Internal distribution code:

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

Datasheet for the decision of 18 May 2017

Case Number: T 0903/13 - 3.5.05

Application Number: 04717990.8

Publication Number: 1618666

IPC: H04L9/00

Language of the proceedings: EN

Title of invention:
METHOD AND APPARATUS FOR PROTECTING THE TRANSFER OF DATA

Applicant:
SONY ELECTRONICS, INC.

Headword:
Conditional access to encrypted content data/SONY

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - after amendment

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 0903/13 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 18 May 2017

Appellant: (Applicant)	SONY ELECTRONICS, INC. One Sony Drive Park Ridge, New Jersey 07656 (US)
Representative:	D Young & Co LLP 120 Holborn London EC1N 2DY (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 11 December 2012 refusing European patent application No. 04717990.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	F. Blumer

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, dispatched on 11 December 2012, refusing European patent application No. 04 717 990.8 on the ground of lack of inventive step (Article 56 EPC) with respect to a main request and a first auxiliary request, having regard to the disclosure of

D1: US 6 157 719

and common general knowledge.

The examining division also raised a clarity objection (Article 84 EPC) against the first auxiliary request.

II. Notice of appeal was received on 14 January 2013. The appeal fee was paid on 25 January 2013. A statement setting out the grounds of appeal was received on 5 April 2013. The appellant (applicant) requested that the decision of the examining division be set aside and that a patent be granted on the basis of the claims of the main request. In addition, oral proceedings were requested as an auxiliary measure.

III. A summons to oral proceedings was issued on 7 March 2017. In a communication pursuant to Article 15(1) RPBA dated 16 March 2017 the board gave its preliminary opinion that the claims did not meet the requirements of Article 56 EPC, having regard to the disclosure of D1 and common general knowledge.

IV. With a letter of reply dated 18 April 2017, the appellant provided further arguments in respect of inventive step.

V. Oral proceedings were held on 18 May 2015, during which the appellant submitted amended claims as a main request. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the following documents:
- claims 1 to 21, filed as main request during oral proceedings before the board,
- description pages:
  - 1 to 4 and 6 to 42 as published,
  - 5 and 5a as filed on 1 October 2012,
- drawing sheets 1/21 to 21/21 as published.

At the end of the oral proceedings, the decision of the board was announced.

VI. Claim 1 of the main request reads as follows:

"A secure content delivery system (1100), comprising:
a set-top box (1140) to initiate a request (1111) for program data, the request including a unique identifier of the set-top box, the set-top box having a memory storing a unique key of the set-top box; and
a conditional access (CA) control system (1120) in communication with the set-top box and a mating key server (1130), the CA control system configured:
to transmit information including the unique identifier and a mating key generator (1121) to the mating key server,
to receive from the mating key server a mating key (1122) being based on the transmitted unique identifier and the mating key generator, the mating key being used to encrypt a control word used for scrambling the program data prior to transmission to the set-top box
the mating key obtained by the mating key server accessing a copy of the unique key stored in the mating

key server, and encrypting the mating key generator using the copy of the unique key, and
to transmit the mating key generator and the encrypted control word to the set-top box;
the set-top box configured to encrypt the received mating key generator using the unique key to obtain a key identical to the mating key, to use the obtained mating key to decrypt the encrypted control word, and to use the decrypted control word to descramble scrambled program data".

The request comprises further independent claims directed to a corresponding method (claim 13) and a related mating key gateway (claim 19).

Reasons for the Decision

1. The appeal is admissible.

2. Article 123(2) EPC

The board is satisfied that the amendments to independent claims 1, 13 and 19 made during the oral proceedings are based on the description as originally filed, in particular the passages on page 33, lines 15 to 19 and from page 34, line 25 to page 35, line 1, and thus meet the requirements of Article 123(2) EPC.

3. Inventive step - Article 56 EPC

It was common ground during the oral proceedings that D1 represented the closest prior art and that the differences between the subject-matter of claim 1 and the disclosure of D1 were that:

- the CA control system transmits the unique identifier of the set-top box and a mating key generator to the mating key server,
- the mating key server generates a mating key based on the unique identifier and the mating key generator and transmits it to the CA control system,
- the mating key is obtained by the mating key server accessing a copy of the unique key stored in the mating key server,
- both the mating key server and the set-top box encrypt the mating key generator using the unique key of the set-top box to obtain the mating key.

These distinguishing features define firstly that the mating key which is used for encrypting the control word in the CA control system is generated inside the mating key server and the set-top box by encrypting a mating key generator using the unique key of the set-top box. In D1, the equivalent of the mating key, namely the multi-session key MSK, is issued by a transaction encryption device (see Figure 6, 603) and sent to the CA control system ("Control suite" 607 in Figure 6). Thus, in contrast to claim 1, the mating key in D1 is not generated from a unique key of the set top-box.

Secondly, these distinguishing features define that the CA control system sends the mating key generator to the set-top box to enable regeneration of the mating key inside the set-top box, whereas in D1 the mating key is sent encrypted to the set-top box, using public key encryption.

The appellant first argued that the system of

claim 1 enhanced security because the unique key was stored safely in two remote locations, namely the set-top box and the mating key server, and was never transmitted to the CA control system. It was therefore safe from interception by hackers, which led to enhanced protection of the mating key encrypting the control word. In the board's view, the use in D1 of an asymmetric encryption scheme for transmitting the mating key between the CA control system and the set-top box also leads to protection of the mating key on the transmission path. A comparison of the level of security of the two different schemes used in claim 1 and in D1 for making the mating key available at the set-top box would however be based on a considerable number of parameters, for instance the algorithm used in D1 and the protection of the transmission link between mating key server and CA control system in claim 1, which are specified neither in the application nor in document D1. The board therefore considers that an alleged technical effect related to security enhancement alone cannot be used to support inventive step.

Further, the appellant stated that the distinguishing features of claim 1 resulted in a simpler way of protecting data content communicated between a CA control system and a set-top box, independently of the set-top box manufacturer. In particular, the appellant plausibly argued that the unique identifier used to retrieve the unique key could have any format, such as a serial number given by any manufacturer, which allowed the set-top boxes of any manufacturer to be used with a single CA control system. In contrast the system of D1 needed the set-top box and the CA control system to be registered with a certification authority in order for the CA control system to get the certified

public key of the set-top box. Thus, the board acknowledges that the features of claim 1 enable a simpler and more straightforward implementation of conditional access to content data, without having to rely on a Public-Key-Infrastructure.

Based on this achieved technical effect, the objective technical problem can thus be formulated as how to achieve a simpler conditional access system while maintaining a high level of security.

The skilled person starting from D1 would have to perform several steps to arrive at the subject-matter of D1. He would first have to move from an asymmetric encryption scheme to transfer the mating key from the CA control system to the set-top box to a symmetric encryption scheme in which the mating key is kept secret in both parts. Then, the skilled person would have to share the mating key in the specific way taught in claim 1 by generating it in the mating key server and the set-top box using a mating key generator and the unique key of the set-top box. Although the encryption schemes used by the system of claim 1 are known per se and the skilled person is aware that a symmetric encryption scheme would be simpler to implement, the above-mentioned steps involve more than the mere replacement of a public key encryption scheme by a symmetric encryption scheme and also more than the mere use of a key derivation scheme for symmetric key generation. The board therefore acknowledges that the skilled person would not arrive at the subject-matter of claim 1 without the use of inventive skills.

For these reasons, the board judges that claim 1 meets the requirements of Article 56 EPC, having regard to the prior art on file. Independent claim 13 comprises

the same features as claim 1 but expressed in terms of a method claim. Independent claim 19 relates to a mating key gateway co-operating with a mating key server, a plurality of subscriber management systems and a set-top box for substantially performing the method of claim 13. Therefore, claims 13 and 19 also meet the requirements of Article 56 EPC.

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 with the order to grant a patent on the basis of the following documents:
   - Claims 1 to 21, filed as main request during oral proceedings before the board
   - Description pages
     - 1-4, 6-42 as published
     - 5, 5a as filed on 1 October 2012
   - Drawing sheets 1/21 to 21/21 as published.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated