Internal distribution code:

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

Datasheet for the decision of 14 April 2020

Case Number: T 0953/16 - 3.5.03

Application Number: 10165524.9

Publication Number: 2395781

IPC: H04W12/08, H04W12/02, H04Q3/00, H04L29/06

Language of the proceedings: EN

Title of invention:
Method and system for secure provisioning of a wireless device

Applicant:
BlackBerry Limited

Headword:
Secure provisioning of a wireless device/BLACKBERRY

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 13(2)

Keyword:
Inventive step - main and first auxiliary request (no): juxtaposition of well-known features
Admission of auxiliary requests filed after notification of summons - (no): no exceptional circumstances

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 0953/16 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 14 April 2020

Appellant: (Applicant)	BlackBerry Limited 2200 University Avenue East Waterloo, ON N2K 0A7 (CA)
Representative:	Gill Jennings & Every LLP The Broadgate Tower 20 Primrose Street London EC2A 2ES (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 24 September 2015 refusing European patent application No. 10165524.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	K. Bengi-Akyürek
Members:	J. Eraso Helguera
	R. Romandini

Summary of Facts and Submissions

I. An appeal was lodged by the applicant against the decision of the examining division refusing the present European patent for lack of inventive step with respect to the independent claims of each of a main request, a first and a second auxiliary request.

II. In its decision, the examining division referred *inter alia* to the following prior-art documents:

D1: WO 2009/002042 A2;

D2: GB 2 414 138 A;

D4-1: Menezes A et al.: "Handbook of Applied Cryptography", CRC Press, 1997, pp. 397-399.

III. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims of either of a **main request** and a **first auxiliary request**, both filed with the statement of grounds of appeal, or, in the alternative, on the basis of the claims of either of a **second** and a **third auxiliary request**, both filed with a reply to the summons to oral proceedings issued by the board. With the reply, the appellant informed the board that it would not be attending the oral proceedings and requested a final decision.

IV. The board then cancelled the oral proceedings.

V. Claim 1 of the **main request** reads as follows:

"A method of enabling one or more communication services on a wireless device (201), wherein the method is performed in a system that comprises a device developer provisioning system (308), a carrier provisioning system (306) and a wireless device (201), the method comprising:

receiving, at the device developer provisioning system (308), a request from the carrier provisioning system (306) for provisioning information to provision the wireless device (201), the request indicating a setting on the wireless device that is to be varied by the provisioning information, the carrier provisioning system (306) being connected to the wireless device (201) through a wireless network;

generating provisioning information using a private algorithm on the device developer provisioning system (308), wherein the private algorithm is an algorithm which is unknown to the carrier provisioning system (306);

securing the provisioning information at the device developer provisioning system (308), to produce secure provisioning information, wherein the secure provisioning information contains time information, added to the provisioning information prior to encryption, indicating currency of the provisioning information, and wherein the wireless device (201) is configured to ignore the encrypted secure provisioning information if the provisioning information is not sufficiently current;

sending the secure provisioning information from the device developer provisioning system (308) to the carrier provisioning system (306) for transmission to the wireless device (201); and

sending the secure provisioning information corresponding to the request from the carrier

provisioning system (306) to the wireless device (201);
wherein the secure provisioning information is kept confidential between the device developer provisioning system (308) and the wireless device (201)."

Claim 1 of the **first auxiliary request** reads (board's underlining indicating additions with respect to claim 1 of the main request):

"A method of enabling one or more communication services on a wireless device (201), wherein the method is performed in a system that comprises a device developer provisioning system (308), a carrier provisioning system (306) and a wireless device (201), the method comprising:
receiving, at the device developer provisioning system (308), a request from the carrier provisioning system (306) for provisioning information to provision the wireless device (201), the request indicating a setting on the wireless device that is to be varied by the provisioning information, the carrier provisioning system (306) being connected to the wireless device (201) through a wireless network;
generating provisioning information using a private algorithm on the device developer provisioning system (308), wherein the private algorithm is an algorithm which is unknown to the carrier provisioning system (306);
securing the provisioning information at the device developer provisioning system (308), to produce secure provisioning information, wherein the secure provisioning information contains time information, added to the provisioning information prior to

encryption, indicating currency of the provisioning information, and wherein the wireless device (201) is configured to ignore the encrypted secure provisioning information if the provisioning information is not sufficiently current;
sending the secure provisioning information from the device developer provisioning system (308) to the carrier provisioning system (306) for transmission to the wireless device (201), wherein the secure provisioning information is kept confidential between the device developer provisioning system (308) and the wireless device (201);
generating further provisioning information by the carrier provisioning system (306); and
sending (418) the secure provisioning information corresponding to the request and the further provisioning information from the carrier provisioning system (306) to the wireless device (201)."

Claim 1 of the **second auxiliary request** reads (board's underlining indicating additions with respect to claim 1 of the main request):

"A method of enabling one or more communication services on a wireless device (201), wherein the method is performed in a system that comprises a device developer provisioning system (308), a carrier provisioning system (306) and a wireless device (201), the method comprising:
receiving, at the device developer provisioning system (308), a request from the carrier provisioning system (306) for provisioning information to provision the wireless device (201), the request indicating a setting on the wireless

device that is to be varied by the provisioning information, the carrier provisioning system (306) being connected to the wireless device (201) through a wireless network;
generating provisioning information using a private algorithm on the device developer provisioning system (308), wherein the private algorithm is an algorithm which is unknown to the carrier provisioning system (306);
securing the provisioning information at the device developer provisioning system (308), to produce secure provisioning information, wherein securing the provisioning information comprises encrypting the provisioning information and wherein the secure provisioning information contains time information, added to the provisioning information prior to encryption, indicating currency of the provisioning information, and wherein the wireless device (201) is configured to ignore the encrypted secure provisioning information if the provisioning information is not sufficiently current;
sending the secure provisioning information from the device developer provisioning system (308) to the carrier provisioning system (306) for transmission to the wireless device (201); and
sending the secure provisioning information corresponding to the request from the carrier provisioning system (306) to the wireless device (201);
wherein the step of securing ensures the secure provisioning information is kept confidential between the device developer provisioning system (308) and the wireless device (201)."

Claim 1 of the **third auxiliary request** reads (board's underlining indicating additions with respect to claim 1 of the main request):

"A method of enabling one or more communication services on a wireless device (201), wherein the method is performed in a system that comprises a device developer provisioning system (308), a carrier provisioning system (306) and a wireless device (201), the method comprising:

receiving, at the device developer provisioning system (308), a request from the carrier provisioning system (306) for provisioning information to provision the wireless device (201), the request indicating a setting on the wireless device that is to be varied by the provisioning information, the carrier provisioning system (306) being connected to the wireless device (201) through a wireless network;

generating provisioning information using a private algorithm on the device developer provisioning system (308), wherein the private algorithm is an algorithm which is unknown to the carrier provisioning system (306);

securing the provisioning information at the device developer provisioning system (308), to produce secure provisioning information, <u>wherein securing the provisioning information comprises encrypting the provisioning information and</u> wherein the secure provisioning information contains time information, added to the provisioning information prior to encryption, indicating currency of the provisioning information, and wherein the wireless device (201) is configured to ignore the encrypted secure provisioning information if the provisioning information is not sufficiently current;

sending the secure provisioning information from the device developer provisioning system (308) to the carrier provisioning system (306) for transmission to the wireless device (201), wherein the step of securing ensures the secure provisioning information is kept confidential between the device developer provisioning system (308) and the wireless device (201); generating further provisioning information by the carrier provisioning system (306); and sending (418) the secure provisioning information corresponding to the request and the further provisioning information from the carrier provisioning system (306) to the wireless device (201)."

Reasons for the Decision

1. MAIN REQUEST

1.1 Claim 1 - inventive step (Articles 52(1) and 56 EPC)

1.1.1 The present application distinguishes between core communication services, provided by a wireless carrier, and value added services, provided by a third party value added service provider ("VASP"), for example, a manufacturer or a developer of the wireless device (see paragraph [0003]). The manufacturer or developer of the wireless device (acting as VASP) may wish to keep certain provisioning information or methods of generating provisioning information private, that is, secret from wireless carriers and others (see paragraph [0069]), while still using the carrier provisioning system to send the value-added service provisioning

information to the wireless device (see paragraph [00120]).

1.1.2 In order to achieve this goal, public or private key encryption may be employed to transfer encrypted (or otherwise secure) data from a device developer provisioning system to the wireless device (see paragraph [0070]). To provide even greater security, provisioning information received from the device developer provisioning system may be time and/or date stamped (see paragraph [0071]).

1.1.3 In view of the problem identified in the application, the board considers document **D1** to be the most promising springboard towards the invention, because D1 also relates to a method of enabling communication services on a wireless device (see D1, page 8, lines 16-22). Just like in the application, D1 distinguishes between carrier provisioning information ("first type of OTA data") and value-added service provisioning information ("second type of OTA data"). Both types of OTA data are secured through encryption at the carrier provisioning system ("OTA server") before being sent together to the mobile terminal.

1.1.4 Using the wording of present claim 1, **D1** discloses (board's outline):

A method of enabling one or more communication services on a wireless device ("mobile terminal 120"), wherein the method is performed in a system that comprises a device developer provisioning system ("database 141"), a carrier provisioning system ("OTA server 140") and a wireless device (see e.g. Fig. 1), the method comprising:

(a) receiving, at the device developer provisioning system, a request from the carrier provisioning system for provisioning information to provision the wireless device, the request indicating a setting on the wireless device that is to be varied by the provisioning information (see p. 8, l. 23-24: "The OTA server may search the database for the OTA data ..."), the carrier provisioning system being connected to the wireless device through a wireless network (see Fig. 1);

(b) generating provisioning information ("second type of OTA data") (see p. 7, l. 8-13: "OTA data, such as ... mobile applications (hereinafter 'applets') corresponding to various types of additional services ..."; see p. 9, l. 9-15: "... a second type of OTA key that is used for service information such as an applet for the use of an additional service ..."; see p. 9, l. 22-25: "If the requested OTA data is a second type of OTA data ...");

(c) securing the provisioning information at the carrier provisioning system to produce secure provisioning information ("second type of encrypted OTA data") (see p. 9, l. 5-15: "Such OTA keys for encrypting OTA data may include ... a second type of OTA key that is used for service information such as an applet for the use of an additional service ..."; see p. 9, l. 22-25: "If the requested OTA data is a second type of OTA data, the OTA server may create a second type of encrypted OTA data by encrypting the second type of OTA data using a second type of OTA key ..."),

(d) sending the secure provisioning information corresponding to the request from the carrier provisioning system to the wireless device (see p. 10, l. 10-13: "Thereafter, the OTA server may

send the created message to the message center ... The message center may send the message to the mobile terminal ...").

1.1.5 The subject-matter of claim 1 thus differs from the method known from D1 in the following features (board's underlining):

(e) the provisioning information is generated using a private algorithm on the device developer provisioning system, wherein the private algorithm is an algorithm which is unknown to the carrier provisioning system, is secured at the device developer system and sent to the carrier provisioning system for transmission to the wireless device;
(f) the secure provisioning information is kept confidential between the device developer provisioning system and the wireless device;

(g) the secure provisioning information contains time information, added to the provisioning information prior to encryption, indicating currency of the provisioning information;
(h) the wireless device is configured to ignore the encrypted secure provisioning information if the provisioning information is not sufficiently current.

1.1.6 In the following analysis, "securing the provisioning information" in feature (c) has been interpreted to involve encryption, whereas feature (f) has been interpreted as a result of the preceding steps, in particular of the securing step, in line with the appellant's interpretation in its reply to the summons.

1.1.7 Thus, the technical effects achieved by these features are considered to be the following:

Re: features (e) and (f)
- by generating the provisioning information using a private algorithm and securing it at the device developer provisioning system, it is ensured that this information is kept secret from the carrier wireless system, e.g. due to an administrative security policy.

Re: features (g) and (h)
- by introducing time information before encryption, uniqueness and timeliness are provided, protecting the system against replay and interleaving attacks and enhancing thereby security.

1.1.8 The subject-matter of claim 1 does not involve an inventive step for the following reasons:

1.1.9 The two groups of distinguishing features are associated with independent partial objective problems. This means in turn that the contribution of those features to an inventive step can be individually assessed, i.e. on the merits of each group of distinguishing features *per se*.

1.1.10 As regards the first group of distinguishing features, database 141 of D1 may assemble and manage OTA data to be installed or stored in the smart card (see D1, page 8, lines 1-2). Such OTA data does not merely include carrier-related information, but also information corresponding to other additional services in the financial, communication, medical, security and broadcasting fields (see D1, page 7, lines 8-13).

It would be apparent for the skilled person that under certain administrative circumstances, e.g. if the *service* provider is not the *carrier* provider, the information corresponding to the additional service should be fed into the database by an external device developer system and the carrier provisioning system need not be privy to the algorithm used for its generation or to its actual content. The carrier provisioning system should not be able to tamper with it either.

In such a case, the most straightforward option available to the skilled person would be to secure the information right at the device developer system (i.e. at database 141 of D1), e.g. by encrypting or digitally signing it, so that the information about that service stored in the database and accessed by the OTA server of D1 would already be secured by the source, i.e. by the device developer system.

1.1.11 As regards the second group of distinguishing features, incorporating time-stamping information before performing encryption is a well-known measure in the field of security (see e.g. **D4-1**, page 399, last paragraph: "Timestamps may be used to provide timeliness and uniqueness guarantees, to detect message replay ...").

Thus, the skilled person starting out from D1 and seeking to ensure a high level of confidentiality and integrity for the information provisioned by a service provider to a mobile terminal over a carrier provisioning system would arrive at the claimed subject-matter by the mere exercise of measures commonly known in the field of network security and

without the involvement of any inventive skills.

1.1.12 In view of the above, the board concludes that the two groups of distinguishing features are associated with distinct partial objective problems. They represent a mere juxtaposition of features which are not functionally interdependent and do not mutually influence each other to achieve a synergistic technical effect over and above the sum of their respective individual effects.

1.1.13 The appellant submitted, securing the information to ensure its confidentiality was provided through both **encryption**, as implied by feature (e), and using time information according to the features of the second group, i.e. features (g) and (h). Thus, these features were clearly functionally dependent on each other as they achieved the synergistic effect of ensuring security of the provisioning information between a device developer system and the wireless device such that the information remained confidential and to ensure that it was current, i.e. up-to-date. There was nothing in D1 that would lead the skilled person to ensure that the encryption was carried out at a hypothetical external device. The teaching in D1 was based on the fact that the *OTA server* carried out the encryption. Thus, the teaching in D1 was to ensure that encryption is carried out at the OTA server even in the case where this external device is present.

1.1.14 The board is not convinced. Firstly, as to the appellant's allegation that D1 is directed to sending encrypted OTA data from an OTA server and is not related to providing manufacturer or developer control, the board notes that present claim 1 in fact relates to a method of enabling one or more communication services

on a wireless device. Hence, there is no indication of *manufacturer or developer control*. The mobile applications or "applets" of D1 (see p. 7, l. 8-13) are in any case understood to be created by corresponding **developers** before being stored in the database.

Secondly, D1 does disclose **securing** provisioning information through **encryption**, the difference resides only in which entity performs the encryption. For this reason, there is no synergy between the **choice of entity** performing the encryption, which ensures which parties will be privy to the information, and the **use of the time-stamp**, which ensures that the information is current, irrespective of which entity generates it.

Finally, D1 establishes that the mobile applications or "applets" correspond to various types of additional services, for use in the financial, communication, medical, security and broadcasting fields (see e.g. p. 7, l. 8-13). Although D1 does not disclose who the developer of the mobile applications is, in view of the amount and type of fields to be covered, the skilled person would easily consider the use of *external* developers for the creation of applications (e.g. a bank or a medical provider is likely to provide the same service to users of different wireless carriers). It is under this purely administrative scenario where the need to keep certain data secret from the wireless carrier becomes apparent (if not mandatory for regulatory, i.e. non-technical, reasons).

1.2 Hence, the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC) and the main request is not allowable (Article 52(1) EPC).

2. FIRST AUXILIARY REQUEST

2.1 Claim 1 - inventive step (Articles 52(1) and 56 EPC)

2.1.1 D1 further discloses the amended features of claim 1 of the first auxiliary request:

- generating further provisioning information ("first type of encrypted OTA data") by the carrier provisioning system (see p. 9, l. 5-9: " ... a first type of OTA key that is used for terminal information such as an authentication value for the authentication of a mobile terminal, a phone book, and a language for the setting of the mobile terminal, ..."; see see p. 9, l. 16-21: "... if the requested OTA data is a first type of OTA data, the OTA server may create a first type of encrypted OTA data by encrypting the first type of OTA data using a first type of OTA key ...");
- sending the secure provisioning information corresponding to the request ("second type of encrypted OTA data") and the further provisioning information ("first type of encrypted OTA data") from the carrier provisioning system to the wireless device (see p. 9, l. 5-9; see p. 9, l. 16-21).

2.1.2 The subject-matter of claim 1 of the first auxiliary request thus differs from the method known from D1 in the same features as the ones identified above for claim 1 of the main request.

2.1.3 Hence, the subject-matter of claim 1 of the first auxiliary request does not involve an inventive step (Article 56 EPC) for the same reasons stated above for

the main request, and the first auxiliary request is not allowable (Article 52(1) EPC).

3. SECOND AND THIRD AUXILIARY REQUEST

These auxiliary requests were filed *after* the notification of the summons to oral proceedings. Claim 1 of those requests further includes, in essence, the features of encrypting the provisioning information and of generating further provisioning information by the carrier provisioning system (see point V above).

3.1 Admission into the appeal proceedings (Article 13(2) RPBA 2020)

3.1.1 The appellant submitted that the second and third auxiliary requests were filed in response to a clarity objection raised by the board in its communication under Article 15(1) RPBA 2020, that its response was the first opportunity the appellant had had to respond to such an objection, and as such, these requests were a legitimate response to the objections raised in the board's communication.

3.1.2 According to Article 13(2) RPBA 2020, any amendment to a party's appeal case made after notification of a summons to oral proceedings shall, in principle, not be taken into account unless there are exceptional circumstances, which have been justified with cogent reasons by the party concerned.

3.1.3 Although the amendments made to claim 1 of the second and third auxiliary requests constitute an attempt to clarify the claims, the inventive-step objections raised by the board in its communication under Article 15(1) RPBA 2020 already took those features

into account in its interpretation of claim 1 (see also point 1.1.6 above). It is therefore apparent that the amendments made do not add anything of substance to the discussion of inventive step, and therefore, they do not address all the outstanding issues raised by the board.

3.1.4 In view of the board's conclusions on inventive step for the main and first auxiliary request, the board sees no exceptional circumstance that could justify the admission of the second and third auxiliary requests into the appeal proceedings. Hence, the board decides not to take them into account (Article 13(2) RPBA 2020).

4. As there is no allowable claim request, it follows that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

A. Nielsen-Hannerup K. Bengi-Akyürek

Decision electronically authenticated