Internal distribution code:

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

Datasheet for the decision of 16 May 2018

Case Number: T 2270/15 - 3.5.06

Application Number: 05708671.2

Publication Number: 1725923

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
SECURE MODE CONTROLLED MEMORY

Applicant:
Nokia Technologies Oy

Headword:
Secure mode controlled memory/NOKIA

Relevant legal provisions:
EPC 1973 Art. 84

Keyword:
Claims - clarity (no)

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 2270/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 16 May 2018

Appellant: (Applicant)	Nokia Technologies Oy Karaportti 3 02610 Espoo (FI)
Representative:	Ruuskanen, Juha-Pekka Page White & Farrer Bedford House John Street London WC1N 2BF (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 22 January 2015 refusing European patent application No. 05708671.2 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 is against the decision of the examining division, with reasons dispatched on 22 January 2015, to refuse European patent application No. 05708671 for lack of inventive step, Article 56 EPC 1973, and for lack of compliance with Article 123(2) EPC.

II. The appellant requests that the decision be set aside and that a patent be granted on the basis of claims 1-31, 1-27, 1-27 or 1-23, respectively, of a main request or one of three auxiliary requests as filed with the grounds of appeal.

III. Claim 1 of the main request reads as follows:

"A method of enhancing data security, which data is to be executed in an electronic device (101) comprising a secure execution environment (104) to which access is restricted, the method comprising the steps of:

generating (S303), in said secure execution environment, a new secret key repeatedly;

verifying (S302), in said secure execution environment, the integrity of data to be written into storage (110);

encrypting (S304), in said secure execution environment, the data by means of said new secret key; and

writing (S305) the encrypted data into storage; and

executing the encrypted data from the storage characterized by further comprising:

reordering address locations of said storage (110) in address space at the time of boot, wherein the order of the address locations in address space is altered."

Claim 1 of auxiliary request 1 differs from claim 1 of the main request in that the preamble also sets out that the data to be executed is "consisting of program code" and in that the new secret key is generated repeatedly "when the device is booted".

Claim 1 of auxiliary request 2 reads as follows:

"A method of enhancing data security, which data consisting of program code is to be executed by circuitry in an electronic device (100), wherein the circuitry comprises a secure execution environment (104) containing security related components to which access is restricted and a processor (103), the method comprising the steps of:

generating (S303), by the processor in a secure execution mode in which the processor is given access to said secure execution environment, a new secret key repeatedly when the circuitry is booted;

reordering address locations of a temporary memory (110) in address space at the time of boot, wherein the order of the address locations in address space is altered

receiving data from a permanent memory (112), wherein the permanent memory is external to the circuitry (101);

verifying (S302), by the processor in said secure execution mode, the integrity of data to be written into the temporary memory (110);

encrypting (S304), by the processor in said secure execution mode, the data by means of said new secret key;

writing (S305) the encrypted data into temporary memory (110);

setting the processor (103) in a normal operation mode where the processor is not given access to the secure execution environment; and

executing the encrypted data from the temporary memory.

Claim 1 of auxiliary request 3 differs from claim 1 of auxiliary request 2 in not containing the "reordering" and "setting" steps, and in that the "executing" step at the end of claim 1 has been replaced by the following text:

"... executing the encrypted data from the temporary memory,

setting, by a protected application, the processor (103) in one of at least two different operating modes; and

storing protected data relating to device security in the secure execution environment wherein

the processor is given access to said secure execution environment when the secure processor operating mode is set, and

the processor is denied access to said secure execution environment when a normal processor operating mode is set."

All requests also contain further independent claims relating to a system, a computer-program and a computer-readable medium which correspond to independent method claim 1.

IV. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the independent claims of all requests were unclear,

Article 84 EPC 1973, and lacked inventive step over the prior art on file, Article 56 EPC 1973.

V. In response to the summons, the appellant filed neither amendments nor arguments, but indicated in its letter of 1 May 2018 that it would not attend the oral proceedings and that the appeal should be decided without further submissions from its side.

VI. Oral proceedings took place on 16 May 2018 in the absence of the appellant. At their end, the chairman announced the board's decision.

Reasons for the Decision

The appellant's absence from the oral proceedings

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.

2. In its preliminary opinion, the board raised detailed objections under Article 84 EPC 1973 and, partially under the proviso of the clarity problems, under Article 56 EPC 1973. The appellant did not respond in substance to the board's preliminary opinion, and the board has no occasion to deviate from it. The following reasons are thus based on the board's major clarity objections, and, for the purposes of this decision, it

is not necessary to go into whether the claimed subject-matter also lacks inventive step.

The invention

3. The application relates to the secure execution of program code.

3.1 It considers the situation that a device contains program code in permanent memory which must, for execution, be copied into temporary memory (such as NAND and RAM, respectively; see figure 1, nos. 110 and 112; page 4, lines 24-29; page 14, lines 25-32).

3.2 Once the program code has been loaded from permanent memory, its "integrity" is verified, so as to ensure that it has not been tampered with during transmission (see page 4, lines 29-32). Before it is then stored in temporary memory, one or more new keys are generated and used to encrypt the program code (see page 5, lines 3-9, the paragraph bridging pages 7 and 8, and page 16, paragraph 3). It is disclosed that the new key (or keys) can be generated either at every new boot or only at some, chosen "randomly" or "regularly" (see page 6, lines 13-18).

3.3 Security relevant data such as cryptographic keys is stored in a dedicated storage area which is also referred to as a "secure execution environment". The processor has two operating modes (also referred to as "operation" or "execution" modes): a "secure" one and a "normal" one. Access to the secure execution environment is possible only in the secure mode (see page 9, line 30, to page 10, line 19; page 13, paragraph 2; figure 1, no. 104). More specifically, in

the secure mode, the device generates and stores the keys (see page 5, lines 5-9 and 28-31), verifies the program code integrity (page 16, lines 10-15) and encrypts the program code (page 16, lines 15-21).

3.4 The application states that "address locations [may be] permuted" or "re-ordered" "in address space at boot" or "reboot" so as to further "impede[] attacks on the system". The entire pertinent disclosure is contained on page 8 (lines 3-11) and is reproduced here for convenience:

"According to still another embodiment of the present invention, address locations are permuted in address space at boot. This permutation, or reordering, makes it difficult for an attacker to know where a specific address is located in address space. For example, the address located at position number 1024 in address space is, at reboot, mapped to address location number 2048. At a further reboot, the address is mapped to position number 512, etc. This impedes attacks on the system."

Clarity, Article 84 EPC 1973, and claim construction

4. The board considers that the independent claims of all requests are unclear due to the two processor operating modes (see subsequent point 5), and the independent claims of the main request and auxiliary requests 1 and 2 are further unclear due to the "reordering" feature (see point 6 below).

5. All claims contain the feature of "executing the encrypted data". The auxiliary requests make explicit that the data is program code. In the board's understanding, encrypted data cannot be executed

directly, but needs to be decrypted before execution. To the extent that the independent claims (all requests) leave this open, the board considers them unclear, Article 84 EPC 1973.

5.1 On the assumption that the data is decrypted before it is executed, the question arises where the keys are stored and from where the processor obtains them for decryption.

5.2 It is claimed that the keys are generated in the secure execution environment (main request and auxiliary request 1) by the processor operating in the secure execution mode (auxiliary requests 2 and 3). It is disclosed (but not claimed) that they are stored in the secure execution environment (see page 5, lines 28-31).

5.3 The independent claims of auxiliary request 2 specify that the processor operation mode is set to "normal" before the "encrypted data" is executed and that, in the normal operation mode, the processor has no access to the secure execution environment. The keys being stored there, this seems to imply that the processor has no access to the keys necessary for decrypting the data to be executed.

5.4 Claim 1 of auxiliary request 3 specifies that the processor has a normal operating mode but not when the normal mode is set. This also renders claim 1 of auxiliary request 3 unclear, Article 84 EPC 1973.

6. The step of "reordering address locations" (contained in the independent claims of all but auxiliary request 3) is unclear.

6.1 The examining division found the reordering feature to be the only difference between claim 1 of the then main request and the closest prior art (see page 5, paragraph 2). The appellant did not challenge this finding, but based its arguments in favour of novelty and inventive step of the main request exclusively on the reordering feature (see the grounds of appeal, points 3.3.1 to 3.3.17).

6.2 Claim 1 of the main request and auxiliary request 1 leaves open which address locations are "reordered". Claim 1 of auxiliary request 2 specifies this to be the address locations of the temporary memory into which the encrypted data is eventually written. Claim 1 of none of these requests, however, specifies how the "reordering" is meant to be carried out, nor is it disclosed in the description (see page 8, lines 3-11, and point 3.4 above). Also the appellant's explanation of the reordering is not disclosed - explicitly or implicitly - in the application (see the grounds of appeal, points 3.3.1.13 and 14).

6.3 The reordering feature, apparently and expressly central for the claimed invention, is therefore unclear and renders unclear the independent claims of the three highest-ranking requests, Article 84 EPC 1973. It can be left open whether it is also insufficiently disclosed and whether, therefore, the application additionally does not comply with Article 83 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