BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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 April 2013

Case Number: T 1669/10 - 3.5.06

Application Number: 07749562.0

Publication Number: 1991927

IPC: G06F 9/445

Language of the proceedings: EN

Title of invention:
PORTABLE DEVICE COMPRISING A BIOS SETTING

Applicant:
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.

Headword:
Portable token/HEWLETT-PACKARD

Relevant legal provisions:
EPC Art. 56, 84, 123(2)

Keyword:
"Original disclosure (yes)"
"Clarity (yes)"
"Inventive step (yes)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1669/10 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 19 April 2013

Appellant: (Applicant)
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.
Intellectual Property Administration
20555 S.H. 249
Houston TX 77070 (US)

Representative:
Schoppe, Fritz
Schoppe, Zimmermann, Stöckeler & Zinkler
Patentanwälte
Postfach 246
D-82043 Pullach bei München (DE)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 16 April 2010 refusing European patent application No. 07749562.0 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: D. H. Rees
Members: S. Krischer
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. The appeal is directed against the decision of the examining division, posted on 16 April 2010, to refuse the application 07749562 for lack of inventive step over documents:

D3 US 2003/0145191 A1, 31 July 2003,
D4 US 2002/0099934 A1, 25 July 2002,

and common general knowledge in the art.

II. A notice of appeal including a statement of the grounds was received on 28 June 2010. The fee was received the same day. Oral proceedings were requested.

III. In its summons to oral proceedings, the board gave its preliminary opinion that the arguments set out in the appealed decision (section 15) did not convincingly prove that claim 1 lacked an inventive step. However, the board raised clarity objections and required the description to be adapted.

IV. In a letter dated 12 April 2013, the appellant filed amended claims and description pages.

V. Oral proceedings were cancelled.

VI. The appellant *requests* that the decision be set aside and a patent be granted on the basis of claims 1-5 and description pages 3, 4 filed on 15 April 2013, description pages 1, 1a, 1b, 2, 5 filed on 18 February 2010 and drawing sheets 1, 2 as originally filed.

VII. Claim 1 of the sole request reads as follows:

"1. An electronic system (50), comprising:

a storage (58) holding a BIOS (60);

a token reader (64) for providing an interface between the electronic system and a portable token (70), wherein the portable token (70) comprises a predetermined signature and a non-volatile storage comprising a basic input/output system (BIOS) setting (72) to be applied from said portable token (72) onto the electronic system (50) to which the portable token (70) can be coupled; and

a user authentication device (57);

wherein following the begin (102) of a boot process the electronic system (50) is configured to

authenticate (104) a user by inputting a user-unique value into the electronic system (50) via the user authentication device (57) and by authenticating the user on the basis of the user-unique value;

determine (106), after successfully authenticating the user, if the portable token (70) comprising the BIOS setting (72) is installed in said electronic system (50);

authenticate said BIOS setting (72) to a user, said authenticating said BIOS setting (72) to a user comprising searching for a predetermined

signature on the portable token (70), wherein the signature includes a value that corresponds to the user-unique value that was used to authenticate the user; and

apply (108) said BIOS setting (72) from said potable [sic] token (70) onto said electronic system (50) if said predetermined signature is found on the portable token (70) and includes the value that corresponds to the user-unique value."

VIII. Claim 4 is a corresponding independent method claim.

Reasons for the Decision

1. *Original disclosure*

1.1 The examining division did not raise any objections under Article 123(2) EPC in its decision and the board concurs that there was no reason to do so with respect to the claims as refused.

1.2 The independent claims 1 and 4 of the present sole request have been amended somewhat with respect to the refused claims. The board finds that the amendments satisfy the requirements of Article 123(2) EPC:

- claim 1, paragraph 3: correction of a typing error ("an" -> "and");
- claim 1: the step of authenticating said BIOS setting (paragraph 8) was separated from the step of determining if a token is installed (paragraph 7) - see original description paragraph [11]; a

corresponding separation can be found in claim 4, paragraphs 5, 6;

- claim 1, paragraph 8/claim 4, paragraph 6: "searching the for the/a predetermined signature" was corrected by "searching for a predetermined signature" - see original description page 4, lines 8-10;
- claim 1, paragraph 9/claim 4, paragraph 7: "and includes the value that corresponds to the user-unique value" was added - see original description paragraphs [11], [12], especially original page 4, line 14.

1.3 As to the amendments of the description (paragraphs [10], [11]), the board also takes the view that they satisfy the requirements of Article 123(2) EPC, since they have simply been amended to specify that certain steps (e.g. the user authentication) are mandatory for the claimed invention, and not mere embodiments, as required to satisfy Article 84 EPC.

2. *Clarity*

The clarity objections (Article 84 EPC) raised in the board's summons to oral proceedings (5.1-5.3, 5.5-5.8) have all been overcome by the amendments filed on 15 April 2013 (see the preceding section).

3. *Inventiveness*

3.1 The application *relates* to an authenticated loading of BIOS settings from a "portable token" (e.g. smart card or USB memory stick, original description page 3, line 4) during booting a computer. This is useful if several users of the same computer each desire to have their own BIOS settings (page 1, lines 8, 9), or if a

single user, such as a network administrator, wants to boot up each of a number of computers with customised BIOS settings (page 5, lines 3-5). These settings of a user are stored on his personal token, together with a user-unique signature. The user puts his token in a token reader and initiates the booting, e.g. by pressing the power-on button (page 3, lines 19, 20). Then, the user has to authenticate himself, e.g. by inputting a password or his fingerprint (lines 26-32). After successful authentication, the computer searches for the signature on the token. If the signature found corresponds to the password (or fingerprint) entered by the user, then the BIOS settings on the token are considered authentic and are applied to the computer.

3.2 The appealed decision (section 15) argues that a combination of documents *D3, D4 and general knowledge* would lead to the subject-matter of claim 1.

3.3 The board agrees with the decision that D3 is well-suited to serve as the *closest prior art*, since it has the following features of claim 1 in common: A computer is booted with BIOS settings from a portable token (flash memory, [25], line 2) if the latter is available (abstract, [36]). Otherwise the BIOS settings are taken from the built-in BIOS ROM ([34]). The token in D3 also serves the same purpose as in the application ([3]: "... so that the system environment that a user desires can be applied to any other computer systems").

3.4 According to the appealed decision (15.2), claim 1 *differs* from D3 in that additionally the user and the BIOS settings are authenticated. The user is authenticated by entering a user-unique value (e.g. password or fingerprint). After successful user

authentication, the BIOS settings are authenticated by checking if the entered user-unique value corresponds to a signature on the token.

3.5 The objective technical *problem* relative to D3 was said (15.4) to be how to guarantee that a user will gain access to the valid BIOS settings for which he has been earlier authorised.

3.6 The grounds of appeal (page 3, last paragraph, line 8) propose a similar *problem*: to avoid the use of BIOS settings by users who are not authenticated to do so and to avoid a user who has managed to authenticate himself using non-authenticated BIOS settings. This is said to be for security reasons, since by using other BIOS settings during booting the user might get access to ports allowing him to transmit data from the computer which is not wanted for some (unspecified) reason.

3.7 As to the reasoning in the appealed decision, the board is unconvinced; D4 is situated in a quite different context and solves the problem in a different way to the present claim. The system described in D4 has an additional central server which stores the BIOS settings for several users. The solution that D4 proposes consists in using the token (a smart card; D4, [20]) for identifying or authenticating the user by the server, but not for storing the BIOS settings as in D3. The user does not have to enter a password, but only to install the smart card in the computer ([22]). The user ID is read from the smart card by the computer and transmitted to the server ([22]). Then, the server selects the BIOS settings for this user by a table lookup for the received user ID and transmits it to the

computer ([23]). There is no separate check that the user is authorised to use the BIOS settings, since the server is trusted.

3.8 In contrast to the appellant (page 5, paragraph 3) who interprets the entering of the smart card by the user and the transmission of the user ID to the server as a mere *identification*, the board does consider this to be user *authentication*, since an identification with a thing owned by a user is a well-known authentication technique. But the user authentications in D4 and in the claim are different: in D4 the user is authenticated by ownership (token), in the claim by knowledge (password) or inherence (fingerprint).

3.9 Applying the teaching of D4 to D3 could either mean adding a server to the scheme of D3, or applying the user authentication scheme and the BIOS setting selection of D4 to D3. The first possibility does not make sense for the problem posed. The second possibility (authentication using the user ID on the token followed by selection of BIOS settings among several ones of different users) would not lead to the claimed subject-matter; there would be no preliminary authentication of the user, independent of the token.

3.10 Thus, the board agrees with the appellant that a skilled person would not be motivated to combine D3 with D4, or at least would not do so in such a way as to arrive at the claimed subject-matter.

3.11 The decision further suggests that the claimed subject-matter is a mere juxtaposition of two known features. However in the board's view, the two authentication processes of current claim 1 are not so distinct and

separate as they are presented as in the decision. Therein, it is stated that "the combination of these two authentication processes does not involve a new, surprising effect" (page 7, paragraph 2, first sentence). The board disagrees.

3.12 The combination of the two authentication checks serves the common goal of preventing a known user who has been authenticated in the first check from using a token belonging to somebody else (see grounds of appeal, page 3, last paragraph). This prevention might be not only for organisational reasons but also for technical ones, as for example in order to improve the reliability and stability of the computer. For example a system administrator might forget his token in the reader and a technically less qualified employee might later boot the computer with the administrator's token still inserted. Without the second authentication, the employee might risk an accidental misuse of the possibly unexpected and unwanted capabilities he would have with the computer booted with the BIOS settings of the administrator.

3.13 Thus, the objective technical *problem* relative to D3 can be formulated as how to improve the reliability and stability of a computer which can be booted with the BIOS settings on a portable token.

3.14 None of the prior art documents at hand addresses this problem, nor does any of them prevent booting with BIOS setting on a token other than the user's own.

3.15 The board has considered the argument that it would be enough to carry out only the second authentication check to prevent a user from booting with the BIOS

settings of a different user. This is true, but the claimed invention has the further advantage that it would allow the use of a lower security level for the second check than for the first check, e.g. in merely storing on the token the user's login name as the "value that corresponds to the user-unique value", and not his password or fingerprint, since the password or fingerprint is already checked during the first authentication. This would also lessen the administration work when the user changes his password.

3.16 The board concludes that claim 1 is inventive in the sense of Article 56 EPC.

3.17 All the essential features of system claim 1 have corresponding features in independent method claim 4. Therefore, claim 4 is also inventive in the sense of Article 56 EPC.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent on the basis of claims 1-5 and description pages 3, 4 filed on 15 April 2013, description pages 1, 1a, 1b, 2, 5 filed on 18 February 2010 and drawing sheets 1, 2 as originally filed.

The Registrar: The Chairman:

B. Atienza Vivancos D. H. Rees