Internal distribution code:

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

Datasheet for the decision of 11 October 2016

Case Number: T 1892/13 - 3.5.06

Application Number: 07867226.8

Publication Number: 2080095

IPC: G06F9/48

Language of the proceedings: EN

Title of invention:
SYSTEM AND METHOD FOR SHARING ATRUSTED PLATFORM MODULE

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

Headword:
Sharing a Trusted Platform Module/HEWLETT-PACKARD

Relevant legal provisions:
EPC 1973 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 1892/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 11 October 2016

Appellant: (Applicant)	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, TX 77070 (US)
Representative:	Zinkler, Franz 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 21 March 2013 refusing European patent application No. 07867226.8 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 21 March 2013, to refuse European patent application No. 07 867 226.8 for lack of inventive step.

II. A notice of appeal was filed on 17 May 2013, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 25 June 2013. The appellant requested that the decision be set aside and that a patent be granted on the basis of the pending application documents.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claims were unclear, Article 84 EPC 1973, and lacked inventive step, Article 56 EPC 1973, in particular over the prior art acknowledged in the application itself.

IV. In response to the summons, with a letter dated 11 August 2016, the appellant filed an amended set of claims to replace the claims on file.

V. Oral proceedings were held on 11 October 2016. During these proceedings, the appellant filed several new sets of claims, each replacing the earlier one, in which a number of features with which the board had issues under Article 84 EPC 1973 and Article 123(2) EPC were deleted. Claim 1 of the final set of claims 1-8 (filed at 15:05) reads as follows:

"A method for sharing a trusted platform module, TPM, (130) the TPM being in a computing system (10) using an operating system, OS, (121), the OS (121) extending

from a user process layer (21) through a system process layer (22) and into a kernel model layer (23) of the computing system (10),

the TPM (130) being a single command processing device configured to operate a single process at any time and which allows connection only with the entity which initiated the currently running process, the TPM (130) being unchangeable by a user,

the method using a device (234) being in communication with the TPM (130) via a first communication path, the device being in communication via a second communication path with the OS (121), the device (234) being configured to access to restricted TPM internal cryptographic functionalities via the first communication path

the method comprising:

at an OS level (21, 22, 23), accessing a desired security functionality of the TPM (130) disposed outside the OS (121) by executing (301) an OS-level process on the TPM (130);

receiving (304), from the device (234) via the second communication path, through the OS (121), a request for use of the TPM (130) by the device (234);

pausing execution of the OS-level process by the TPM (130); and

after pausing execution of the OS-level process, performing a communication between the TPM (130) and the device (234) using the first communication path and executing (312), by the TPM (130), the non-OS-level process."

The wording of independent system claim 5 corresponds largely to that of claim 1.

VI. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis

of the claims filed during the oral proceedings at 15:05. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application refers to the "industry standard specifications for hardware-enabled trusted computing and security technologies", in particular for what is called a trusted platform module (TPM) (see description, paragraph 1).

1.1 According to the description, a TPM provides security relevant operations such as encryption and decryption to an operating system (OS) and "securely wraps" them in a dedicated piece of hardware (see paragraph 1, lines 3-5). The description further states that a TPM is "essentially a single command processing device" which can only operate on a single process at a time and which allows connection only with the entity that initiated the currently running process (see paragraph 1, lines 5-10).

1.2 The application seeks to overcome limitations of the standard. Firstly, the application states that "it may be preferable to perform security operations [...] outside the control of the OS" because "firmware, which is outside the OS, may be more resistant to interference by user actions ..." (page 1, paragraph 2, lines 5-8). Secondly, if access to the TPM by other entities than the OS (e.g. BIOS, firmware or external devices) is allowed, then the single-process limitation

of the TPM may cause problems such as "delays and state corruption" (see page 2, lines 1-5). The description also alludes to protecting against "spoofing" by a "rogue OS" (see paragraph 8, lines 11-13).

1.3 The invention relates to "sharing a TPM" between a computing system and what the description refers to as a "system locality entity (SLE)" (see paragraph 8, lines 1-4). An SLE may effectively be any device close to the computing system which requires access to the TPM service (a smart card or USB device, firmware, BIOS, some circuit, "etc."; see paragraph 9, lines 5-10), provided it "adheres to TPM restrictions of not exposing the TPM internal cryptographic capabilities to a user or an application for general use" (see paragraph 8, lines 4-7). It is stated that the SLE "proves its 'locality' using either a hardware signal that cannot be spoofed by a rogue OS" or by communicating with the TPM on a designated memory mapped input/output (MMIO) range for that locality" (paragraph 8, last sentence).

1.4 When an SLE needs to access the TPM (figure 3, no. 302) the SLE authenticates itself to the TPM in order to obtain authorization (figure 3, no. 303; paragraph 18). Thereafter, the running "OS-level" process may be pre-empted. That is, the SLE process takes priority over the OS-level process, which is paused and eventually resumed (see paragraphs 19-21).

Claim construction

2. Claim 1 refers to a "trusted platform module", which, at first glance, may be understood as a component complying with the corresponding specifications

according to the standard of the Trusted Computing Group (TCG) mentioned in the description (see paragraph 1).

2.1 The standard (in its relevant version) is however not identified in the description, let alone set out in the claims. Moreover, the term "TPM", as used in the application, would be understood by the skilled person as not being compliant with the standard (see paragraph 7, last sentence).

2.2 The board therefore takes the view that the term "trusted platform module (TPM)" is a label for a hardware component which does not, by itself, imply any features. Rather, a TPM according to the claims is any component having the features expressly mentioned in the claims, namely that it is a "single command processing device" which is "unchangeable by a user" and provides "cryptographic functionalities". Hence the board takes the view that the skilled person would understand that the "desired security functionality of the TPM" must lie in providing "internal cryptographic functionalities".

3. Claim 1 does not define what it means for a TPM to be "unchangeable by a user". This justifying a broad reading, the board takes the view that any integrated circuit has this feature, because it is, to a degree, "unchangeable by a user".

4. Claim 1 refers to a "device" having two "communication paths", one between the TPM and the device and the other between the device and the OS. It is claimed that the second one is used for the access "request" from the device, through the OS, to the TPM and that the

first one is used for "a communication" between the TPM and the device after an OS-level process running on the TPM has been paused. The board understands that the latter communication must be distinct from the access request. Otherwise, it is undefined what that communication is or achieves. Also the nature of the communication paths is not specified.

Inventive step

5. The board considers that the most suitable starting point for assessing inventive step is the prior art acknowledged in the description.

5.1 It is clear from paragraph 1 of the description that a TPM is, *inter alia*, a single-threaded integrated circuit providing cryptographic services, and receives, from the main processor of the computing system and "through the OS", requests to perform "OS-level processes". Further details of the TPM are, in the board's judgment and as explained above, immaterial for the assessment of inventive step.

5.2 The differences between the subject-matter of claim 1 and the generic set-up acknowledged in the description are as follows.

(a) The TPM functionality is also accessible "through the OS" from an external "device".
(b) A running "OS-level process" is pre-empted (i.e. paused and replaced) by one originating from the device, referred to as a "non-OS-level process".
(c) After the OS-level process has been paused, "a communication" is performed between the TPM and the device.

5.3 Feature (a) implies a call to a corresponding OS interface function and thus the existence of one "communication path" between the device and the TPM. The "communication" according to feature (c), as it must be different from the access request, represents another, second "communication path". The board therefore considers that the claimed two communication paths do not represent a further difference between the claimed invention and the known set-up.

5.4 The appellant argued that feature (a) solved the problem of increasing security by providing the TPM services to the device "outside the control of the OS" (see the description, paragraph 1). The board disagrees. Claim 1 as it stands does not exclude all communication between the device and the TPM being "through the OS" and thus, to some extent, under the control of the OS.

5.5 The board therefore considers that features (a) and (b) solve the problem of making the valuable TPM services more widely available, i.e. to some "device" outside the computing system of which the TPM is a part.

5.6 In order to solve that problem, the skilled person would provide a suitable interface to the device, for instance as an obvious option, by making the existing OS interface available to it. This is difference (a). The skilled person would also be aware that multiple requests might have to be scheduled and be familiar with, *inter alia*, the concept of pre-emptive scheduling. During the oral proceedings, the appellant conceded that pre-emptive scheduling was common knowledge in the art. If the requests from the device were more urgent than the internal ones, an obvious scenario, the skilled person would, without taking an

inventive step, handle them by means of pre-emptive scheduling. This is difference (b).

5.7 An effect of feature (c) is that it provides a tighter coupling between the TPM and the device during scheduling. A more specific problem cannot be derived from feature (c) for lack of details in the claim of the communication in question.

5.8 The skilled person would realize, as a usual matter of design, that it would be useful for the device to be informed when its request is being served. Under these circumstances it would be obvious for the skilled person to provide "a communication" between the TPM and the device when execution of the "non-OS-level" device process is about to be executed.

6. In summary, the board comes to the conclusion that the subject-matter of claim 1 lacks inventive step over the the system known from the description, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated