

Internal distribution code:

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

**Datasheet for the decision
of 16 April 2013**

Case Number: T 0513/12 - 3.5.03

Application Number: 95933027.5

Publication Number: 780039

IPC: H04K 1/00, G06F 1/00

Language of the proceedings: EN

Title of invention:
Roving software license for a hardware agent

Applicant:
Intel Corporation

Headword:
Roving software license/INTEL

Relevant legal provisions:
EPC Art. 56, 84, 123(2)

Relevant legal provisions (EPC 1973):
-

Keyword:
"Inventive step - main request and first to third and fifth
auxiliary requests (no)"
"Added subject-matter - fourth auxiliary request (yes)"
"Clarity - fourth auxiliary request (no)"

Decisions cited:
-

Catchword:
-



Case Number: T 0513/12 - 3.5.03

D E C I S I O N
of the Technical Board of Appeal 3.5.03
of 16 April 2013

Appellant: Intel Corporation
(applicant) 2200 Mission College Boulevard
P.O. Box 58119
Santa Clara
CA 95052-8119 (US)

Representative: Walker, Ross Thomson
Forresters
Skygarden
Erika-Mann-Str. 11
80636 München (DE)

Decision under appeal: Decision of the examining division of the
European Patent Office posted 9 August 2011
refusing European patent application
No. 95933027.5 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: M.-B. Tardo-Dino
Members: F. van der Voort
T. Snell

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 95933027.5 which was published as international application PCT/US95/11136 with publication number WO 96/08092 A.

II. The reasons given for the refusal were that the subject-matter of claims 1 of a main request and an auxiliary request did not involve an inventive step (Articles 52(1) and 56 EPC) having regard to the disclosure of:

D3: CA 1 310 425

and taking into account the teaching of:

D4: "Applied cryptography: protocols, algorithms, and source code in C", B. Schneier, first edition, 1993, John Wiley & Sons, Inc., pages 180 and 181.

The following document was also referred to in the examination procedure:

D2: "Applied cryptography: protocols, algorithms, and source code in C", B. Schneier, second edition, 1996, John Wiley & Sons, Inc., pages 31 to 34, 52 to 54, and 185 to 187.

III. With the statement of grounds of appeal the appellant filed new sets of claims and submitted arguments in support. The board understood the appellant to be requesting that the decision under appeal be set aside

and a patent be granted on the basis of claims of a main request or, failing that, on the basis of one of first to fifth auxiliary requests, all requests as filed with the statement of grounds. Oral proceedings were conditionally requested.

- IV. In a communication annexed to a summons to oral proceedings the board raised, without prejudice to its final decision, objections under Article 52(1) EPC in combination with Article 56 EPC (lack of inventive step) against claims 1 of the main request and first to third and fifth auxiliary requests and objections under Articles 84 and 123(2) EPC against claim 1 of the fourth auxiliary request.
- V. In response to the summons the appellant requested that the date for the oral proceedings be changed, for which reasons were given. No substantive submissions in response to the objections raised in the communication were filed.
- VI. The board subsequently cancelled the scheduled oral proceedings and fixed a new date for the oral proceedings. With a second communication the appellant was informed accordingly.
- VII. In response to the second communication the appellant informed the board that it would not attend the oral proceedings. No substantive submissions were filed.
- VIII. Oral proceedings were held on 16 April 2013 in the absence of the appellant.

In accordance with the written submissions the appellant had requested that the decision under appeal be set aside and a patent be granted on the basis of claims of a main request or, failing that, on the basis of one of first to fifth auxiliary requests, all requests as filed with the statement of grounds.

At the end of the oral proceedings, after deliberation, the board's decision was announced.

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

"A first integrated circuit component adapted for exchanging a license token, necessary for executing a licensed software program, with a second integrated circuit component, the first integrated circuit component comprising:

processing means (123) adapted to process information completely within the first integrated circuit component;

first storage means (127) adapted to store a unique key pair (127a), an authentication digital certificate (127b), a public key (127c) of a manufacturer of the first integrated circuit component, and said license token within the first integrated circuit component, said first storage means (127) being coupled to said processing means (123);

second storage means (128) adapted to store said information processed by said processing means (123), said second storage means (128) being coupled to said processing means (123);

means (126) adapted to generate said unique key pair (127a) to reside within the first integrated

circuit component, said generating means (126) being coupled to said processing means (123); and

interface means (125) adapted to provide a direct communication link between a system employing the first integrated circuit component and a remote system employing the second integrated circuit component to exchange said license token, said interface means (125) being coupled to said processing means (123).".

Claim 1 of the **first auxiliary request** reads as follows:

"A first integrated circuit component adapted for exchanging a license token, necessary for executing a licensed software program, with a second integrated circuit component, the first integrated circuit component comprising:

processing means (123) adapted to process information completely within the first integrated circuit component;

first storage means (127) adapted to store a unique key pair (127a) including a private key, an authentication digital certificate (127b) for verifying the authenticity of the key pair, a public key (127c) of a manufacturer of the first integrated circuit component, and a license token, said first storage means (127) being coupled to said processing means (123);

second storage means (128) adapted to store said information processed by said processing means (123), said second storage means (128) being coupled to said processing means (123);

generating means (126) adapted to generate said unique key pair (127a), said generating means (126) being coupled to said processing means (123); and interface means (125) adapted to enable communication between the first integrated circuit component and the second integrated circuit component to exchange a license token encrypted using said public key (127c), said interface means (125) being coupled to said processing means (123), characterised in that:

the processing means (123), the generating means (126) and the first storage means (127) all reside within the first integrated circuit component, the processing means (123) being adapted to decrypt an encrypted token received from said second integrated circuit component using said private key without the private key being communicated outside of the first integrated circuit component."

Claim 1 of the **second auxiliary request** differs from claim 1 of the first auxiliary request in that the fifth and sixth paragraphs are amended to read as follows:

"generating means (126) adapted to generate said unique key pair (127a), said generating means (126) being coupled to said processing means (123), characterised in that the first integrated circuit component further comprises:

interface means (125) adapted to enable communication between the first integrated circuit component and the second integrated circuit component to exchange a license token encrypted using said public key (127c), wherein said interface means (125) includes

a bus interface which allows the first integrated circuit component to internally decrypt and store said license token received from the second integrated circuit component and to internally encrypt and transmit said license token to the second integrated circuit component;".

Claim 1 of the **third auxiliary request** differs from claim 1 of the first auxiliary request in that the following paragraphs are inserted between the first and second paragraphs:

"an integrated circuit component package (122); characterised in that:

a single die (121) is encapsulated within the integrated circuit component package, the die comprising:"

and in that in the last two paragraphs the following wording is deleted:

"characterised in that:

the processing means (123), the generating means (126) and the first storage means (127) all reside within the first integrated circuit component,".

Claim 1 of the **fourth auxiliary request** reads as follows:

"A multi-chip module within a first node that is adapted for exchanging a license token, necessary for executing a licensed software program, with a second node, the multi-chip module comprising:

a processor, and

a hardware agent means (120) coupled to the processor, the hardware agent means comprising:

an integrated circuit component package (122), and at least one die (121) encapsulated within the integrated circuit component package, wherein the at least one die comprises:

processing means (123) adapted to process information completely within the first integrated circuit component,

first storage means (127) adapted to store a unique key pair (127a) including a private key, an authentication digital certificate (127b) for verifying the authenticity of the key pair, a public key (127c) of a manufacturer of the first integrated circuit component, and a license token, said first storage means (127) being coupled to said processing means (123),

second storage means (128) adapted to store said information processed by said processing means (123), said second storage means (128) being coupled to said processing means (123),

generating means (126) adapted to generate said unique key pair (127a), said generating means (126) being coupled to said processing means (123), and

interface means (125) adapted to enable communication between the first integrated circuit component and the second integrated circuit component to exchange a license token encrypted using said public key (127c), said interface means (125) being coupled to said processing means (123),

the processing means (123) being adapted to decrypt an encrypted token received from a second integrated circuit component of the second node using said private key without the private key being

communicated outside of the hardware agent means (120)."

Claim 1 of the **fifth auxiliary request** differs from claim 1 of the third auxiliary request in that in the third paragraph the term "single die" is replaced by "die" and in that in the last paragraph the following wording is added after "the first integrated circuit component":

", to store said license token that is needed to operate a licensed software application".

Reasons for the Decision

1. *Procedural matters*

- 1.1 The present decision is based on objections under Article 52(1) EPC in combination with Article 56 EPC as well objections based on Articles 84 and 123(2) EPC. These objections had already been raised in the board's first communication. The appellant had the opportunity to present its comments on these objections. However, no substantive submissions in response to the objections raised were filed. Further, in deciding not to attend the oral proceedings, the appellant chose not to make use of the opportunity to comment at the oral proceedings on any of the objections but, instead, chose to rely on arguments as set out in the statement of grounds, which the board duly considered. Under these circumstances, the board was in a position to give a decision in accordance with Article 113(1) EPC.

1.2 Although the appellant withdrew the request for oral proceedings, the board considered it to be expedient to hold oral proceedings for reasons of procedural economy (Article 116(1) EPC). The appellant had informed the board that it would not attend the oral proceedings and, indeed, was absent. The oral proceedings were therefore held in the absence of the appellant (Rule 115(2) EPC, Article 15(3) RPBA).

2. *Main request - claim 1*

2.1 D3 discloses (see, in particular, Fig. 1) a first component 14 ("local node") adapted for exchanging a license token 27 (Fig. 2B), necessary for executing a licensed software program 24A (Fig. 2C), with a second component 20 ("remote node", page 7, line 22, to page 8, line 2, and page 15, lines 9 to 13), in which the first component 14 includes:

- processing means ("CPU 18", page 16, lines 8 to 10) adapted to process information completely within the first component 14;
- first storage means (i.e. a first part of "system memory 16", page 10, lines 9 to 11) adapted to store the license token 27 within the first component 14 (page 22, lines 11 to 13), the first storage means being coupled to the processing means 18;
- second storage means (i.e. a second part of "system memory 16") adapted to store the information processed by the processing means 18 (page 15, lines 13 to 15, and page 22, lines 17 to 19), the second storage means being coupled to the processing means 18;
- generating means ("operating system 15", page 15, lines 13 to 15) adapted to generate a unique identification ("UID") to reside within the first

component 14, i.e. stored in encrypted form in the system memory 16 (page 15, lines 22 to 24), the generating means 15 being coupled to the processing means 18; and

- interface means ("network 11" and "network link 13") adapted to provide a direct communication link between a system employing the first component 14 and a remote system employing the second component 20 to exchange the license token 27, the interface means 11, 13 being coupled to the processing means 18.

Since it is implicit that the system memory 16 is adapted to store any kind of digital information, the system memory 16 is equally adapted to store, for example, a unique key pair, an authentication digital certificate, and a public key of a manufacturer of the first component.

2.2 The subject-matter of claim 1 of the main request thus differs from the first component, i.e. node 14, disclosed in D3 in that according to claim 1:

- i) the first component is an integrated circuit component; and
- ii) the generating means is adapted to generate a unique key pair to reside within the first integrated circuit component.

2.3 At the priority date it was well-known to implement CPUs and system memories as integrated circuits. Hence, it would have been obvious to a person skilled in the art to implement the CPU 18 and the system memory 16 of the node 14 as an integrated circuit. In the absence in

the claim of any further details of the integrated circuit, using the language of the claim, a node including the integrated circuit may be referred to as an integrated circuit component. Hence, feature i) does not contribute to an inventive step.

Further, as acknowledged in the application in suit, public key cryptography was a conventional technique for securely transferring digital information from a first node to a second node (application in suit, page 9, lines 2 to 10, and document D2, section 2.5). Hence, at the priority date it would have been obvious to the skilled person, when faced with the problem of implementing under secure communications the licence transfer embodiment disclosed in D3, which involves the loading and transfer of a licence token 27 and the sending of encrypted authorisation codes C1 and C2 (page 17, line 24, to page 18, line 12, and page 22, lines 6 to 13), to apply public key cryptography for the same purpose. Public key cryptography includes the generation of a unique key pair and may include a digital certification process using an authentication digital certificate and a public key of a manufacturer (application in suit, page 9, penultimate line, to page 12, line 11, and Figs 2 and 3, and D2, section 8.12). Hence, adapting the generating means 15 to generate a unique key pair to reside within the first component (feature ii)) does not contribute to an inventive step either. The skilled person would therefore, without the exercise of inventive skill, have arrived at a first integrated circuit component which includes all the features of claim 1 of the main request.

2.4 The appellant argued that the technical effect of the difference between D3 and the invention was "to improve security by preventing the private key from being communicated outside of the integrated circuit component". This would "minimise access to the private key through virus attack", which was "a common method of disrupting a computer system to obtain its private key".

The board does not find this argument convincing, since the claim does not refer to a "private key" and does not include features by means of which a communication of a private key outside of the integrated circuit component is prevented and/or features by means of which access to a private key through a virus attack is minimised, it being noted that even an integrated circuit component which is capable of generating and storing a private key would not necessarily preclude access to the private key from outside the integrated circuit component, e.g. by a virus attack. The board further notes that, in any case, as pointed out in the application in suit (page 9, penultimate line, to page 10, line 14, and Fig. 2), it was well-known that in public key cryptography, i.e. asymmetric key cryptography, the private key is exclusively known and used by one of the nodes and, hence, is not to be communicated to, e.g., the other node which sends or receives the encrypted message.

In the board's view, feature ii) (see point 2.2 above) together with a storage of the unique key pair, the authentication digital certificate, the public key of a manufacture and the licence token would arguably contribute to improving the security of the arrangement

for exchanging the licence token between the first and second integrated circuit components in that public key cryptography for exchanging the licence token might be used. However, as noted above (cf. point 2.3 above), using this technique was well-known at the priority date.

2.5 For the above reasons, the subject-matter of claim 1 of the main request does not involve an inventive step (Articles 52(1) and 56 EPC).

3. *Auxiliary requests - claims 1*

3.1 Re. claim 1 of the first auxiliary request:

In the absence of any constructional details of the integrated circuit, the additional feature according to which the processing means, the generating means and the first storage means all reside within the first integrated circuit component is considered as being redundant, since these means are already defined as being part of the first integrated circuit component. Further, the additional feature according to which the processing means is adapted to decrypt an encrypted token received from the second integrated circuit component using the private key merely relates to the above-mentioned conventional public key cryptography and, hence, does not contribute to an inventive step either.

3.2 Re. claim 1 of the second auxiliary request:

Providing a bus interface for interconnecting the CPU and system memory and for providing I/O functions was a

common feature in traditional computer architecture at the priority date. Hence, implementing the interface means of D3 by including a bus interface does not contribute to an inventive step. In the first integrated circuit component referred to at point 2.3 above, the bus interface would allow the first integrated circuit component to internally decrypt and store the licence token received from the second integrated circuit component and to internally encrypt and transmit the license token to the second integrated circuit component.

3.3 Re. claim 1 of the third auxiliary request:

As noted above, at the priority date it was well-known to implement CPUs and system memories as integrated circuits. The same applies to internal bus interfaces for interconnecting the CPU and the system memory and for providing I/O-functions.

The board further notes that D3 mentions the Apollo DN3000 as an example of a stand-alone computer (page 16, lines 6 to 10). This computer was based, and this was not contested by the appellant, on a Motorola 68000 processor, in which the CPU, the system cache memory and the bus interface were on a single die. Hence, implementing the first integrated circuit node 14 accordingly does not contribute to an inventive step.

3.4 Re. claim 1 of the fourth auxiliary request:

The appellant argued in writing that a basis for the amendments in claim 1 of the fourth auxiliary request

could be found in the application as filed at page 13, lines 21 to 27, and page 15, lines 6 to 11. The board notes however that at page 13 reference is only made to a "single integrated circuit in the form of a die", which does not provide a basis for "at least one" die. Further, the cited passage at page 15 relates to another alternative implementation, in which the hardware agent is one component of a multi-chip module which includes a host processor. Claim 1 does not however refer to a host processor and uses the term "hardware agent means" instead of "hardware agent". Further, the passage at page 15 does not directly and unambiguously disclose that the hardware agent in question includes all of the features of the embodiment shown in Fig. 5. Claim 1 is therefore directed to a combination of different embodiments, without the application as filed providing a basis for the combination. Hence, claim 1 does not comply with the requirement of Article 123(2) EPC.

Further, claim 1 is not clear (Article 84 EPC) in that there are no antecedents for "the first integrated circuit component" and "the second integrated circuit component" (see point IX above, claim 1, seventh and tenth paragraphs).

3.5 Re. claim 1 of the fifth auxiliary request:

The considerations set out above in respect of claim 1 of the third auxiliary request equally apply to claim 1 of the fifth auxiliary request.

4. The objections set out above were already raised in the board's communication as annexed to the summons to oral

proceedings. The appellant did not however file any substantive submissions in response and, further, chose not to attend the oral proceedings (see points IV to VII above).

5. In view of the above, the board concludes that the subject-matter of claims 1 of the main request and first to third and fifth auxiliary requests does not involve an inventive step (Articles 52(1) and 56 EPC), whilst claim 1 of the fourth auxiliary request does not comply with the requirements of Article 84 EPC (clarity) and Article 123(2) EPC.
6. As claim 1 of each request is not allowable, each of the requests as a whole is not allowable.
7. There being no allowable request, it follows that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairwoman:

G. Rauh

M.-B. Tardo-Dino