Internal distribution code:

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

Datasheet for the decision of 30 November 2020

Case Number: T 1974/16 - 3.5.03

Application Number: 11749378.3

Publication Number: 2601771

IPC: H04L29/06

Language of the proceedings: EN

Title of invention:
System and method for securely using multiple subscriber profiles with a security component and a mobile telecommunications device

Patent Proprietor:
Thales Dis France SA

Opponent:
Giesecke+Devrient Mobile Security GmbH

Headword:
Multiple subscriber profiles/THALES

Relevant legal provisions:
EPC Art. 100(a), 54
RPBA Art. 12(4)
RPBA 2020 Art. 12(8)

Keyword:
Decision in written proceedings: no oral proceedings necessary
Novelty - main request (no)
Admittance of new requests - all auxiliary requests (no): should have been filed earlier

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 1974/16 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 30 November 2020

Appellant: (Patent Proprietor)	Thales Dis France SA 6, rue de la Verrerie 92190 Meudon (FR)
Respondent: (Opponent)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 24 June 2016 revoking European patent No. 2601771 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	K. Schenkel
	R. Winkelhofer

Summary of Facts and Submissions

I. This appeal of the patent proprietor is against the decision of the opposition division to revoke the opposed patent for lack of novelty having regard to the disclosure of

D4: WO 2008/128874 A1.

II. The appellant requests that the decision under appeal be set aside and that the opposition be rejected (**main request**), i.e. the patent be maintained as granted, or, in the alternative, that the patent be maintained on the basis of one of **first to third auxiliary requests** filed with the statement of grounds of appeal.

III. The respondent (opponent) has not filed any observations or requests.

IV. Claim 1 of the **main request** (patent as granted) reads as follows (labelling added by the board):

(a) "A method for allowing a mobile telecom device to use multiple subscriber profiles, a subscriber profile including the full set of data associating a particular subscriber to an operator, said method comprising:
(b) - operating a security function to perform a cryptographic operation on a subscriber profile using a cryptography key of the security function thereby producing a cryptographically protected profile;
(c) - storing the cryptographically protected subscriber profile;

(d) - activating the cryptographically protected subscriber profile by operating the security function to verify that the cryptographically protected subscriber profile has been cryptographically protected using the cryptography key of the security function, and upon verifying that the cryptographically protected subscriber profile has been protected using the cryptography key of the security function, activating the cryptographically protected subscriber profile."

V. Claim 1 of the **first auxiliary request** differs from claim 1 of the main request in that features (b) and (d) read as follows (board's underlining indicating changes vis-à-vis claim 1 as granted):

(b) "- operating a security function in said mobile telecom device to perform a cryptographic operation on a subscriber profile using a cryptography key of the security function thereby producing a cryptographically protected profile";

(d) "- activating the cryptographically protected subscriber profile by operating the security function in said mobile telecom device to verify that the cryptographically protected subscriber profile has been cryptographically protected using the cryptography key of the security function, and upon verifying that the cryptographically protected subscriber profile has been protected using the cryptography key of the security function in said mobile telecom device, activating the cryptographically protected subscriber profile in said mobile telecom device".

VI. Claim 1 of the **second auxiliary request** differs from claim 1 of the main request in that features (b) and (d) read as follows (board's underlining indicating changes vis-à-vis claim 1 as granted):

(b) "- operating by a secure zone of said mobile telecom device or by a UICC comprised in said mobile telecom device a security function to perform a cryptographic operation on a subscriber profile using a cryptography key of the security function thereby producing a cryptographically protected profile";

(d) "- activating the cryptographically protected subscriber profile by operating the security function in said mobile telecom device to verify that the cryptographically protected subscriber profile has been cryptographically protected using the cryptography key of the security function, and upon verifying that the cryptographically protected subscriber profile has been protected using the cryptography key of the security function, activating the cryptographically protected subscriber profile in said secure zone of said mobile telecom device or said UICC".

VII. Claim 1 of the **third auxiliary request** differs from claim 1 of the main request in that features (b), (c) and (d) read as follows (board's underlining indicating changes vis-à-vis claim 1 as granted):

(b) "- operating by a secure zone of said mobile telecom device or by a UICC comprised in said mobile telecom device a security function to perform a cryptographic operation on a subscriber profile using a cryptography key of the security

function thereby producing a cryptographically protected profile";

(c) "- storing the cryptographically protected subscriber profile outside of said secure zone";

(d) "- importing and activating the cryptographically protected subscriber profile in said secure zone by operating the security function in said mobile telecom device to verify that the cryptographically protected subscriber profile has been cryptographically protected using the cryptography key of the security function, and upon verifying that the cryptographically protected subscriber profile has been protected using the cryptography key of the security function, activating the cryptographically protected subscriber profile in said secure zone of said mobile telecom device".

Reasons for the Decision

1. Decision in written proceedings

Given that the parties did not request oral proceedings before the board under Article 116(1) EPC and that the board does not consider holding oral proceedings expedient or necessary, this decision is handed down in writing (cf. Article 12(8) RPBA 2020).

2. Background of the opposed patent

The present patent relates to the management of profiles of a subscriber for accessing a telecommunication network by means of a mobile device

and in particular to a method of allowing the use of multiple subscriber profiles.

3. Main request - claim 1 - novelty (Article 54 EPC)

3.1 Preliminary observations as to the claim features

3.1.1 Claim 1 of the main request does not specify which device carries out steps (b), (c) or (d).

3.1.2 Further, although feature (a) mentions "multiple subscriber profiles", in the method, only *one* is activated and hence used by the "mobile telecom device". Thus, the method of claim 1 does not require that *multiple* subscriber profiles really exist but only that *one* of a conceivable multiplicity of profiles can be used as input for steps (b) to (d).

3.2 Prior-art document **D4** relates to the transfer of "soft SIM credentials" (i.e. a subscriber profile) from a "transferring mobile device" to a "target mobile device" (cf. abstract and page 1, lines 11 to 14). The transfer method of D4 allows a mobile device (target mobile device) to use multiple subscriber profiles since the soft SIM credentials of any transferring mobile device out of a conceivable multiplicity of mobile devices can be transferred.

The subscriber profile is transferred via a secure connection which uses cryptographic operations, such as authentication, and which may include encryption using a cryptographic key (page 5, lines 20 to 29). The result of such an operation is a cryptographically protected (subscriber) profile.

The target mobile device verifies the received cryptographically protected profile and, in case of a successful verification, activates it (page 5, line 29 to page 6, line 7). The verification may include decrypting the received profile which implies the verification of the key used for encrypting the profile (page 5, line 29 to page 6, line 5). In order to enable the necessary cryptographic operations on the target mobile device, the protected profile is implicitly stored.

3.3 Using the language of present claim 1, **D4** discloses

(a) A method for allowing a mobile telecom device to use multiple subscriber profiles ("soft SIM credentials" of multiple transferring mobile devices; page 5, lines 5 and 6), a subscriber profile including the full set of data associating a particular subscriber to an operator (credentials, e.g. a subscriber key corresponding to a user; page 1, lines 11 to 14), said method comprising:

(b) operating a security function to perform a cryptographic operation on a subscriber profile using a cryptography key of the security function thereby producing a cryptographically protected profile (the transferring device may encrypt the soft SIM credentials using the target device's key; see page 5, lines 20 to 29);

(c) storing the cryptographically protected subscriber profile (implied by the fact that the target mobile device verifies and installs the received profile, necessarily requiring the storage of the profile; see page 5, lines 29 und 30);

(d) activating the cryptographically protected subscriber profile by operating the security

function to verify that the cryptographically protected subscriber profile has been cryptographically protected using the cryptography key of the security function (the received SSIM is verified by decrypting it and checking associated signatures/keys; page 5, line 29 to page 6, line 7), and upon verifying that the cryptographically protected subscriber profile has been protected using the cryptography key of the security function, activating the cryptographically protected subscriber profile (if able to verify, the received SSIM is installed/activated; page 6, lines 5 to 7).

3.4 D4 therefore discloses a method with **all** the features of claim 1 of the main request.

3.5 The appellant argues that document D4's purpose is only to transfer an SSIM from one mobile terminal to another mobile terminal and not to export a subscriber profile and to import it later on the same terminal.

The board notes that the method of claim 1 is not limited to a method in which steps (b) and (d) are executed in the same mobile terminal.

3.6 Consequently, claim 1 is not new over D4. The main request is therefore not allowable under Articles 52(1) and 54 EPC.

4. First to third auxiliary requests - claim 1 (Article 12(4) RPBA 2007)

4.1 In accordance with Article 12(4) RPBA 2007, Article 25(2) RPBA 2020, the board has the power to hold inadmissible requests which could have been

presented during the first-instance (here: opposition) proceedings.

4.2 Claim 1 of the **first auxiliary request** differs from claim 1 of the main request in that features (b) and (d) are carried out in the mobile device which is to be allowed to use multiple subscriber profiles.

4.3 To the same effect, claim 1 of the **second and third auxiliary requests** states that the steps of features (b) and (d) are carried out "in a secure zone of the mobile device".

4.4 Those amendments substantially change the whole set-up since they now define in which *components* of a telecommunication system the essential steps are performed. Thus, auxiliary requests adding such limitations in order to differentiate the claimed subject-matter over the disclosure of D4 or the other prior-art documents, which had been introduced by the opponent, could and *should* have been filed already in the opposition proceedings.

4.5 The appellant did neither file any claim request nor defended the patent during the opposition proceedings.

4.6 In view of the above, the board has decided not to admit first to third auxiliary requests into the appeal proceedings (Article 12(4) RPBA 2007, Article 25(2) RPBA 2020).

5. As there is no allowable request on the basis of which the opposed patent can be maintained, the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated