Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 10 October 2018

Case Number:	T 1515/14 - 3.5.03
Application Number:	08019831.0
Publication Number:	2187592
IPC:	H04L29/06
Language of the proceedings:	EN

Title of invention:
Machine-to-machine device and smartcard for use in the device

Applicant:
Vodafone Holding GmbH

Headword:
Machine-to-machine device/VODAFONE

Relevant legal provisions:
EPC Art. 56
EPC R. 103(1)(a)

Keyword:
Inventive step - (no)
Reimbursement of appeal fee - (no)

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1515/14 - 3.5.03

DECISION
of Technical Board of Appeal 3.5.03
of 10 October 2018

Appellant: (Applicant)
Vodafone Holding GmbH
Mannesmannufer 2
40213 Düsseldorf (DE)

Representative:
Jostarndt Patentanwalts-AG
Philipsstrasse 8
52068 Aachen (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted on 24 January 2014 refusing European patent application No. 08019831.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	F. van der Voort
Members:	K. Schenkel
	P. Guntz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 08019831.0, with European publication number EP 2 187 592 A1.

II. The refusal was based, *inter alia,* on the grounds that the subject-matter of claim 1 of each of a main request, a first auxiliary request, and a second auxiliary request did not involve an inventive step when starting out from the disclosure of D2 (= WO 2004/114144 A).

III. In the statement of grounds of appeal, the appellant requested that the decision be set aside and that a patent be granted on the basis of the claims of a single request as filed with the statement of grounds of appeal. The claims of the request were said to be essentially identical to the claims of the first auxiliary request considered by the examining division in its decision and, for this reason, the appellant requested that the appeal fee be reimbursed. Further, it conditionally requested that oral proceedings be held.

IV. In a communication accompanying a summons to oral proceedings, the board, without prejudice to its final decision, raised objections under Articles 84 and 123(2) EPC against claims 1 and 11. It also raised objections under Article 52(1) EPC in conjunction with Article 56 EPC in respect of the subject-matter of claims 1 and 11, starting out from document D2 and taking into account the common general knowledge of the person skilled in the art. In the communication, the following document, which is an excerpt from a general textbook in the field of smartcards, was referred to by the board, exercising its discretion under Article 114(1) EPC:

D6: "HANDBUCH DER CHIPKARTEN"; Wolfgang Rankl, Wolfgang Effing; 5. Auflage; 8/2008; Carl Hanser Verlag; pages 295 to 306, 879 to 882, and 904 to 910.

The board further noted in its communication that the appeal fee could only be reimbursed if the appeal were deemed allowable and a reimbursement were equitable by reason of a substantial procedural violation (Rule 103(1)(a) EPC).

V. By letter dated 8 October 2018, the appellant informed the board that it would not be attending the oral proceedings.

VI. Oral proceedings were held on 10 October 2018 in the absence of the appellant.

The board understood the appellant to be requesting in writing that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 11 as filed with the statement of grounds of appeal. Further, it requested that the appeal fee be reimbursed.

At the end of the oral proceedings, after due deliberation, the chairman announced the board's decision.

VII. Claim 1 reads as follows:

"A device (202) having remote access capability comprising

- a connection module (210) for connecting the device (202) to a remote location (224);

- a component (204; 206) of the device (202) accessible in conjunction with a communication with the remote location (224); and

- a smartcard (208) comprising a control module integrated into the smartcard interfacing with the connection module (210), the control module (210) *[sic]* being adapted to communicate with the remote location (224) via the connection module (210), the smartcard (208) further comprising an I/O interface;

characterized in that

the control module further interfacing with the component (204; 206) of the device (202) to access the component (204, 206) in conjunction with a communication with the remote location (224), where the smartcard (208) provides different interfaces for connecting to the component (204; 206) and to the connection module (210), and where the smartcard comprises a secure identification and/or authentication means, and wherein the smartcard (208) and the component (204; 206) are connected via an USB interface or a SWP interface of the smartcard (208), and wherein the smartcard (208) and the connection module (210) are connected via the I/O interface of the smartcard (208)."

Reasons for the Decision

1. Claim 1 - inventive step

1.1 The present application concerns machine-to-machine communication for connecting a device to a remote location (cf. the title and the abstract).

1.2 Document D2 is considered to represent the closest prior art and discloses a machine-to-machine (M2M) module 110 for connecting a remote device 112 to a server 118 via a base station 108 (see the title, the abstract, page 4, lines 10 and 11 and lines 29 to 32, and Figs. 1 and 2). In the following, the M2M module and the remote device are regarded as one unit.

Using the language of claim 1, D2 discloses a device having remote access capability ("M2M module 110" in combination with "remote device 112", page 4, lines 9 to 11, Figs. 1 and 2) and including:

a connection module ("radio interface" respectively the circuitry of the "M2M module" for establishing it, page 4, lines 9 and 10) for connecting the device to a remote location ("base station 108", *ibid.*);

a component ("remote device 112", page 4, lines 10 and 11) of the device ("M2M module 110" and "remote device 112") accessible in conjunction with a communication with the remote location (page 4, lines 29 to 32, Fig. 1, the communication between the remote device 112 and the server 118 is routed through the base station 108);

a smartcard ("built-in SIM", page 4, lines 11 to 13); and

a control module ("Java virtual machine (JVM) 122", page 5, lines 5 to 10) interfacing with the connection module (Fig. 2, the line between block 122 and M2M gateway 114 implies a connection to the radio interface and the network connected to it), the control module being adapted to communicate with the remote location via the connection module (page 4, lines 29 to 32);

the smartcard further comprising an I/O interface (implicitly part of a SIM card);

wherein the control module further interfaces with the component of the device to access the component in conjunction with a communication with the remote location (page 4, lines 29 to 32);

wherein the control module provides different interfaces for connecting to the component and to the connection module (Fig. 2 shows two different lines between the Java virtual machine 122 and, respectively, the remote device 112 and the M2M gateway 114, which implicitly includes a connection to the radio interface or the corresponding circuitry of the device 110);

wherein the smartcard comprises a secure identification and/or authentication means (a SIM card provides identification and authentication of a subscriber);

and wherein the control module and the component are connected.

1.3 The device of claim 1 thus differs from the device disclosed in D2 in that:

(a) the control module is integrated into the smartcard;

(b) the different interfaces for connecting to the component and to the control module are provided by the smartcard;

(c) the smartcard is connected to the component via a USB interface or an SWP interface; and

(d) the smartcard is connected to the connection module via the I/O interface of the smartcard.

The board notes that D2 discloses "means for operating" the control module ("Java virtual machine", page 2, lines 22 to 25 and claim 10), but is silent about its specific implementation. Integrating the control module into the smartcard according to feature (a) has the technical effect that the data processing means of the smartcard can be used as the platform for running the control module. A further technical effect of feature (a) is a higher level of integration, leading to a reduced complexity with fewer components.

1.4 Starting out from D2, a technical problem underlying the subject-matter of claim 1 may therefore be seen in finding an implementation for the control module with reduced complexity.

1.5 At the filing date of the present application, smartcards implemented as a subscriber identity module (SIM) card used in a mobile communication device and including an I/O interface and an SWP interface were well-known in the art. See, for example, document D6, page 302 and figure 9.29, which shows a connection module ("baseband controller") connected to the I/O-interface of the smartcard and a component ("NFC-Controller") connected to the SWP interface of the smartcard. Further, it was well-known that a SIM card could be used not only for identification and authentication but also for the tamper-proof execution of programs (see, e.g., D6, page 879, point 19.4.4, and page 904 to 910, point 19.4.4.6).

The device of D2 is program controlled, and the board notes that it was well-known that functions implemented in program could easily be concentrated in one controller, as long as it had enough processing power.

The skilled person, starting out from D2 and faced with the above-mentioned problem, would therefore, taking into account the common general knowledge, use the data processing capabilities and the interfaces of the smartcard for implementing the functions of the control module and for interfacing with the connection module and the component, thereby integrating the control module into the smartcard. As a result, the different interfaces for connecting the component to the control module are provided by the smartcard as specified by feature (b).

Features (c) and (d) further specify the interfaces to the component and the connection module and do not produce any synergistic effect with features (a) and (b). At the filing date, it was well-known to use the I/O interface of a smartcard for connecting it to a connection module (see, for example, D6, page 302, figure 9.29, "baseband controller") and to use an SWP interface for connecting it to a further component ("NFC-Controller", *ibid.*).

The skilled person, starting out from D2 and faced with the above-mentioned technical problem, would therefore, using common general knowledge, arrive at a device which includes all the features of claim 1, without exercising inventive skill.

1.6 Arguments of the appellant

The appellant argued that most of the interfaces depicted in Fig. 2 of D2 were mere software interfaces. The board notes, however, that claim 1 does not specify whether the interfaces between the control module and, respectively, the component and the connection module are software or hardware interfaces. Further, the M2M module 110 and the remote device 112 in Fig. 2 of D2 are hardware components, which implies that the interface between them is a hardware interface. Since the component 114 ("M2M GATEWAY", Fig. 2) is linked to the M2M module 110 via the base station 108 and the radio interface (Fig. 1), the other interface of the M2M module 110 shown in Fig. 2 implicitly includes a hardware interface to connect the Java virtual machine to the radio interface or the corresponding circuitry.

The appellant further argued that D2 did not provide a hint as to how the built-in SIM was integrated in the M2M device and that the interface for connecting to the remote device was not directly related to the built-in SIM. However, the board notes that, accepting that D2 does not disclose that the two interfaces shown in Fig. 2 between the control module and, respectively, the remote device and the connection module are directly related to the built-in SIM card, there is no suggestion in D2 which would prevent the skilled person, using common general knowledge, from using interfaces provided by the smartcard when integrating the control module into the smartcard.

Further, the appellant argued that in D2 the Java virtual machine was a key component in the device, which was needed to configure parameters of the M2M device in an easy way. If it had been the intention to run the Java virtual machine on the SIM, it would have been mentioned in D2. A SIM was usually used to provide a secure identification and/or authentication service in a mobile communication network and was only mentioned in D2 as a secondary aspect for connecting the M2M module to a communication network. Further, D2 disclosed that "Applications 120 use the services of the module's operating system and other supporting applications" (page 5, lines 11 and 12). Such an operating system was usually running on an application processor.

The board is not convinced by these arguments. At the filing date, smartcards with an operating system and what is known as Java Cards for executing Java programs were well-known. Further, although D2 relates to the configuration of parameters of an M2M module by means of a Java application (abstract and claim 1), it neither requires nor suggests that the SIM card used for establishing a connection to a wireless network and the means for running the Java virtual machine be kept as separate entities.

The appellant further argued that the smartcard of the device of claim 1 could only be accessed via the connection module by means of the restrictive code instructions which were available for communication via the I/O interface of the smartcard, which enhanced the security of the device. The technical problem was therefore to provide an improved M2M device. The board notes however that an enhanced security provided by the integration of the control module into the smartcard is not the only technical effect. Other formulations of the problem are possible, see above, in which enhanced security manifests itself as a bonus effect. In any case, formulating the problem as enhancing the security would all the more motivate the skilled person to implement the control module into a smartcard with data processing capabilities, an I/O interface, and an SWP interface.

1.7 In view of the above, the board concludes that the subject-matter of claim 1 does not involve an inventive step (Articles 52(1) and 56 EPC). The request is therefore not allowable.

2. Request for reimbursement of the appeal fee

According to Rule 103(1)(a) EPC, one of the conditions for a reimbursement of the appeal fee is that the board deems the appeal to be allowable. Since this condition is not met, the request for reimbursement of the appeal fee is to be rejected.

Order

For these reasons it is decided that:

1. The appeal is dismissed.

2. The request for reimbursement of the appeal fee is rejected.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets

S. Lichtenvort F. van der Voort

Decision electronically authenticated