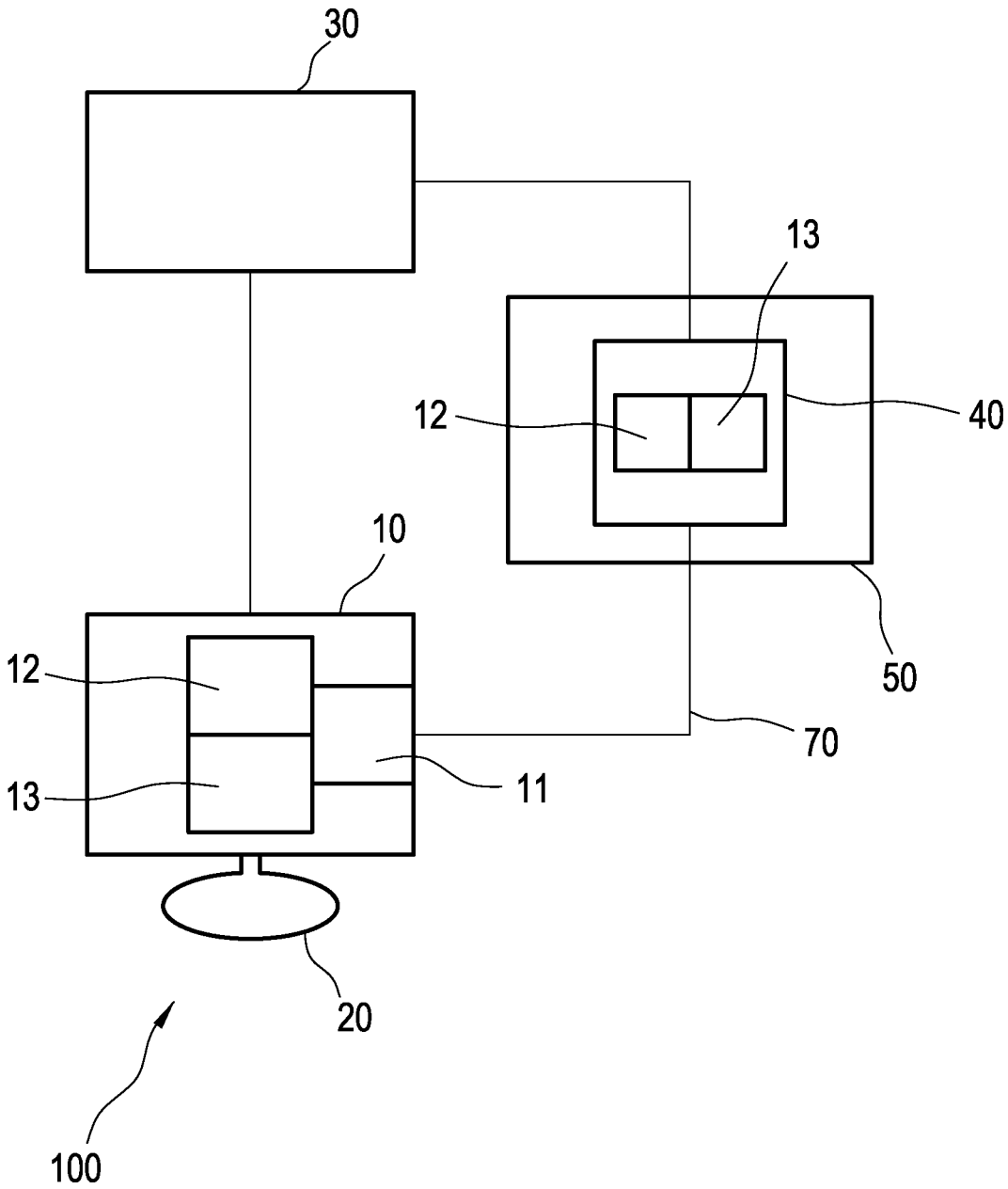

Fig. 3