

**Internal distribution code:**

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

**Datasheet for the decision  
of 19 February 2013**

**Case Number:** T 0662/10 - 3.5.03

**Application Number:** 00903728.4

**Publication Number:** 1151625

**IPC:** H04Q 7/32

**Language of the proceedings:** EN

**Title of invention:**

Method for the utilisation of applications stored on a subscriber identity module (SIM) and for the secure treatment of information associated with them

**Patent proprietor:**

TeliaSonera Finland Oyj

**Opponent:**

Giesecke & Devrient GmbH

**Headword:**

Utilisation of applications stored on a SIM/TELIASONERA

**Relevant legal provisions:**

EPC Art. 56, 99, 108

EPC R. 76(2)(c), 99(2), 111(2)

**Keyword:**

"Admissibility of opposition and opponent's appeal - yes"

"Inventive step (all requests) - no"

**Decisions cited:**

T 0220/83



Case Number: T 0662/10 - 3.5.03

**D E C I S I O N**  
**of the Technical Board of Appeal 3.5.03**  
**of 19 February 2013**

**Appellant 1:** TeliaSonera Finland Oyj  
(patent proprietor) Teollisuuskatu 15  
FI-00510 Helsinki (FI)

**Representative:** Turi, Michael  
Samson & Partner  
Patentanwälte  
Widenmayerstrasse 5  
D-80538 München (DE)

**Appellant 2:** Giesecke & Devrient GmbH  
(opponent) Prinzregentenstrasse 159  
D-81677 München (DE)

**Decision under appeal:** **Interlocutory decision of the opposition  
division of the European Patent Office posted  
27 January 2010 concerning maintenance of  
European patent No. 1151625 in amended form.**

**Composition of the Board:**

**Chairman:** F. van der Voort  
**Members:** A. J. Madenach  
R. Moufang

## Summary of Facts and Submissions

I. The present appeal arises from the decision of the opposition division posted on 27 January 2010 according to which it was found that, account having been taken of the amendments made by the patent proprietor during the opposition proceedings, European patent No. 1151625 and the invention to which it related met the requirements of the Convention.

The opposition was based on the grounds of Articles 100(a) and (b) EPC.

The opposition division came to the conclusion that, whereas the requirements of Article 83 EPC were met, the main request was not allowable because the subject-matter of claim 31 lacked novelty having regard to the disclosure of

O3: TS 100 977 v.6.1.0 (1998-07), "Digital cellular telecommunications systems (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 6.1.0 Release 1997)".

A first auxiliary request was held allowable. In particular, the subject-matter of claims 1, 19 and 31 was found to be novel over O3 and to involve an inventive step having regard to the disclosure of O3 in combination with either

O1: Rankl, W. et al.: "Handbuch der Chipkarten", 2. Auflage; pages 32, 122-127, 130-138, 393 and 407-414; Carl Hanser Verlag, Munich (DE), 1996

or

012: WO 93/20538 A1.

- II. A first appeal against the decision was filed by the patent proprietor (appellant 1) on 26 March 2010, the appropriate fee was paid and the statement of grounds of appeal was filed. Appellant 1 requested that the decision be set aside and that the patent be maintained as granted. As an auxiliary measure it requested that the patent be maintained in amended form on the basis of a set of claims, filed with the statement of grounds of appeal, which was identical to the set of claims as maintained by the opposition division. Oral proceedings were conditionally requested.
- III. A second appeal against the decision was filed by the opponent (appellant 2) on 29 March 2010, the appropriate fee was paid and the statement of grounds of appeal was filed. Appellant 2 requested that the appealed decision be set aside and that the patent be revoked in its entirety. Oral proceedings were requested as an auxiliary measure.
- IV. Further arguments were filed by appellant 1 with a letter received on 24 January 2011.
- V. The board summoned the appellants to oral proceedings. In a communication accompanying the summons, the board gave its preliminary opinion.
- VI. In preparation for the oral proceedings appellant 1 filed with a letter dated 21 January 2013 a set of

claims 1 to 30 of a second auxiliary request and maintained the previous main and auxiliary requests, the latter as first auxiliary request. Appellant 1 further announced that it would not be attending the oral proceedings.

VII. Oral proceedings took place on 19 February 2013 in the absence of appellant 1. After deliberation, the chairman announced the board's decision.

VIII. Independent claim 31 of the main request reads as follows:

"Subscriber identity module (SIM), comprising a data processing device (15), a storage device (16) connected to the data processing device (15), and a data transfer device (17) connected to the data processing device (15) and provided with a connection interface (IF) for the transfer of information between the mobile station (2) and the subscriber identity module (SIM), on which subscriber identity module (SIM) applications and encryption algorithms associated with encryption methods are stored, characterized in that the subscriber identity module (SIM) comprises means (4) for storing the keys needed for encryption and/or signature in a space (3) to which only a predetermined partition stored on the subscriber identity module SIM has a right of access in a given operating mode."

Claim 31 of the first auxiliary request reads as follows:

"Subscriber identity module (SIM) for the utilization of applications stored on the subscriber identity module (SIM) and for secure treatment of information associated with them in a telecommunication system, comprising

a data processing device (15),

a storage device (16) connected to the data processing device (15),

a data transfer device (17) connected to the data processing device (15) and provided with a connection interface (IF) for the transfer of information between the mobile station (2) and the subscriber identity module (SIM), on which subscriber identity module (SIM) applications and encryption algorithms associated with encryption methods are stored, characterised by

means (4) for storing the keys needed for encryption and/or signature in a distinct space (3) to which only a predetermined partition stored on the subscriber identity module SIM has a right of access in a subset mode, wherein an operating mode, comprising the subset mode and a normal communication mode, of the subscriber identity module (SIM) is selected by giving a predetermined code at start-up."

Independent claim 19 of the second auxiliary request reads as follows:

"System for the utilization of applications stored on a subscriber identity module (SIM) and for secure treatment of information associated with them in a telecommunication system comprising

a telecommunication network (1),  
a mobile station (2) connected to the  
telecommunication network (1), and  
a subscriber identity module (SIM) connected to  
the mobile station (2), said system comprising means  
for:  
starting the mobile station (2),  
giving a predetermined code by means of which a  
desired operating mode of the mobile station and the  
subscriber identity module (SIM) is selected,  
characterised by the desired operating mode comprising  
a normal mobile communication mode and a subset mode,  
and  
means (4) for saving the keys required for  
encryption and/or signature to the subscriber identity  
module (SIM), in a space (3) to which only a  
predetermined partition stored on the subscriber  
identity module SIM has a right of access in a given  
operating mode."

In view of the board's decision it is not necessary to  
recite the further independent claims.

## **Reasons for the Decision**

1. *Procedural matters*
- 1.1 Appellant 1, duly summoned, had informed the board that  
it would not be attending the oral proceedings, which  
were therefore held in its absence (Rule 115(2) EPC,  
Article 15(3) RPBA).

1.2 The present decision considers the admissibility of the appeal of appellant 2 and the admissibility of the opposition, issues which were also addressed in the board's communication, and is further based on objections under Article 52(1) EPC in combination with Article 56 EPC which had also been raised in the board's communication. Appellant 1 had the opportunity to present its comments on these objections. In deciding not to attend the oral proceedings appellant 1 chose not to make use of the opportunity to comment at the oral proceedings on any of the objections and, instead, to rely on the arguments set out in the statement of grounds of appeal and the letters dated 24 January 2011 and 21 January 2013, which the board duly considers below.

1.3 In view of the above and for the reasons set out below, the board was in a position at the oral proceedings to give a decision which complied with the requirements of Article 113(1) EPC.

2. *Admissibility of the appeals and the opposition*

2.1 The admissibility of the appeal by appellant 1 was not contested and the board sees no reason to question this. This appeal is therefore admissible.

2.2 Appellant 1 questioned the admissibility of appellant 2's appeal arguing that it was not substantiated.

In the board's view, the statement setting out the grounds of appeal filed by appellant 2 meets the standards applied by the boards in that it indicates



the reasons for setting aside the impugned decision and the facts and evidence on which the appeal is based, as required by Rule 99(2) EPC.

More specifically, in section I of the statement of grounds of appeal, the legal basis, *i.e.* insufficient disclosure, is indicated, as are the factual reasons why the decision is considered wrong in this respect, namely because a contradiction between the description and statements made during the oral proceedings before the opposition division on the one hand and the wording of the claim on the other hand results in a skilled person in the art not being able to carry out the invention, contrary to the requirement of Art. 83 EPC. Similarly, the legal basis and factual reasons are given in respect of the requirements of Art. 123 EPC (Section II of the grounds of appeal) and Art. 56 EPC (Section III and IV; including reasons as to why further documents should be admitted). With respect to the ground of lack of inventive step, the board notes that Rule 99(2) EPC does not require a specific way of indicating the facts and evidence, *e.g.* use of the so-called problem-and-solution approach. Appellant 2 nevertheless indicates, after a detailed analysis of document 03, what it considers to be the difference between the subject-matter of claim 31 and the disclosure of document 03 (point IV.2, first sentence) and it argues that this difference is known from other documents.

In summary, the statement of grounds of appeal of appellant 2 not only provides the legal and factual reasons on which the case for setting aside the decision is based, but also presents arguments which

enable the board to understand immediately why the decision is alleged to be incorrect and on what facts these arguments are based, without first having to make investigations of its own (T 220/83, OJ 1986, 249).

2.3 For these reasons, the appeal filed by appellant 2 is admissible.

2.4 Appellant 1 further argued that the opposition was not admissible on the ground that it was not substantiated as required by Rule 76(2)(c) EPC.

In this respect, the board notes that the notice of opposition introduces documents D1-D8 as prior art. Under section IV of the notice of opposition, features a to d, a31 and b31 of claims 1, 19 and 31 (*cf.* section II) of the patent as granted are compared with the disclosure of document D1 (now O1). It is concluded that the subject-matter of claims 1, 19 and 31 lacks novelty. It is true that the opponent did not clearly distinguish between independent claims 1, 19 and 31. It is, however, the board's understanding that the skilled reader would at least have been able to read section IV of the notice of opposition on claim 1 of the patent. With one ground of opposition substantiated, the opposition is admissible.

The board additionally notes with respect to the ground of lack of inventive step that according to the established case law there is no need for the opponent to expound on a lack of inventive step objection for the subject-matter of those claims which are argued to lack novelty. Still, in section V the notice of opposition gives arguments in support of a lack of

inventive step objection in respect of several of the dependent claims.

With respect to the ground of insufficient disclosure, the board notes that the notice of opposition explains in section III which particular feature ("a predetermined partition") is considered to be in conflict with the description. The opponent deduces from this conflict that it would be impossible for the skilled person to carry out the claimed invention. The board considers here too that the notice of opposition meets the requirements of Rule 76(2)(c) EPC.

2.5 For these reasons, the opposition is admissible.

2.6 Appellant 1 further argued that the interlocutory decision lacked reasoning (Rule 111(2) EPC) with respect to the admissibility of the opposition.

The board notes however that in the decision (point II, A) 1.) the opposition division indicated that, for the grounds of opposition according to Article 100(a) and (b) EPC, corresponding facts in the form of substantiated arguments and evidence - with references to passages of the patent specification in the case of Article 100(b) EPC, and an analysis of claimed features with references to prior-art documents in the case of Article 100(a) EPC - were mentioned in the notice of opposition, and that both the proprietor's representatives and the opposition division had been able to analyse the arguments without any further investigation. The board indeed notes that the notice of opposition, in particular its section IV, meets the generally accepted standards for admissibility.

2.7 For these reasons, the board concludes that the interlocutory decision is sufficiently reasoned on this point as required by Rule 111(2) EPC.

3. *Claim 31 of the first auxiliary request, inventive step (Articles 52(1) and 56 EPC)*

3.1 The subject-matter of claims 31 of the main request and the first auxiliary request relates to a subscriber identity module and was deemed by the opposition division to have the broadest scope (point II, B) 2.1 of the decision under appeal). Further, claim 31 of the first auxiliary request encompasses all the features of claim 31 of the main request. Claim 31 of the first auxiliary request will be considered first.

3.2 The board considers O3 as representing the closest prior art for the subject-matter of claim 31.

O3 is a technical specification defining the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of GSM as well as those aspects of the internal organisation of the SIM which are related to the network operation phase (page 9, first paragraph). Hence, O3 relates to a subscriber identity module (SIM). By reference to further technical specifications of the SIMs to which O3 applies (pages 9 and 10) and in view of the fact that the SIM is capable of executing commands (p. 17, point 5.6) and capable of storing algorithms and keys (p. 27, points 7.1 and 7.2), it is implicit that the SIM comprises a data processing device, a storage device connected to the data

processing device, and a data transfer device connected to the data processing device and provided with a connection interface for the transfer of information between the mobile station and the SIM. Nor has it ever been contested that the SIM as described in O3 disclosed these features.

The general structure of files stored on the SIM is shown in Figure 3 (page 22), Figure 7 (page 26) and Figure 8 (page 90). The file structure consists of a master file (MF), dedicated files (DF), and elementary files (EF). Examples of dedicated files are DF<sub>GSM</sub>, DF<sub>TELECOM</sub>, and DF<sub>IS-41</sub>, which may coexist on a multi-application card (pages 23 and 90).

Section 11.2.1 (pages 93 and 94) describes the SIM initialisation procedure, which comprises the ME selecting the dedicated file DF<sub>GSM</sub> and the running of the CHV1 (card holder verification, see page 28) verification procedure. After successfully performing the CHV1 verification, a number of procedures are run by the ME, including *inter alia* the Cipher Key request (page 94). The ciphering key Kc is the key for ciphering transmissions under GSM and, together with other keys, e.g. ciphering key KcGPRS (page 74), is intended to insure the secure treatment of information in a telecommunication system (pages 12, 27 and 54). After successful completion of the SIM initialisation, the mobile station is ready for a GSM session (page 94). The above-mentioned procedure is an application in the sense defined in O3 in section 3.1 (page 11), since it comprises a set of security mechanisms (verification procedure), files (DF<sub>GSM</sub>), data (the elementary files (EF) involved) and protocols (set of procedures

required by the application). It follows that the SIM is for the utilisation of an application stored on it and for the secure treatment of information associated with it, *i.e.* in this case the ciphering of transmissions under GSM.

The ciphering keys are stored as corresponding files, *e.g.* EF<sub>KC</sub> and EF<sub>KCGPRS</sub>, on the SIM card (see the file structure of Figure 8, page 90). Hence, the keys needed for encryption are stored in a space which is a distinct space, since it is dedicated to the storage of the ciphering keys. It follows from the initialisation procedure mentioned above that only a predetermined partition stored on the SIM has a right of access to the ciphering keys.

3.3 The subject-matter of claim 31 of the first auxiliary request differs from the SIM card disclosed in O3 in that the right of access to the stored keys is in a subset mode, wherein an operating mode, comprising the subset mode and a normal communication mode, of the SIM is selected by giving a predetermined code at start-up.

3.4 Since the term "subset mode" has no specific meaning in the art, it is understood by the board in its broadest sense and, hence, includes a communication mode. This understanding is not changed by the statement in the description of the patent in suit that a "subset mode" is used as a synonym for a "security mode" (*cf.* paragraph [0014] of the patent specification), since a communication mode which uses ciphering keys, as in GSM, may also be understood as a security mode. Further, the board does not see any difference between a "normal"

communication mode, as referred to in the claim, and a communication mode.

With this understanding, which is at variance with that of the opposition division, the problem underlying the claimed subject-matter when starting from O3 may be seen in expanding the functions of the known SIM card in order to give the user a choice between several usage modes, at least one of which comprises a restricted right of access.

- 3.5 This problem and its solution are already suggested to the skilled person by O3. The file structure shown in section 6.6 (page 26) and in Figure 8 (page 90) of O3 includes at the same level as DF<sub>GSM</sub> the further files DF<sub>TELECOM</sub> and DF<sub>IS-41</sub>. O3 is specifically concerned with the interface between the SIM and the ME for use during the network operation phase of GSM (page 9, first paragraph), with the consequence that after SIM activation the ME selects DF<sub>GSM</sub> (section 11.2.1, second paragraph, page 93). Considering that further network operation possibilities like DF<sub>TELECOM</sub> and DF<sub>IS-41</sub> exist on the SIM card, it would have been obvious to the skilled person that a user should be able to make use of them. An obvious way of using network operations under, say, IS-41, which is a further mobile communication standard existing in parallel to the GSM standard, would be to replace the selection of DF<sub>GSM</sub> by the ME (section 11.2.1, second paragraph, page 93) by a user selection between DF<sub>GSM</sub> and DF<sub>IS-41</sub>. User selection must obviously involve entering a code. Hence, the desired operating mode would be selected by giving a predetermined code at start-up. Furthermore, in the above example with network operations under IS-41, there would be two

communications modes both using encryption. Hence, the desired operating mode would always be a communication mode with a security feature. It follows that both the GSM mode and the IS-41 mode may be considered as normal communication modes or subset modes. At least when the GSM mode is considered as corresponding to the subset mode, the right of access is reserved to a predetermined partition stored on the SIM, as already explained at point 3.2 above.

3.6 From the above, it follows that, starting out from the disclosure of O3, the person skilled in the art would have arrived at the subject-matter of claim 31 without the exercise of inventive skill.

3.7 Appellant 1 argued that according to claim 31 applications and encryption algorithms associated with encryption methods were stored additionally to the typical storage of the temporal key for speech encryption/decryption (e.g. the file  $EF_{Kc}$  in O3) and that speech encryption/decryption was not an application run on the SIM.

The board notes however that the claim does not include the feature of an additional storage of algorithms and the feature of an application which runs on the SIM. As to the latter point, the board furthermore notes that claim 31 is directed to a SIM, *i.e.* a product, and that it is difficult to see how a SIM can be defined in terms of an application running on it.

Appellant 1 further argued with reference to the description at paragraph [0015] that the feature "distinct space" expressed a specific hardware space in



contrast to a logical space as in O3 (*cf.* the dedicated files EF<sub>KC</sub> and EF<sub>GPRS</sub>). The board cannot accept this argument. In the board's view, a SIM which consists of various partitions (*cf.* paragraph [0015] of the patent specification) allows an interpretation according to which these partitions are logical in nature. In the language of computing the wording "a distinct space ... is set apart ..." (*cf.* paragraph [0015]) does not imply that the space is a physical space. The further argument that a physical "space" would allow storing of more than one key, unlike the logical space used in O3 for the ciphering keys, disregards the possibility that the term "space" can denote more than one logical space. The board also notes that claim 31 is directed to a "subscriber identity module ... comprising ... means (4) for storing the keys". Claim 31 does not require that the "distinct space" be in addition to the "storage device" which is part of the SIM. "Distinct" is rather understood as referring to a dedicated space.

Appellant 1 further argued that if the mobile device and the SIM can be put into a specific operating mode by inputting a predetermined code, in which mode the space in which the key is stored is accessible, this space would not be accessible in the normal mobile communication mode. This argument is not convincing, since in a GSM communication mode ciphering keys are also used and, hence, accessible (see point 3.4 above). In any case, the claim is silent on access rights in other modes.

Appellant 1 further argued that under GSM speech data was encrypted in the mobile station and not in the SIM. This may be correct, but the board fails to see how the

feature according to which applications and encryption algorithms associated with encryption methods are stored on the SIM would exclude an encryption which is to be performed by the mobile device.

A further point raised by appellant 1 is the presumed connection between the features "on which subscriber identity module (SIM) applications and encryption algorithms associated with encryption methods are stored" and "means (4) for storing the keys needed for encryption and/or signature in a distinct space" in the sense that the keys were necessarily related to the stored applications and encryption algorithms. The board notes that the claim formulation is such that it leaves this open.

Further, appellant 1 referred to section 7.3 (first paragraph) of 03 according to which "No file access conditions are currently assigned by GSM to the MF and DFs.". This was said to have the consequence that no file access conditions were defined over whole directories. The board, however, considers the relevant access procedure to be implemented by the SIM initialisation as described in section 11.2.1, independently of an individual file access. This initialisation is relevant for the entire ME and DF<sub>GSM</sub>, as shown at point 3.2 above.

3.8 The board thus concludes that the subject-matter of claim 31 of the first auxiliary does not involve an inventive step (Article 56 EPC). This request is therefore not allowable.

4. *Claim 31 of the main request, inventive step (Articles 52(1) and 56 EPC)*

4.1 Claim 31 of the main request is broader in scope than claim 31 of the first auxiliary request (see point VIII above). *Inter alia*, it does not specify that the right of access is in a subset mode which is itself an operating mode, the operating modes comprising a subset mode and a normal communication mode.

4.2 It follows that the main request is not allowable either.

5. *Claim 19 of the second auxiliary request, inventive step (Articles 52(1) and 56 EPC)*

5.1 The subject-matter of claim 19 of the second auxiliary request does not give rise to considerations as regards the SIM other than those set out above in respect of claim 31 of the first auxiliary request.

Claim 19 of the second auxiliary request is directed to a system comprising a telecommunication network, a mobile station connected to the telecommunication network, and a SIM connected to the mobile station.

O3 specifically discloses the interface between a SIM and a mobile station (ME in O3) for use during network operations of a telecommunication network (GSM in O3, see section 1, first paragraph, page 9). Hence, O3 describes a system having the above features.

Further, the known system is for the utilisation of applications stored on the SIM and for secure treatment

of information associated with them in a telecommunication system, as follows from the reasoning in point 3.2 above. It is implicit that the known system includes means for starting the mobile station, namely in order to be in a position to activate (section 4.3.2, page 14) and initialise (section 11.2.1, page 93) the SIM.

For the reasons set out at points 3.4 and 3.5 above it was obvious to the skilled person to provide means for giving a predetermined code used to select a desired operating mode of the mobile station and the SIM, wherein the desired operating mode comprises a normal mobile communication mode and a subset mode.

Finally (see point 3.2 above) the known system comprises means for saving the keys required for encryption to the SIM in a distinct space to which only a predetermined partition stored on the subscriber identity module SIM has a right of access in a given operating mode.

5.2 With respect to claim 19, appellant 1 specifically argued that the claimed system required more than one operating mode to be available for selection by a respective predetermined code. The board notes however that the presence of more than one operating mode is known from O3 and that the selection between them would have been obvious to the skilled person for the reasons set out at points 3.4 and 3.5 above.

5.3 It follows that the subject-matter of claim 19 of the second auxiliary request does not involve an inventive

step (Article 56 EPC). The request is therefore not allowable.

6. Since none of the requests of the patent proprietor is allowable, the patent is to be revoked.

## **Order**

### **For these reasons it is decided that:**

1. The decision under appeal is set aside.
2. The patent is revoked.

The Registrar:

The Chairman:

G. Rauh

F. van der Voort