Internal distribution code:

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

Datasheet for the decision of 21 April 2021

Case Number: T 1716/12 - 3.5.06

Application Number: 07749803.8

Publication Number: 2011049

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
SELECTIVELY UNLOCKING A CORE ROOT OF TRUST FOR MEASUREMENT (CRTM)

Applicant:
Hewlett-Packard Development Company, L.P.

Headword:
Conditional CRTM unlocking/HP

Relevant legal provisions:
EPC 1973 Art. 84, 56, 111
RPBA 2020 Art. 11

Keyword:
Claims - clarity (yes)
Inventive step (yes)

Decisions cited:

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 1716/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 21 April 2021

Appellant: (Applicant)	Hewlett-Packard Development Company, L.P. 10300 Energy Drive Spring TX 77389 (US)
Representative:	Zimmermann, Tankred Klaus Schoppe, Zimmermann, Stöckeler Zinkler, Schenk & Partner mbB Patentanwälte Radlkoferstrasse 2 81373 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 27 February 2012 refusing European patent application No. 07749803.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	G. Zucka
	M. Müller

Summary of Facts and Submissions

I. The appeal is against the decision by the examining division, dispatched with reasons on 27 February 2012, to refuse European patent application 07749803.8, on the basis that claim 1 was not clear (Article 84 EPC 1973) and lacked novelty (Article 54 EPC 1973) in view of the following document:

D1 = US 2003/208338 A1

The following documents were also cited during the examination procedure:

D2 = US 2006/010326 A1
D3 = US 2002/120845 A1
D4 = US 2005/021968 A1

II. A notice of appeal was received on 23 April 2012, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 14 June 2012.

III. On 26 May 2017, the board sent to the appellant a communication pursuant to Rule 100(2) EPC. It expressed its preliminary opinion that the subject-matter of claim 1, and for similar reasons claim 7, was not inventive; Article 56 EPC 1973.

IV. On 15 September 2017, the appellant replied to this communication, filing a new claim set and providing arguments in favour of the presence of an inventive step.

V. On 19 November 2019, the board issued a summons for oral proceedings, to be held on 5 February 2020.

VI. On 23 December 2019, the appellant replied to the summons, filing a new claim set and providing arguments in favour of the presence of an inventive step. He also informed the board that he did not intend to attend the oral proceedings.

VII. On 14 January 2020, in view of the new submissions, the board cancelled the scheduled oral proceedings.

VIII. The appellant requests that the decision under appeal be set aside and a patent be granted on the basis of claims 1 to 8 filed on 23 December 2019. The further text on file is:

description pages
2 to 8 as published,
1, 1a and 1b received on 8 December 2010;

drawing sheets
1 to 3 as published.

IX. Independent claim 1 reads as follows:

"A computer system (100), comprising:
processor (134); and
a Basic Input/Output System (BIOS) module (110) coupled to the processor (100),
wherein the BIOS module (110) comprises a boot block (112) storing instructions executed during a boot process of the computer system (100) and a signature domain (116) storing a signature, wherein the boot block (112) and the signature domain (116) are used as a Core Root of Trust for Measurement (CRTM) (118) that specifies predefined policies and is configured to perform integrity measurements to establish whether the

computer system (100) can be trusted, wherein the CRTM is configured to conditionally unlock itself, wherein the boot block (112) comprises a lock function (114);

wherein the computer system is configured to execute the lock function (114) during each boot process of the computer system (100) before the boot block (112) transfers control to an operating system of the computer system, wherein the lock function (114) is configured to search a predetermined location (119) of the BIOS module (110) for a signature, to unlock the CRTM (118) and to delete the signature in the predetermined location if the signature stored in the signature domain (116) and the signature in the predetermined location (119) match, and to lock the CRTM (118) if the signatures do not match; and

a CRTM update utility (152) configured to update the CRTM (118) during the computer system's runtime once the computer system has booted if the CRTM (118) is unlocked."

X. Independent claim 5 relates to a method having method features corresponding to the apparatus features of claim 5, comprising a step of configuring the BIOS, and steps carried out by the computer system in use. Claim 5 reads as follows:

"A method, comprising:

configuring at least part of a Basic Input/Output System (BIOS) (110) to provide Core Root of Trust for Measurement (CRTM) (118) functions that specify predefined policies and are configured to perform integrity measurements to establish whether a computer system (100) can be trusted;

during each boot process of the computer system and before transferring control to an operating system of the computer system, unlocking the CRTM if a signature

stored in a signature domain of the CRTM (118) and a signature in a predetermined location of the BIOS (110) match, deleting the signature in the predetermined location of the BIOS 8110) if the signatures match, and locking the CRTM (118) if the signatures do not match; and

if the CRTM (118) is successfully unlocked, updating the CRTM (118) during the computer's runtime once the computer associated with the CRTM (118) has booted."

Reasons for the Decision

1. *The admissibility of the appeal*

The appeal is admissible.

2. *The invention*

The application relates to a computer system comprising a processor and a BIOS coupled to the processor. The BIOS module stores a Core Root of Trust for Measurement(CRTM), wherein the CRTM conditionally unlocks itself. In order to allow an update of the BIOS whilst protecting the CRTM validity, the CRTM conditionally unlocks itself and it is updated during the computer's runtime.

3. *Amendments; Article 123(2) EPC*

3.1 The board has established that the amendments introduced in claim 1 are disclosed in the original application documents.

3.1.1 "the BIOS module comprises a boot block storing instructions executed during a boot process of the computer system and a signature domain storing a signature, wherein the boot block and the signature domain are used as a Core Root of Trust for Measurement (CRTM)": This is disclosed in par. [0012].

3.1.2 "[The CRTM] specifies predefined policies and is configured to perform integrity measurements to establish whether the computer system can be trusted": This is disclosed in par. [0001], lines 5 and 6, and in par. [0013], line 12.

3.1.3 "the CRTM is configured to conditionally unlock itself": This is implicitly originally disclosed in par. [0014] and [0015], because the CRTM is unlocked if the signatures match and remains locked if the signatures do not match.

3.1.4 "the computer system is configured to execute the lock function during each boot process of the computer system": This is disclosed in par. [0014], first two sentences.

3.2 The amendments to claim 1 therefore satisfy the requirement of Article 123(2).

3.3 The amendment to claim 5 also satisfies the requirement of Article 123(2), for the reason given under 3.1.2 above.

4. *Clarity; Article 84 EPC 1973*

4.1 According to the appealed decision (Reasons point 11), then claim 1 recited a lock function being comprised in a boot block, and a CRTM that selectively unlocks itself. It further specified that the lock function unlocks the CRTM under certain circumstances. This left the reader in doubt as to whether the recited lock function is precisely the part of the CRTM that selectively unlocks it, or whether it is a separate lock function, meaning that there are two lock functions, one belonging to the CRTM for self-unlocking itself and one outside the CRTM but still in the boot block, for selectively unlocking the CRTM from the outside. The decision hence considered then claim 1 to be unclear (Article 84 EPC 1973), given that the description did not support two separate lock functions.

4.2 The board considers that this clarity objection has been remedied by the specification in present claim 1 that it is the boot block, which is part of the CRTM , which comprises a lock function. The present wording of the claim thus excludes the interpretation that there may be a separate lock function outside the CRTM but still in the boot block.

4.3 The board itself raised the following clarity and interpretation issues in its communication of 19 November 2019:

4.3.1 The expression "runtime once the computer system has booted" needs to be interpreted rather broadly, as was set out in the communication of 26.05.2017, point 5.

4.3.2 The term "selectively" is unclear (Article 84 EPC 1973) and should probably be replaced by "conditionally".

4.3.3 The wording "before the boot block (112) transfers control to an operating system" leaves doubt whether the transfer is part of the claimed subject-matter and therefore renders the claim unclear (Article 84 EPC 1973).

4.3.4 Similar remarks apply to independent claim 5. In addition, it is not clear what is meant by "a method for a computer system". This wording should probably be replaced by "a method of operating a computer system".

4.3.5 It may also have to be discussed whether claim 1 is unclear due to the fact that it concerns a computer system defined in terms of method steps ("the BIOS module ... stores", "the lock function ... is executed").

4.3.6 The appellant is also invited to advance reasons why the term "Core Root for Trust Management (CRTM)" must be considered clear and how precisely it has to be interpreted. Presently, the board has its doubts. In particular, it should be explained whether, as the board considers, the CRTM must be construed as program code and how a piece of program code can be construed as comprising a boot block and a signature domain, as the claims require.

4.4 The board is satisfied that those issues were dealt with satisfactorily by amendment and by argument (see the appellant's letter received on 23 December 2019, pages 2 to 4):

4.4.1 The board still judges that the expression "runtime once the computer system has booted" needs to be interpreted rather broadly. It is however satisfied that the claim's wording at least implies that the computer system has a BIOS module comprising a part called a "boot block", which stores instructions that are carried out when the computer system starts, including the execution of a lock function, and "runtime" is the time after those instructions have been carried out.

4.4.2 The term "selectively" in claim 1 has been replaced by "conditionally", as suggested by the board.

4.4.3 The board has come to the conclusion that the phrase "before the boot block transfers control to an operating system" does not imply that the transfer itself is a step of claimed method. The board deems this phrase to be redundant, because everything the CRTM does must necessarily be before it yields control to the operating system, but not to a degree that the claim would be rendered unclear.

4.4.4 Regarding independent claim 5, the unclear expression "for a computer system" was removed.

4.4.5 Claims 1 to 4 directed to a computer system are no longer defined in terms of method steps.

4.4.6 As regards the meaning of the term "Core Root for Trust Management (CRTM)", the appellant referred to the National Institute of Standards and Technology (NIST) which defines it as follows (see https://csrc.nist.gov/glossary/term/Core_Root_of_Trust_for_Measurement):

"The first piece of BIOS code that executes on the main processor during the boot process. On a system with a Trusted Platform Module the CRTM is implicitly trusted to bootstrap the process of building a measurement chain for subsequent attestation of other firmware and software that is executed on the computer system."
Source(s):
NIST SP 800-147

The document NIST SP 800-147 is not pre-published. Nonetheless, with reference to prior art documents - such as, for instance, H. Brandl, "Trusted Computing: The TCG Trusted Platform Module Specification", Embedded Systems 2004, section 4.1 - the board has convinced itself that it reflects the understanding of the skilled person at the priority date of the present application as to what is a CRTM, in particular that it is primarily BIOS *code*.

By stating that "the boot block and the signature domain are used as a Core Root of Trust for Measurement (CRTM)", claim 1 effectively redefines a CRTM, i.e. in the application the CRTM comprises not only code but also (variable) data, viz. the signature domain. From the context of the claim, the expression "are used as" is to be interpreted as "constitute".

The board considers such definition to be clear.

5. *Inventive step; Article 56 EPC 1973*

5.1 According to the board, D1 is a suitable starting point for the analysis of inventive step.

5.2 As set out in the appealed decision (Reasons 12.1), D1 discloses a computer system (see [0019]) comprising:

a processor (see [0019]);

a Basic Input Output System (BIOS) module coupled to the processor and comprising a boot block (see [0019]-[0021]),

wherein the boot block comprises a lock function (see par. [0023] : "boot block is normally locked" and par. [0028] indicates explicitly that "the boot block will be locked prior to continuing the POST sequence if the digital signature is not valid". The boot block is technically the first code executed, which implies that it performs this lock function itself. In any case, if some form of locking routine was present before what is referred to as boot block in D1, the combination of this locking routine and of the boot block would correspond to the claimed boot block);

wherein the BIOS module stores a Core Root of Trust for Measurement (CRTM) (see [0020]) that selectively unlocks itself (see [0023] : "boot block is normally locked" and [0024]: "if the signature is authentic, the POST sequence will continue with the boot block unlocked");

wherein the lock function is executed during each boot process of the computer system (see par. [0023]: "boot block is normally locked" and par. [0028] indicates explicitly that "the boot block will be locked prior to continuing the POST sequence if the digital signature is not valid". The boot block is technically the first code executed, which implies that it performs this lock function itself and is executed during each boot),

the lock function searching a predetermined location of the BIOS module for a signature and unlock the CRTM only if the signature is present and valid (see par. [0028] : "the digital signature of the updated POST/BIOS routine is authenticated"- which implies a search for their presence and a validation.

"if the signature is authentic, the boot block remains unlocked" and is locked otherwise (see last sentence). It is noted that these signatures are stored in a secure communication buffer that is apparently on a physically distinct EEPROM from the memory including most of the BIOS code, see par 20 and figure 2. However, there is no unambiguous definition of what exactly constitutes the BIOS, especially for new technology where the code in what traditionally constitutes the BIOS is modified as in the present case. Hence, it is legitimate to consider the "BIOS" to also comprise code and data in the physically separate EEPROM 220 that is involved in BIOS-level functions.)

The appellant has not objected this finding and the board agrees with it.

5.3 The subject-matter of claim 1 distinguishes itself from D1 in that:

- An update takes place not before but after authentication;

- The boot block is used as part of the CRTM;

- The computer system additionally comprises a CRTM update utility configured to update the CRTM during the computer system’s runtime once the computer system has booted;

- The CRTM additionally comprises a signature domain storing a signature;

- The lock function is executed before the boot block transfers control to an operating system of the computer system;

- The lock function deletes the signature in the predetermined location if the signature stored in the signature domain and the signature in the predetermined location match.

5.4 The essential distinguishing features are:

(1) the CRTM is updated after the boot process, and

(2) the signature in the predetermined location is deleted if the signature stored in the signature domain and the signature in the predetermined location match.

5.5 Feature (1) has the effect that the boot code does not need to include code for updating the CRTM.

Feature (2) has the effect that only one boot cycle is available for updating the unlocked CRTM and, upon subsequent reboot, the lock function will cause the CRTM to lock unless a correct signature has been written again in the predetermined location. Although this is not explicitly stated in the description, the implication is that security is enhanced.

5.6 The problem solved by the distinguishing features is therefore to provide a CRTM update functionality which is not part of the boot code, whilst minimising the impact on security.

5.7 Features (1) and (2) are not disclosed by any of the prior art documents:

In D2, controlled and certified code is incorporated into the function of the CRTM. The existing CRTM is not

modified but extended. The signature used in D2 is not deleted;

D3 relates to authentication of a remote entity so that it may change hard-locked critical security information normally accessible only during the POST and only to trusted entities such as the BIOS. D3 mentions neither a CRTM nor a signature;

D4 relates to secure firmware updating using authentication credentials. The CRTM is not updated and there is no signature deletion.

There is also no apparent reason why the skilled person would want to introduce features (1) and (2) in the computer system disclosed by D1, even if he or she wanted to solve the mentioned problem of increasing security.

5.8 The board therefore holds that the subject-matter of independent claim 1 and, for similar reasons, of independent claim 5 is inventive (Article 56 EPC 1973).

6. *Other issues*

The board has no occasion to raise any objections to the claims on its own volition.

However, the board notes that the description appears to require adaptation to the present claims. In the present case, the board takes the view that for instance the sentence spanning pages 3 and 4 of the description, stating that "*In at least some* embodiments, the BIOS 110 of the computer 100 comprises a boot block 112 and a signature domain 116 used as a CRTM 118A" needs adaptation under Article 84 EPC 1973,

given that according to claim 1 this is the case for all embodiments.

7. *Remittal*

According to Article 11 RPBA 2020, the board shall not remit a case to the department of first instance, unless special reasons present themselves for doing so. In this board's view, the remittal "with a description to be adapted", as has become common practice of the boards of appeal, is, effectively, a remittal for further prosecution within the meaning of Article 111(1) EPC and under the limitations according to Article 111(2) EPC. As the appellant has indicated, its absence from oral proceedings, dealing with the adaptation of the description in the appeal proceedings would require a further written dialogue with the appellant before an eventual remittal with the order to grant a patent. The board takes the view that it is more efficient to deal with the adaptation of the description as part of the grant procedure under Rules 71(3) and (6) EPC, and considers this to be special reasons for remittal under Article 11 RPBA 2020.

Order

For these reasons it is decided that:

1. The appealed decision is set aside.
2. The case is remitted to the first instance for further prosecution.

The Registrar: The Chairman:

L. Stridde W. Sekretaruk

Decision electronically authenticated