Internal distribution code:

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

Datasheet for the decision of 19 March 2014

Case Number: T 1210/10 - 3.5.06

Application Number: 99913850.6

Publication Number: 990326

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
APPARATUS AND METHOD OF READING A PROGRAM INTO A PROCESSOR

Applicant:
Motorola Solutions, Inc.

Headword:
Secure loading/MOTOROLA

Relevant legal provisions:
EPC Art. 123(2)
EPC 1973 Art. 56
RPBA Art. 15(3)

Keyword:
Oral proceedings - held in absence of appellant
Amendments - added subject-matter (no)
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 1210/10 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 19 March 2014

Appellant: (Applicant)	Motorola Solutions, Inc. 1303 East Algonquin Road Schaumburg IL 60196 (US)
Representative:	Boult Wade Tennant Verulam Gardens 70 Gray's Inn Road London WC1X 8BT (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 16 December 2009 refusing European patent application No. 99913850.6 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. Rees
Members: M. Müller
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with written reasons dispatched on 16 December 2009, to refuse the European patent application no. 99913850.6 for violation of Article 123 (2) EPC. The decision also referred to *inter alia* the documents

D1: "Cryptographic Microcode Loading Controller for Secure Function", IBM TDB, Vol. 34, No. 4B, pp. 34-36, September 1991 and
D2: WO 98/15082 A1,

and argued, in a section entitled "Further Remarks", that independent claims 1 and 7 lacked an inventive step over D1 and D2, Article 56 EPC 1973.

II. An appeal was lodged on 24 February 2010 and the appeal fee was paid on the same day. A statement of grounds of appeal was received on 26 April 2010. It was requested that the decision under appeal be set aside and, as a main request, that the application proceed to grant based on the documents on file at the time of the decision or, as an auxiliary request, based on an amended set of claims as filed with the grounds of appeal. The present application documents thus are as follows:

claims, nos.
1-10 as filed with letter of 10 March 2008 (main request) or with the grounds of appeal (auxiliary request)
description, pages
1, 5, 6 as published
2, 2a, 3, 4, 7, 8 as filed with letter of 10 March 2008
drawings, sheets
1/2-2/2 as published

III. With a summons to oral proceedings, the board informed the appellant that, according to its preliminary opinion, the main request complied with Article 123 (2) EPC but did not show an inventive step in the sense of Article 56 EPC 1973, in particular over D1 in combination with D2.

IV. The appellant did not respond in substance to the board's considerations, filing neither amendments nor arguments. Instead, with letter dated 11 March 2014, the appellant indicated that neither the applicant nor the representative would be attending oral proceedings.

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

"A method comprising the steps of: entering (301) a bootstrap mode of a processor (101); during the bootstrap mode: reading (303), by a memory (105) within the processor (101), a bootstrap program from a device external (103) to the processor (101); decrypting (307) the bootstrap program yielding a decrypted program; characterised by performing (311) authentication verification on the decrypted program; executing (317), by the processor (101), the decrypted program only after the decrypted program is authenticated, and when the decrypted program fails to be authenticated, inhibiting (315) execution of the decrypted program by the processor (101)."

Claim 1 of the auxiliary request coincides with that of the main request except that the "decrypting" step reads as follows:

"... decrypting (307) the bootstrap program using a key embedded inside the processor (101) yielding a decrypted program; ..."

Both requests also contain an independent processor claim 7 which corresponds largely with the respective independent method claim.

VI. Oral proceedings took place as scheduled in the absence of anyone for the appellant. At the end of the oral proceedings, the chairman announced the board's decision.

Reasons for the Decision

Decision in the appellant's absence

1. According to Article 15(3) RPBA the board is not obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned. Therefore, and further in accordance with Article 15(3) RPBA, the board treats the appellant as relying only on its written case. The following reasons are substantially those communicated to the appellant in the annex to the summons to oral proceedings.

The invention

2. The application relates to a processor which, in a "bootstrap mode", downloads a program from an external source for later execution, and addresses the problems that the external source may be tampered with and that undesirable programs may enter the processor. The invention is meant to solve these problems while maintaining the possibility to reprogram the processor at a later time (original description, p. 1, lines 32-36, and p. 2, 1-5).

2.1 As a solution it is proposed to use encryption and authentication to secure the download: Programs are loaded in encrypted form so that the processor must decrypt them before execution. Additionally, the decrypted program must pass an authentication procedure before it is allowed to run on the processor.

2.2 The application describes a single "preferred embodiment" and mentions several times that the key used for decryption is "embedded inside", or "stored within", the processor (see p. 2, lines 35-36; p. 3, lines 28-31; p. 6, lines 22-24; fig. 1). This feature was also contained in independent claims 1 and 7 as originally filed. Independent claims 1 and 7 according to the main request lack this feature, while those of the auxiliary request contain it.

The prior art

3. D1 discloses a microcontroller having the option to update microcode by loading it from an external source (see *e.g.* p. 34, 2nd par.). It is observed in D1 that manufacturers of microcontrollers "consider the microcode proprietary" and do not wish to have it exposed "while awaiting loading" (see *e.g.* p. 34, last par.). As a solution D1 proposes to "encrypt the microcode for transportation and storage and decrypt it "within the confines of the microcontroller itself" (p. 35, 3rd par.). This may happen "on power-up, reset, or specific command" (p. 35, 5th par.). It is disclosed that the decryption key, which the microcontroller must "have", is kept in a "key storage element" (see *loc. cit.* and the figure). It is further disclosed that the entire microcontroller may be coated with a material which cannot be removed without ruining the chip and thereby

preventing access to secure data (see sentence bridging pp. 35 and 36).

4. D2 relates to the update of program code - specifically computer firmware such as the BIOS - in general computing systems (see p. 1, 1st and 2nd par.) and addresses the security of this operation (see p. 2, 2nd par.). It is proposed to require that a new BIOS be authenticated before it can be written into the BIOS memory. It is disclosed to provide a cryptographic coprocessor which stores the BIOS and enforces authentication of BIOS updates (see p. 2, last par.; fig. 1). It is disclosed that the cryptographic coprocessor may be part of the host processor and that the key needed for authentication may be preloaded in the host processor (p. 5, lines 1-3; p. 7, 2nd par.). If authentication fails, the new BIOS is deleted and is never used (p. 6, lines 9-12). D2 also discloses that "BIOS upgrade code could be encrypted" (p. 6, 4 lines from the bottom).

Added subject matter

5. Independent claims 1 and 7 as originally filed required that the "key [was] embedded inside", or "stored within", the processor while the independent claims of the present main request, identical to those subject to decision under appeal, lack this feature. The decision argued (reasons 10) that the omission of this feature was not allowable because the description did not disclose "that the key could be provided in [any other] way" than embedded in the processor.

5.1 The appellant refers to a sentence in the description (p. 6, lines 22-24) saying that "[t]he key ... used for decryption is embedded inside the processor in the preferred embodiment" and argues that "[a] common sense

reading of this statement would make it clear that" it was only preferred but not essential for the invention for the key to be embedded inside the processor (p. 2, 7th par.). The decision under appeal dismissed this argument because the description left open "what the non-preferred embodiments would be". *Inter alia*, the decision argues (reasons 10.1) that non-preferred embodiments might not need encryption at all. The decision under appeal thus seems to argue that the original description does not disclose an embodiment in which encryption is used but based on a key stored outside the processor.

5.2 On the same point the decision argues (reasons 10) that omission of the feature is not warranted by the test according to the then applicable Guidelines C-VI, 5.3.10, "since it requires modification of other features to compensate for the change".

5.3 It appears to be undisputed that the sentence on page 6, lines 22-24, by explicitly referring to the preferred embodiment, implies that the pertinent feature may not be present in other embodiments. The board further considers that the statement must be read in its context, namely a paragraph which throughout, before and after the pertinent sentence (p. 6, 2nd par.), discusses encryption. In this context it would be implausible for the skilled person to read, as the decision suggests, the sentence as invoking embodiments which do not use encryption at all. Rather, the skilled person would read this sentence as disclosing, directly and unambiguously, that the decryption key could also be stored outside the processor, in the context of the otherwise unchanged preferred embodiment. The board also agrees with the appellant that the omission of the "embedding" feature does not seem to require "real mo-

dification of other features ... to compensate for the change" (see grounds of appeal, p. 3, lines 1-3).

5.4 In summary, the board disagrees with the decision under appeal in finding that the independent claims of the main request do not go beyond the application as originally filed, Article 123 (2) EPC.

Inventive step

6. During examination, document D1 was consistently used as the starting point for the assessment of inventive step. The board agrees that this is a suitable choice, if not the only one as was explained in the summons.

6.1 According to the decision under appeal claim 1 of the main request differs from D1 in the use of authentication in addition to the use of encryption (see reasons 11.1, feature a). The appellant appears to agree with this position (grounds of appeal, p. 3, 2nd par.), and so does the board.

6.2 The appellant argues that the decision under appeal was wrong to base their inventive step objection an a combination of documents D1 and D2 because "a person skilled in the art would not combine these two documents" (grounds of appeal, p. 3, 3rd par.). Thus D2 would not have prompted the skilled person to add authentication to D1. Neither would, so the appellant seems to argue, the common knowledge in the art. As a consequence, the claimed invention was novel and inventive over the cited prior art.

6.3 The board notes that the appellant does not seem to question that D1 and D2 are compatible with each other or that this combination, were the skilled person to

consider it, would yield the claimed invention. Rather, the appellant appears to argue only that the skilled person, starting from D1, would not have had any reason to consider the incorporation of authentication measures as known from D2 (see grounds of appeal, p. 3, 4th and 5th par.).

7. Specifically, the appellant appears to argue as follows with regard to D1: Microcode, being proprietary, will "only be issued by the ... manufacturer" of the pertinent microcontroller. Thus the manufacturer has control over both sides of the microcode transmission, can freely determine the decryption/encryption algorithm used and make sure that only authorized personnel is able to send valid encrypted data. Access to the encryption key and algorithm would then be tantamount to a proof of authorization so that there would be no need for providing specific authentication measures in addition to encryption. The appellant also argues that the skilled person, if he were to increase to security of the system of D1, would not consider authentication but rather modify the encryption by, for instance, increasing key size (grounds of appeal, p. 3, penult. par.).

7.1 The board agrees with the appellant that, in specific circumstances, it might not be worthwhile to invest the effort of using authentication in addition to encryption. The board however considers that in other situations the skilled person would know that authentication is worth the effort because it provides a qualitative increase in security as opposed to a mere quantitative improvement achieved for instance by using longer keys. The board also disagrees with the appellant's opinion that D1 is so narrow as to discourage the skilled person from considering authentication in such situations.

7.2 The board takes the view that microcode, even if proprietary, may well be produced by different companies or departments within a company. It is noted that D1 does not exclude this possibility. Further, the more complex the development situation the more difficult it would be for the manufacturer to keep tight control over the encryption algorithms and keys. As a consequence, a key - whatever its size - might leak and the manufacturer would, in the board's view, naturally address this security risk by adding further, separate security measures to the system of D1.

7.3 The board also disagrees with the appellant's allegation that the only obvious way to address the "risk of an encryption scheme being broken [is] to increase the key size" (grounds of appeal, p. 3, penult. par.) but considers it equally obvious to combine two different security measures with each other: For instance, in order to increase the protection of a door, the board deems it equally obvious to use a stronger lock as to use two different locks.

8. Encryption protects data by limiting its exposure to the owner(s) of the decryption key who will normally be only the rightful receiver(s) of the data. Authentication protects data against silent modification by a fraudster and thus ensures that the receiver can verify authorship. The board considers that the skilled person familiar with encryption will also be familiar with authentication and the differences between both, use them according to circumstances and have no difficulty in practicing either. The skilled person will, in the board's view, also be aware of the relative advantages of encrypting data before adding authentication information (*e.g.* a digital signature) and, as required by

the claims, adding authentication first and encrypting the data then.

9. In view of this, the board concludes that the skilled person would indeed consider D2 in trying to increase the security of the system of D1. In doing this, the skilled person would not limit himself to making encryption stronger but would also consider additional security measures. In considering D2, the skilled person would realise that authentication and encryption serve different but complementary purposes which can be easily combined with each other. The skilled person would thus, in the board's present view, not hesitate to incorporate the teaching of D2 into D1 and so arrive at the claimed invention without an inventive step in the sense of Article 56 EPC 1973.

10. The independent claims of the auxiliary request differ from those of the main request in requiring that the decryption key be embedded inside the processor.

10.1 Document D1 discloses that the decryption key is stored in a dedicated key storage (p. 35, penult. par.) which is part of the microcontroller, if not the microprocessor. D1 also discusses physical protection mechanisms for preventing access to secure data (p. 35, last par. - p. 36, 1st par.). In view of this the board deems it to be obvious, to the skilled person adapting the method of D1 from a microcontroller to a mere processor, to provide a dedicated key storage such as for example a key register within the processor.

10.2 Document D2 discloses specifically that the host processor is "preloaded" with the key needed for authentication (p. 7, 2nd par., last sentence). Insofar as D2 refers to encryption (p. 6, lines 3-5 from the bottom)

this suggests to the skilled person that the decryption key used by the cryptographic coprocessor is preloaded into - *i.e.* embedded in - the host processor, too.

10.3 The board therefore finds that the "embedding feature" of the auxiliary request does not establish an inventive step over either D1 or D2. The analysis of the main request as given above thus carries over to the auxiliary request and shows that its independent claims of the auxiliary requests also lack an inventive step, in the sense of Article 56 EPC 1973 over D1 and D2.

11. The being no allowable request, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

A. Vottner D. Rees

Decision electronically authenticated