Internal distribution code:

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

Datasheet for the decision of 9 May 2016

Case Number: T 1953/13 - 3.5.06

Application Number: 09717157.3

Publication Number: 2250602

IPC: G06F21/00, H04L9/06, G06F3/12, G06F9/00

Language of the proceedings: EN

Title of invention:
UNIT USING OS AND IMAGE FORMING APPARATUS USING THE SAME

Applicant:
Samsung Electronics Co., Ltd.

Headword:
CRUM chip/Samsung

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step (no)

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 1953/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 May 2016

Appellant: (Applicant)	Samsung Electronics Co., Ltd. 129, Samsung-ro Yeongtong-gu Suwon-si, Gyeonggi-do, 443-742 (KR)
Representative:	Appleyard Lees IP LLP 15 Clare Road Halifax HX1 2HY (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 17 April 2013 refusing European patent application No. 09717157.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	A. Teale

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 17 April 2013, to refuse European patent application No. 09 717 157.3. In the decision reference was made to the document

D1: US 7 246 098 B1,

and claim 1 of the then main and auxiliary requests was found to lack inventive step over D1.

II. A notice of appeal was filed on 14 June 2013, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 27 August 2013. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1-10 according to a main or an auxiliary request filed with the grounds of appeal and the description on file. The board understands the appellant to be requesting grant on the basis of the description and drawings as published.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the invention according to both requests lacked inventive step over D1.

IV. In response to the summons, the appellant filed with a letter dated 5 April 2016 amended claims 1-10 according to a main and a first auxiliary request, and further amended claims 1-4 according to a new second auxiliary request.

V. Claim 1 according to the main request reads as follows:

"A method for performing cryptographic data communication in an apparatus which performs the cryptographic data communication with a customer replaceable unit monitoring, CRUM, unit mounted in a replaceable unit of an image forming apparatus, the method comprising:

encrypting data to update information stored in the CRUM unit using data;

generating a communication message by combining a message authentication code, MAC, and the encrypted data; and

transmitting the communication message to the CRUM unit through a serial interface to update the information stored in the CRUM unit,

wherein the CRUM unit comprises a central processing unit, CPU, and a memory unit to store an operating system, OS, of the CPU, and the CPU is coupled to the memory unit,

and the OS of the CPU executes an initialization operation to independently initialize the state of the CRUM unit."

Claim 1 according to the first auxiliary request is identical to claim 1 of the main request with the following phrase added at the end.

"... the initialization including initial driving of application programs used in the CRUM unit, secret calculation information, needed for data communications with the image forming apparatus after initialization, setup of a communication channel, initialization of a memory value, confirmation of a replacement time, setting of register values in the CRUM unit, and setting of internal and external clock signals."

Claim 1 according to the second auxiliary request is identical to claim 1 of the first auxiliary request with the following further phrase added at the end.

"... wherein the data includes information regarding consumables used in the image forming apparatus,
and the communication message includes a command to update status information on use of the consumables stored in the CRUM unit based on the information regarding the consumables,
wherein the communication message is encrypted using the encryption algorithm stored in the apparatus,
wherein the apparatus stores a plurality of encryption algorithms and uses an encryption algorithm corresponding to an encryption algorithm used in the CRUM unit from among the plurality of encryption algorithms."

VI. Oral proceedings were held as scheduled on 9 May 2016. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application relates to an "image-forming apparatus" (for instance, a printer) equipped with a replaceable unit (such as an ink cartridge) comprising a so-called "CRUM" ("Customer Replaceable Unit Monitoring") unit. The CRUM unit is equipped with a chip which enables the host device to retain some form of control over the replaceable unit. It may, for instance, count the number of pieces of paper printed so as to determine the time until the cartridge must be

replaced (see page 1, paragraphs [4] and [6] of the application as originally filed), or it may authenticate the replaceable unit vis-à-vis the apparatus.

1.1 The invention proposes to improve existing CRUM units by providing a "built-in CPU with an operating system" (paragraph [9]). This is said to make the CRUM unit "more secure" (*loc. cit.*). The operating system itself is only characterised by some of the functions it is to carry out. No specific example of an operating system is disclosed. It is also disclosed that "[t]he CPU [of the CRUM chip] may perform initialization using the OS of the CPU, separately from the main body of the image forming apparatus" (paragraphs [12] and [74]). The application also discloses a number of tasks to be performed by the CRUM unit during initialization (see in particular paragraphs [75] to [77]).

1.2 It is further disclosed that the CRUM unit may support several cryptographic algorithms, and that one of them may be selected "when a key write system in a key management system (KMS) [...] generates key generating data" (see paragraph [132]). This is said to make it possible to change the cryptographic algorithm if it has been cracked. The apparatus may also support several cryptographic algorithms so that it can change the cryptographic algorithm in response to a corresponding change in the CRUM unit (see paragraphs [133] to [134]). This setup is said to be advantageous over the prior art which required that a new unit be manufactured and, in particular, that the chip be replaced if the cryptographic algorithm had been cracked (paragraphs [133] and [135]).

The prior art

2. D1 discloses an authentication chip for the control of "consumables" such as print rolls in cameras or ink cartridges in printers (see column 4, lines 22-39).

2.1 Specifically, D1 is concerned with a mechanism able to detect cloned consumables and to block their use, but the authentication chip is also equipped with on-board memory to maintain "state information" (see column 23, line 46, to column 24, line 17; column 25, lines 52-54; column 43, lines 12-19, and column 69, line 64). The authentication chip is set up to authenticate itself towards the customer device (the printer or the camera) by means of an elaborate cryptographic protocol (column 25, lines 32-48). In this context, the use of "message authentication codes" is expressly mentioned (see column 9, lines 22-28, and column 12, lines 3-33).

2.2 The authentication chips are "programmable" (see column 62, line 49 *et seq., and* column 63, lines 2-3). The "programming" is carried out in a "Programming Station" (see column 68, lines 18-20 and 38-40). It is disclosed that manufacture of the chip does not require any particular security, except that the "programming environment" (or "Programming Station environment") must be secure (see *e.g.* column 67, esp. lines 24-25, 31-32 and 57-59, and column 73, lines 6-8).

2.3 The chip is disclosed as having "[b]oot circuitry for loading program code" (col. 69, line 40, and col. 72, line 57 f.) and comprising a "state machine, processor, CPU or whatever is chosen to implement the protocol" (col. 69, lines 64-66).

Inventive step, main request

3. The examining division found (see the decision, reasons 16.2) that claim 1 of the main request differed from D1 by the features that

a) data used to update the information stored in the CRUM is encrypted and that

b) a communication message is generated by combining a message authentication code (MAC) and the encrypted data.

3.1 The examining division further considered that the need to "protect[] the confidentiality and integrity of data in transit" was a problem that would arise naturally in the context of D1, that both encryption and MAC were "standard techniques" for solving this problem (see the decision, reasons 16.3 to 16.5), and that therefore claim 1 of the main request lacked inventive step over D1 (reasons 16.6).

3.2 The appellant challenged the examining division's assumption that D1 disclosed the authentication chip to have its own OS and to carry out an "initialization operation" (see the decision, reasons 16.1, last two paragraphs, and reasons 18 to 18.2; and the grounds of appeal, points 2.5.1, 2.7, 2.11 and 2.12).

3.3 With regard to the operating system, the board agrees with the appellant. The secure programming environment discussed in D1 is not disclosed as being within the authentication chip, but rather appears to be part of an external "Programming Station environment" from which the authentication chip is programmed (see column 67, lines 24-25 and 58-59). And the "boot circuitry" in

the authentication chip "for loading program code" (column 69, line 40) is not an "operating system" either. Notwithstanding the fact that the term "operating system" in itself is a vague one, the board is not aware of anything in D1 that would qualify as the operating system of an authentication chip.

3.4 On the other hand, the board agrees with the examining division that the authentication chip of D1 has to be initialized so that it can perform its functions (see the decision under appeal, points 18 and 20.2) and that, therefore D1 at least implicitly discloses some form of "initialization operation".

4. The board finds that claim 1 of the main request differs from D1 by the following features:

a) and b) as mentioned above.

c) The CRUM chip has an own operating system separate from that of the main controller.

d) The OS of the CRUM chip "executes an initialization operation to independently initialize the state of the CRUM unit".

5. The appellant did not challenge the examining division's conclusion that differences a) and b) did not establish an inventive step. As the board agrees with the examining division on this point, it is not contentious and therefore does not require any further discussion.

6. With regard to difference c), the application states that the operating system on the CRUM chip increases

security (see paragraph [12]), and the appellant argues that it enables faster booting by executing the initialization operation independently from the main controller.

6.1 The board accepts that these might be advantages of the claimed invention over CRUM chips which provide state data in local memory, but are otherwise passive; such CRUM chips are well-known in the art.

6.2 The board disagrees however that the provision of a CRUM chip operating system achieves these advantages *over D1*.

6.3 The system of D1 provides an authentication chip which may store secrets that never leave it (see column 19, lines 35-39) and carries out authentication protocols autonomously. Hence, the independence of the authentication chip from the host device and the increased security are achieved even though the authentication protocols do not rely on an operating system on the authentication chip. The board is not persuaded that the claimed operating system in general further increases security and autonomy.

7. Instead, the board considers that the provision of an operating system achieves the effects which operating systems are generally known to achieve.

7.1 In particular, operating systems simplify software development and improve the portability of software across platforms by separating hardware-specific code from hardware-independent application code. This might enable, for example, the customization of the same kind of authentication chip for several consumer devices by uploading different authentication programs, and there-

by reduce costs in the manufacturing process. Operating systems also manage hardware resources, for instance those necessary for data communication.

7.2 Just as the advantages of operating system are well-known in the art, so too are their costs: operating systems require additional memory and processing time. The board appreciates that both resources are precious in the authentication chips of D1, but notes that this need not be prohibitive. Operating systems for security chips were known in the art before the priority date of the present application, in particular for smart cards. For example, both the JavaCard OS and the MultOS have been available since at least the year 2000. During the oral proceedings, the appellant conceded the existence of these operating systems without any documentary evidence.

7.3 The board notes that D1 discloses authentication chips usable in a variety of applications. Although the applications relating to printers and cameras are discussed in more detail (see *e.g.* column 4, lines 21 *et seq.*), it is expressly stated as being trivial to adapt the authentication chips for other uses (column 1, lines 28-31), smart card applications included (column 1, line 27). This *inter alia* provides, in the board's view, a clear indication to the skilled person that features of smart card chips such as their operating systems may be relevant for the authentication chips in question.

7.4 The board therefore considers that the skilled person would, as a matter of course, balance the advantages and the disadvantages of equipping the authentication chip according to D1 with an operating system, and

would provide such an OS as a matter of usual design, if the required resources were considered affordable.

7.5 The board further finds that, once an operating system was available on the CRUM chip, it would be obvious for any initialization procedure to be carried out under the control of the OS.

7.6 The board therefore concludes that claim 1 of the main request lacks inventive step over D1, Article 56 EPC.

Inventive step, first auxiliary request

8. With regard to the auxiliary request, the examining division acknowledged that the specifically claimed tasks of the "initialization operation" were not known from D1 (reasons 20.1) but found that, an initialization operation being known from D1, the specifically claimed steps were individually obvious initialization steps (reasons 20.2 to 20.3).

8.1 In the grounds of appeal (see point 2.21), the appellant made the general statement that the additional detail "move[d] the requirements of claim 1 further from D1 and ma[d]e more remote the possibility of the person skilled in the art deriving the features of claim 1 from a consideration of D1". In its letter of 5 April 2016 (page 4, paragraph 2), it added that the additional steps were "those that ha[d] a particularly advantageous effect when carried out in parallel with the activities of the main controller".

8.2 During the oral proceedings, the appellant referred to the "confirmation of a replacement time", which the application explains as "checking the remaining amount of toner or ink, anticipating time when the tone or ink

will be exhausted and notifying the main controller [...] of the time" (see paragraph [77]). The appellant stressed that this operation was specific to the application scenario of the present invention and argued that the printer would start-up more quickly when and because this step was carried out during initialization of the authentication chip.

8.3 In the board's view, however, any advantage the "confirmation of replacement time" may have from the claimed setup is not particular to that operation. Rather, the operation, albeit specific to the invention, profits from these advantages in the same way as any other operation that might be performed during initialization.

8.4 In the board's view, therefore, none of the appellant's arguments established that and why any one of the claimed initialization operations profited particularly from parallel processing on the CRUM chip.

8.5 The board takes the following view.

8.5.1 If the interaction between the authentication chip and the host of D1 requires preparation steps, it is a matter of necessity that these be performed before the communication can start. This applies in particular to everything necessary to enable communication, such as "setup of a communication channel" and "setting of internal and external clock signals", but also everything that is required to carry out the authentication of the chip vis-à-vis the host, such as "initial driving" (i.e. starting) "of application programs" (e.g. the cryptographic protocols), the

"initialization of a memory value" and "setting of register values in the CRUM unit".

8.5.2 The calculation of a secret key - which clearly qualifies as "secret information" in the sense of the claims - on the authentication chip may be considered to increase security for two reasons. A secret that is generated externally and has to be loaded into chip memory may leak during the upload process, which is avoided if the chip calculates the secret itself. Moreover, if the chip calculates the secret itself, it is possible to have that chip re-calculate the secret if it has been compromised (see also figure 6 of the application). For both reasons, the board considers it obvious to calculate the secret on the chip itself. That this must take place during "initialization" is obvious because the secret is needed for the subsequent communication between the authentication chip and the host system.

8.5.3 As regards the "confirmation of a replacement time", the board considers that the checking of the remaining amount of toner or ink during "initialization" solves the problem of enabling the image forming apparatus to inform the user in good time that a cartridge should be replaced. The board finds the claimed solution to be obvious however. In a nutshell, it would be obvious to the skilled person that a relevant state of the apparatus must be determined as soon as the user should know about it.

8.5.4 In summary, the board agrees with the conclusion of the examining division that the additionally claimed operations are obvious initialization tasks for the authentication chips according to D1.

8.6 Therefore, the board concludes that claim 1 of the first auxiliary request also lacks an inventive step over D1, Article 56 EPC.

Inventive step, second auxiliary request

9. Claim 1 of the second auxiliary request was amended by incorporation of previous claims 2 to 4.

9.1 Literally, this meant the addition of four new features (corresponding to the last four paragraphs of claim 1 and labelled f) to i) in the grounds of appeal, see page 5, paragraphs 2 to 5). The appellant however made clear during oral proceedings that the first three additional features were added only because the dependency of the previous claims 2 to 4 so required and did not argue that any of these made and contribution towards inventive step of claim 1. The board agrees, noting also that the features of claims 2 to 4 were already addressed, explicitly or implicitly, in the above analysis.

9.2 The appellant argued that the amendments had the primary effect that the apparatus could select one of a plurality of encryption algorithms to be used, and the fact that the selected algorithm corresponded to the algorithm of the CRUM unit meant that the algorithm used by the CRUM unit could also be changed (see grounds of appeal, page 5, paragraph 6).

9.3 In the board's view, the possibility for the apparatus to select one of a plurality of encryption algorithms does not imply that the CRUM unit has the same possibility. The board also considers that claim 1 does not explicitly require it. The board reads the last feature of claim 1 as specifying that each CRUM unit

could use any one (but typically only one) "from a plurality of encryption algorithms" and that the apparatus can select the same one so as to be able to communicate with the CRUM unit.

9.4 Therefore, the effect of the additional feature is not that the CRUM unit and the apparatus can agree on a new encryption algorithm if the old one was cracked. Rather, its effect may be considered to be that one apparatus is able to communicate with - i.e. be compatible with - CRUM units using different encryption algorithms.

9.5 The board considers that this compatibility requirement may arise naturally. The printer manufacturer may want, for instance, to allow the use of CRUM units of a different component supplier or to remain backward compatible with an earlier generation of its own CRUM units. If the external supplier or the latest generation of CRUM chips use a different encryption algorithm, the compatibility requirement directly implies the need for the apparatus to support several encryption algorithms.

9.6 As a consequence, the board considers the added feature to be the obvious solution to a compatibility problem which would naturally arise. Therefore, the board comes to the conclusion that also claim 1 of the second auxiliary request lacks inventive step over D1, Article 56 EPC.

10. During oral proceedings, the appellant made reference to figure 6 and paragraphs [132] to [135] of the application as originally filed to support its case

(paragraphs [153] to [153] referred to in the letter of 5 April 2016 for the same purpose do not exist).

10.1 Arguably, these paragraphs imply that the encryption algorithm in the CRUM unit may be changed and that of the apparatus in response, too (see especially paragraph [134], second sentence).

10.2 At the same time, the cited disclosure is not without problems. Figure 6, stated to provide a "schematic view of the process of changing an cryptographic algorithm" in paragraph [132], contains a component labelled "KMS" which is explained to mean "key management system" in paragraph [132]. The KMS is disclosed to contain a "key write system" and to be capable of generating "key generating data". No further detail about the KMS is disclosed anywhere in the description, not even whether it is a component of the CRUM chip or of the image forming apparatus. The same applies to the "key write system" and the "key generating data". Also, figure 6 depicts the KMS issuing a new key to the CRUM unit, and paragraph [133] states that the "cryptographic algorithm may be changed by acquiring a new key from the KMS". Thus the actual change of the cryptographic algorithm is not detailed anywhere in the description.

10.3 In the board's judgment the language of claim 1 of the second auxiliary request is clear with regard to the feature in question. Hence, the description and figures cannot be invoked to give a more limited interpretation of claim 1 in order to give weight to the appellant's argument in favour of inventive step.

Summary

11. There not being an allowable request, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated