Internal distribution code:

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

Datasheet for the decision of 6 May 2020

Case Number: T 2024/15 - 3.5.04

Application Number: 10152534.3

Publication Number: 2355502

IPC: H04N7/16, G06F21/00

Language of the proceedings: EN

Title of invention:
Preventing the use of modified receiver firmware in receivers of a conditional access system

Applicant:
Irdeto B.V.

Headword:

Relevant legal provisions:
EPC Art. 56, 111(1)
RPBA 2020 Art. 11

Keyword:
Inventive step - closest prior art
Remittal to the department of first instance

Decisions cited:
G 0010/93, T 3247/19

Catchword:

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 2024/15 - 3.5.04

D E C I S I O N
of Technical Board of Appeal 3.5.04
of 6 May 2020

Appellant: (Applicant)	Irdeto B.V. 105 Taurus Avenue 2132 LS Hoofddorp (NL)
Representative:	Boult Wade Tennant LLP Salisbury Square House 8 Salisbury Square London EC4Y 8AP (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 13 May 2015 refusing European patent application No. 10152534.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	C. Kunzelmann
Members:	B. Willems
	G. Decker

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division dated 13 May 2015 refusing European patent application No. 10 152 534.3, which was published as EP 2 355 502 A1.

II. The documents cited in the decision under appeal included the following:

D1: US 2004/064706 A1.

III. The decision under appeal was based on the ground that the subject-matter of claim 1 of the main request and the first to fifth auxiliary requests then on file lacked inventive step over the disclosure of D1 combined with the common general knowledge of the person skilled in the art (Article 56 EPC).

IV. The applicant (hereinafter "*appellant*") filed notice of appeal. With the statement of grounds of appeal, the appellant filed claims according to a main request and first to fifth auxiliary requests and submitted that these requests were identical to the requests on which the decision under appeal was based. It requested that the decision under appeal be set aside and that a European patent be granted on the basis of the claims according to the main request or one of the first to fifth auxiliary requests filed with the statement of grounds of appeal. Oral proceedings were requested, should the board decide not to allow any part of the appeal for any reason. The appellant indicated a basis for the claims in the application as filed and provided arguments as to why the claims of all requests met the requirements of Article 56 EPC.

V. Claim 1 of the main request and claim 1 of the fourth auxiliary request read as follows (the additional wording of claim 1 of the fourth auxiliary request is in *italics*):

"A receiver of a *digital broadcast television* conditional access system (2a) wherein the receiver is arranged to receive a first encrypted control word ($E_{R'}(CW)$) and a first challenge (C);

wherein the receiver comprises:

a firmware memory (22) storing firmware;

a probe module (21) configured to receive the first challenge (C) which is indicative of one or more locations in the firmware memory (22) and to read data from the one or more locations in the firmware memory (22), the data forming a first response (R') to the first challenge (C);

a decrypter (23) configured to decrypt the first encrypted control word ($E_{R'}(CW)$) using the first response (R') to obtain a first control word (CW); and

a descrambler (24) configured to descramble first scrambled content ($E_{cw}(M)$) using the first control word (CW) to obtain first descrambled content (M)."

VI. Claim 1 of the first auxiliary request reads as follows:

"A receiver of a conditional access system (2a) comprising:

a firmware memory (22) storing firmware; and

a descrambler (24) configured to descramble first scrambled content ($E_{CW}(M)$) using a first control word (CW) to obtain first descrambled content (M);

characterized in that the receiver is arranged to prevent use of modified firmware in the firmware memory by the receiver being arranged to receive a first encrypted control word ($E_{R'}(CW)$) and a first challenge (C), and in that the receiver further comprises:

a probe module (21) configured to receive the first challenge (C) which is indicative of one or more locations in the firmware memory (22) and to read data from the one or more locations in the firmware memory (22), the data forming a first response (R') to the first challenge (C);

a decrypter (23) configured to decrypt the first encrypted control word ($E_{R'}(CW)$) using the first response (R') to obtain the first control word (CW)."

VII. Claim 1 of the second auxiliary request and claim 1 of the third auxiliary request read as follows (the additional wording of claim 1 of the third auxiliary request is in *italics*):

"A receiver of a conditional access system (2a) comprising:

a firmware memory (22) storing firmware *that is executed in the receiver*; and

a descrambler (24) configured to descramble first scrambled content ($E_{CW}(M)$) using a first control word (CW) to obtain first descrambled content (M);

characterized in that the receiver is arranged to prevent use of modified firmware in the firmware memory by the receiver being arranged to receive a first encrypted control word (E_R'(CW)) and a first challenge (C), wherein the first encrypted control word (E_R'(CW)) is the first control word (CW) encrypted using data expected in one or more locations in the firmware memory, the one or more locations indicated by the first challenge (C), and in that the receiver further comprises:

a probe module (21) configured to receive the first challenge (C) which is indicative of the one or more locations in the firmware memory (22) and to read data from the one or more locations in the firmware memory (22), the data forming a first response (R') to the first challenge (C);

a decrypter (23) configured to decrypt the first encrypted control word (E_R'(CW)) using the first response (R') to obtain the first control word (CW)."

VIII. In comparison with claim 1 of the third auxiliary request, claim 1 of the fifth auxiliary request has been amended to specify "A receiver of a *digital broadcast television* conditional access system (2a) comprising" (the additional wording of claim 1 of the fifth auxiliary request is in *italics*).

IX. The examining division's arguments, where relevant to the present decision, may be summarised as follows.

(a) Document D1 disclosed a receiver of a conditional access system (see Figure 2, computer 22 connected to token 32) wherein the receiver was arranged to receive a first encrypted control word E_R' (see

paragraph [0052]: "*key ID*") and a first challenge (see paragraph [0051]: "*puzzle*") (see decision under appeal, page 5, last paragraph).

Authentication and descrambling both served the purpose of denying unauthorised access to data by means of cryptography. Therefore, authentication and descrambling were equivalent (see decision under appeal, page 8, penultimate paragraph).

(b) The receiver known from D1 comprised a firmware memory storing firmware (see paragraphs [0041] to [0045]: memory 38 of token 32) (see decision under appeal, page 5, last paragraph).

Any memory became a "*firmware memory*" by storing firmware. Hence, there was no technical difference between a "*firmware memory*" and a memory (see decision under appeal, page 8, last paragraph).

(c) D1 disclosed a decrypter configured to use the first encrypted control word $E_{R'}(CW)$ and the first response R' to obtain a first control word CW (see paragraph [0053], wherein the "*puzzle key*" corresponded to the "*control word*" generated using the public shared secret and the key determined by using the "*key ID*") and a descrambler configured to descramble first scrambled content $E_{CW}(M)$ using the first control word CW to obtain first descrambled content M (see paragraph [0054], wherein the first scrambled content corresponded to session ID and the descrambled content corresponded to the encrypted response).

D1, paragraphs [0052] and [0053], disclosed that the "*key ID*" identified a key to be used in a

cryptographic operation together with the public shared secret. Decrypting the first encrypted control word $E_{R'}(CW)$ using the first response R' was interpreted as using both the "*key ID*" and the public shared secret in a cryptographic operation (see decision under appeal, page 5, last paragraph).

X. The appellant's arguments, where relevant to the present decision, may be summarised as follows.

(a) The examining division had disregarded the presence in the claim of terms of the art which would be readily understood by the skilled person to have a particular meaning (see statement of grounds of appeal, point 2.6).

A skilled person understood that a "*receiver of a conditional access system*" presented descrambled (i.e. intelligible in terms of being watched/ viewed/listened to) content if a user had the correct permissions. This interpretation was reinforced by the definition of the claimed "*descrambler*" (see statement of grounds of appeal, point 2.7).

D1 did not disclose mechanisms applicable to producing descrambled content in a receiver of a conditional access system. The output of D1 was a "yes/no" authentication value, which was not the same as intelligible descrambled content (see statement of grounds of appeal, points 2.8 and 2.9).

(b) Claim 1 clearly recited that the memory was a "*firmware memory storing firmware*".

D1 did not mention firmware being stored in a memory. The memory disclosed in paragraphs [0042] to [0045] was partitioned into three portions, storing respectively: data values representing symmetric public shared secrets; data values representing data encryption/decryption keys; and data values representing symmetric private shared secrets. D1 did not hint at preventing an attacker from modifying firmware in order to obtain decryption keys and/or control words which could be used to circumvent the conditional access system. D1 did not mention any problems perceived with tampering with memory contents (see statement of grounds of appeal, point 2.10).

(c) The examining division had overlooked the particular data specified in claim 1, i.e. the first encrypted control word had been encrypted using the first response and could be successfully decrypted by using the first response. D1 produced an "*encrypted puzzle key*", which a skilled person would not consider analogous to a control word. The "*encrypted puzzle key*" was used to produce an "*encrypted response*", not to produce descrambled content. The skilled person was familiar with the term "*control word*" as a piece of data which could be directly used to descramble content (see statement of grounds of appeal, points 2.11 and 2.12).

(d) D1 did not disclose reading response data from a memory to produce a control word to descramble received data (see statement of grounds of appeal, point 2.13).

Reasons for the Decision

1. The appeal is admissible.

2. *Interpretation of claim 1 of all requests*

2.1 Claim 1 of each request specifies a "*receiver of a (digital broadcast television) conditional access system (2a)*" and "*a first encrypted control word (E_R'(CW))*".

The board does not share the examining division's view that a receiver of a conditional access system arranged to receive a control word can be equated with a computer connected to a token and authenticating with an access control server (see point IX(a) above).

The board is convinced that the person skilled in the art would understand that the claimed receiver outputs descrambled, intelligible content (see point X(a) above). Contrary to the examining division's statement, descrambling and authentication are not equivalent (see point IX(a) above).

The board's interpretation is confirmed by the following references in the description of the application in this case to "*pay-tv applications*" and "*a broadcast stream containing scrambled content*":

Page 1, lines 9 to 12: "*Broadcast networks for pay-tv applications deliver encrypted content to receivers and keys (also known as control words or CWs) associated to the encrypted content to secure devices*";

Page 8, lines 5 to 9: "*A tuner/demodulator module 25 of the receiver 2b receives a broadcast stream containing*

scrambled content $E_{cw}(M)$, entitlement control messages (ECMs) and entitlement management messages (EMMs) in a manner known per se".

2.2 The examining division's argument that a "*firmware memory (22) storing firmware*" differs from a memory on account of the stored firmware is inconsistent with its conclusion that there is no technical difference between the claimed "*firmware memory (22) storing firmware*" and a memory (see point IX(b) above). The board agrees with the appellant that claim 1 clearly specifies a firmware memory storing firmware (see point X(b) above), which is not to be interpreted merely as a memory suitable for storing firmware. Moreover, the board is not convinced that any memory storing firmware is a "*firmware memory*". Firmware is normally stored in a non-volatile memory. The board doubts whether a cache memory temporarily storing a firmware update can be referred to as a firmware memory.

2.3 D1, paragraphs [0053] to [0056], discloses that a public shared secret is read from the token memory by using the challenge puzzle. This secret is subjected to a first round of encryption to generate an encrypted puzzle key and a second round of encryption to generate a response which is sent to an access control server. This server similarly generates a response which it compares with the received response to grant or deny access.

In the context of the application in this case, the person skilled in the art would not consider the claimed control word analogous to the encrypted puzzle key (see point IX(c) above). Although the control word and the encrypted puzzle key are both generated by

reading out the shared secret, they serve completely different purposes. The board shares the appellant's view that the person skilled in the art interprets the term "*control word*" as a piece of data used to descramble content (see point X(c) above).

2.4 Summarising, the examining division based its inventive-step objection on an interpretation of claim 1 which conformed neither to the normal meaning of the terms used nor to the description of the present application. The board agrees with the appellant that the examining division "*disregarded the presence in the claim of terms of the art which would be readily understood by the skilled person to have a particular meaning and implications*" (see statement of grounds of appeal, point 2.6).

3. *All requests - inventive step (Article 56 EPC)*

3.1 D1 discloses a token which can be coupled to a computer data port (see paragraph [0040]). The token comprises a non-volatile memory partitioned into two or more portions. A first portion functions as an identification (ID) pad in which different data values may be stored in predetermined address locations during manufacture of the token. These data values represent symmetric public shared secrets and may remain unchanged during the life of the token (see paragraphs [0042] and [0043]). The token transmits a request to access a network server to a network access control server. The latter generates a challenge including a challenge puzzle and a key ID and transmits the challenge to the token (see paragraphs [0048] and [0049]). The token's processor decomposes the challenge to recover the challenge puzzle and the key ID. The challenge puzzle is mapped to the ID pad

portion of the token's memory and the key ID is sent to the key storage portion of the memory (see paragraph [0050]). The challenge puzzle functions as a set of instructions for accessing selected data address locations in the ID pad storing values representing a symmetric public shared secret (see paragraph [0051]). The encryption key identified by the key ID is retrieved from the token's memory and used to encrypt the public shared secret to generate an encrypted puzzle key (see paragraphs [0052] and [0053]).

3.2 The board agrees with the appellant that D1 neither discloses nor suggests that the shared secret may be used to decrypt the encrypted puzzle key to generate a control word to descramble received data (see point X(d) above). Therefore, D1 is not an appropriate starting point for the assessment of inventive step (Article 56 EPC) of claim 1 of the main request.

3.3 The examining division reasoned that the additional feature of claim 1 of the first auxiliary request did not limit the subject-matter as compared with that of claim 1 of the main request (see decision under appeal, page 7, first paragraph) and that the additional features of claim 1 of the second auxiliary request were a mere re-formulation of the other features defined in the claim (see decision under appeal, page 7, section 3). Thus, the objections of lack of inventive step (Article 56 EPC) raised against claim 1 of the first and second auxiliary requests were based on the same reasons as the objections raised against claim 1 of the main request.

For the reasons set out in point 3.2 above, D1 is not an appropriate starting point for the assessment of

inventive step (Article 56 EPC) of claim 1 of the first and second auxiliary requests.

3.4 With respect to the third auxiliary request, the examining division reasoned that the additional feature that the "*firmware was executed in the receiver*" merely defined firmware and addressed a partial problem. However, the examining division did not identify the partial problem. Instead it stated that the definition of firmware was common general knowledge (see decision under appeal, page 7, section 4). This reasoning corresponds to the interpretation given to firmware in the assessment of inventive step for the main request. Thus, the objection of lack of inventive step (Article 56 EPC) raised against claim 1 of the third auxiliary request was based on the same reasons as the objections raised against claim 1 of the main request. For the reasons set out in point 3.2 above, D1 is not an appropriate starting point for the assessment of inventive step (Article 56 EPC) of claim 1 of the third auxiliary request.

3.5 Claim 1 of the fourth and fifth auxiliary requests differs from claim 1 of the main request in that it specifies a receiver of a digital broadcast television conditional access system. D1 discloses a general-purpose computer (see decision under appeal, pages 7 and 8, section 5). Thus, *a fortiori*, D1 is not an appropriate starting point for the assessment of inventive step (Article 56 EPC) of claim 1 of the fourth and fifth auxiliary requests.

3.6 Claims 3 and 4 of each of the requests specify a smart card. D1 does not disclose a smart card. Therefore, D1 is not an appropriate starting point for the assessment of inventive step (Article 56 EPC) of claims 3 and 4.

4. *Further prosecution*

4.1 According to Article 111(1) EPC, the board, in deciding upon the appeal, may exercise any power within the competence of the department which was responsible for the decision appealed or remit the case to that department for further prosecution.

4.2 The examining division based its inventive-step objection on an interpretation of claim 1 which conformed neither to the normal meaning of the terms used nor to the description of the application in this case (see section 2 above).

Thus, if the board decided not to remit the case to the department of first instance, it would have to carry out a full examination of the application as to the patentability requirements on the basis of the correct interpretation of the claims. This is the task of the examining division (see decision G 10/93 of the Enlarged Board of Appeal, OJ EPO 1995, 172, point 4 of the Reasons). In particular, to assess inventive step, the board would have to elaborate on whether, upon proper interpretation of the terms "*receiver of a conditional access system*" and "*control word*", the subject-matter of claim 1 of any of the requests met the requirements of Article 56 EPC. Since none of the documents cited in the first-instance proceedings disclosed fundamental concepts on which the claimed invention was based, such as a secure memory storing a key for decrypting a received encrypted code word (see, for instance, WO 00/59222 A1), the board would even have to determine whether an additional search was necessary. Hence, the board comes to the conclusion that the issues relevant to patentability in this case

could not be decided upon without undue burden (see T 3247/19, Reasons 11).

4.3 Under these circumstances, which are considered to be "*special reasons*" within the meaning of Article 11 RPBA 2020, and in spite of the long duration of the proceedings thus far, the board exercises its discretion under Article 111(1) EPC and remits the case to the department of first instance for further prosecution.

4.4 The appellant requested oral proceedings only if the board decided "*not* [to] *allow any part of the appeal for any reason*". For the reasons set out in points 4.2 and 4.3 above, the decision under appeal is to be set aside. Thus, the board partly allows the appeal, which is why oral proceedings were not deemed necessary.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division for further prosecution.

The Registrar: The Chairman:

K. Boelicke C. Kunzelmann

Decision electronically authenticated