Internal distribution code:

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

Datasheet for the decision of 17 December 2015

Case Number:	T 2558/12 - 3.5.06
Application Number:	06019603.7
Publication Number:	1777636
IPC:	G06F21/00
Language of the proceedings:	EN

Title of invention:
A digital certificate that indicates a parameter of an associated cryptographic token

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

Headword:
Trust in a cryptographic token/HEWLETT-PACKARD

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step (no)

Decisions cited:
T 0641/00

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

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 2558/12 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 17 December 2015

Appellant:
(Applicant)

HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.
20555 S.H. 249
Houston, TX 77070 (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 8 October 2012 refusing European patent application No. 06019603.7 pursuant to Article 97(2) EPC.

Composition of the Board:

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

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dated 8 October 2012, to refuse European patent application No. 06 019 603.7 for lack of inventive step over the document

D1: WO 01/06727 A2.

II. On 29 November 2012, a notice of appeal and a statement of grounds were received and the appeal fee was paid. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the application documents on file, which at the time were:

description pages 1-19 as originally filed,
description page 1a as filed on 18 October 2007,
claims 1-10 as filed on 12 June 2012, and
drawing sheets 1/4-4/4 as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claims *inter alia* lacked inventive step over D1, Article 56 EPC 1973.

IV. In response to the summons, with letter dated 17 November 2015, the appellant filed amended claims 1-10, 1-8 and 1-4 according to a main request and two auxiliary requests, respectively, and argued in their favour, but indicated that no one would be attending the oral proceedings.

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

"A method for determining by a challenger (220) a level of trust to put in a digital certificate (150, 300), the challenger (220) allowing/disallowing a trusted action dependent from a predefined level of trust, the method comprising:

storing the digital certificate (150) and a user private key (116) by a user computer (102) in a way to be accessible via a cryptographic service module (110) coupled to a cryptographic token (112), wherein the digital certificate (150, 300) comprises a signed public key (152) and signed token information (154) for the cryptographic token (112), and wherein the signed token information (154) comprises physical and operative parameters of the cryptographic token (112);

obtaining, by the challenger (220), the digital certificate (150, 300);

performing, by the challenger (220), a signature verification for the digital certificate (150, 300);

determining a level of trust with the digital certificate (150; 300) based on the physical and operative parameters (304-310) of the cryptographic token (112), the level of trust being determined independently from the signature verification; and

performing an action based on the determined level of trust, wherein, in case the level of trust is greater than a threshold amount, the action is allowed, and wherein, in case the level of trust is less than a threshold amount, the action is limited in scope or not allowed."

VI. Claim 1 of the first auxiliary request differs from claim 1 of the main request in that the following is added at its end:

"... wherein the physical and operative parameters of the cryptographic token (112) are selected from the group consisting of:

- whether the cryptographic token (112) is a hardware token;
- whether the cryptographic token (112) is a software token;
- whether the cryptographic token (112) is a firmware token;
- at least one platform configuration register (PCR) value;
- whether an associated private key is encrypted using the cryptographic token (112);
- whether an associated private key (116) is stored externally to an associated platform (102);
- whether an associated private key (116) is stored internally to an associated platform (102);
- cryptographic operations that are supported by the cryptographic token (112);
- cryptographic key lengths that are supported by the cryptographic token (112);
- a token identification number;
- a token name;
- a token alias;
- a standard related to the cryptographic token (112);
- whether an associated private key (116) is migrate-able;
- whether the token (112) is soldered to an associated platform (102);

- whether the token (112) in removeably [sic] coupled to an associated platform (102);
- a Common Criteria Evaluation Assurance Level (CC EAL);
- a platform certificate uniform resource location (URL);
- a manufacturer of the cryptographic token (112); and
- a manufacturer of a computer system (102) that implements the cryptographic token (112)."

VII. The main and the first auxiliary requests also comprise an independent claim for a storage medium storing a digital certificate which is defined in words broadly corresponding to those of the corresponding method claim 1. For the purpose of this decision, these claims are immaterial. The second auxiliary request is identical to the first auxiliary request with the storage medium claims 5 to 8 discarded.

VIII. Oral proceedings were held on 17 December 2015 as scheduled and, as announced, in the absence of the appellant. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. In general terms, the application is concerned with establishing whether a user is authorised to perform a specific "trusted transaction or trusted communication" and, if so, allowing the transaction or communication (henceforth referred to as "action").

1.1 It is disclosed that a user, requesting a computer application to perform some action, will present a digital certificate (e.g. based on the X.509 standard) which contains, *inter alia*, the user's public key signed by a certificate authority (paragraphs 1 and 23). The user will also present what is called a "cryptographic service module" CSM and/or a "cryptographic token" which "performs the cryptography" (paragraph 2). The requested computer application will determine its trust in the cryptographic token, for instance using a challenge-response dialogue (hence the computer application is also referred to as the "challenger application").

1.2 The term "cryptographic token" is used to refer broadly to a variety of security mechanisms available "to safeguard access to a private key" (see paragraph 25), based on hardware, software or firmware. These cryptographic tokens are characterised by their "physical parameters", such as token type, or "operative parameters", such as supported cryptographic operations or key length (see paragraph 26).

1.3 It is disclosed that these parameters may have a bearing on "the ability of the cryptographic token to protect private keys or other secrets", and hence their "security" or the "trust" that can be put into them (paragraphs 25 and 26). The application is concerned with the problem of how to "establish trust" towards a user and its cryptographic token.

2. As a solution, the application proposes to store security-relevant parameters of the cryptographic token in the digital certificate (preferably in extension fields provided by version 3 of the X.509 standard; see paragraphs 10 and 12), cryptographically signed, and to

communicate them with the certificate to the challenger application, so that it can determine its trust in the cryptographic token (see e.g. paragraph 29). In doing this, "different challenger applications [may be] free to interpret the physical and/or operative parameters independently" (paragraph 33). Depending on the determined level of trust, the challenger application may allow the user to perform the requested action, fully or in limited form, or disallow it (see e.g. paragraphs 46 and 55).

Terminological issues and claim construction

3. Claim 1 of all requests is directed to a "method for determining by a challenger a level of trust to put in a digital certificate", which is stored "in a way to be accessible via a cryptographic service module (110) coupled to a cryptographic token". Claim 1 further specifies that the digital certificate comprises "physical and operative parameters of the cryptographic token".

3.1 The board notes that this wording *refers* to a cryptographic service module and a cryptographic token, but that neither is actually *part* (i.e. feature or object) of the claimed method. In this regard, the board disagrees with the appellant's statement made in its reply dated 17 November 2015 (see page 2, last paragraph).

3.2 The board also observes that a digital certificate may be accessible "via" more than one cryptographic service module or cryptographic token so that it is unclear which is "the" specific cryptographic token the parameters of which are recited in the claim.

3.3 Furthermore, claim 1 does not require that the recited parameters are obtained or derived from the cryptographic token, nor that they are or could be validated against it. As a consequence, the parameters may or may not be an accurate characterisation of the token in question, and, hence, any conclusion drawn from these parameters may or may not be reliable.

3.4 Moreover, the term "level of trust" is a vague one. The method specifies the "level of trust" as a value used to control access to an action but does not otherwise give meaning to the concept of "trust". The board takes it that "trust" is a matter of convention, based on unilateral "interpretation" by the challenger application (see also paragraph 33 of the description) or based on "agreement" between the relevant parties. Either way, the notion of "trust" does not have any specific *technical* meaning.

4. The foregoing notwithstanding, the board considers that the claimed subject-matter is clear enough to be assessed for inventive step, Article 56 EPC 1973.

The prior art

5. D1 relates to computer security based on a PKI architecture and discloses digital certificates comprising a user's identity and the user's public key, "bound" together by a digital signature of the certification authority CA (page 1, line 31, to page 2, line 13). The certificate is evaluated to determine "whether or not to trust a user's signature" (*loc. cit.*) and thus whether a requested transaction is allowed or not (page 2, lines 14-18). D1 further discloses that an X.509 certificate (version 2, see page 3, line 8) may be extended by "policy elements" or "policy identifiers" (page 3, lines 7-31), which define for instance key sizes, whether a customer must appear personally before an autho-

rity or how customers have to identify themselves. It is disclosed that there are "mandatory requirements" such as (certificate) validity, whereas the certificate policy extension contains "discretionary requirements" (page 11, line 17; page 13, lines 26-32). The latter can be enforced at need by the Programmable Policy Module (PPM) (*loc. cit.*; page 5, last paragraph; page 11, lines 17-32; page 18, lines 6-8; claim 13).

Inventive step

6. In the board's view, the PPM of D1 qualifies as a "challenger" according to the claimed invention which allows/disallows a trusted action based on "parameters" contained in a digital certificate. The board also considers that the PPM only allows an action if it has established a sufficient "level of trust" in the given certificate (see page 1, line 32, to page 2, line 2). In the board's judgment, at least some of the policy elements disclosed in D1 qualify as "operative parameters of the cryptographic token" (in particular the "key size", "key algorithm" and "key usage algorithm"; see D1, page 3, lines 7-21, and page 11, line 31; and compare the application, paragraph 26).

7. Claim 1 of the main request thus differs from D1 in the following features:

   a) D1 does not disclose that the challenger allows or disallows an action according to whether the determined "level of trust" is greater or less than a given threshold.

   b) D1 arguably does not disclose that the digital certificate contains "physical parameters [...] of the cryptographic token", certainly not as defined in the description in paragraph 25.

c) D1 does not disclose that the "token information" contained in the licence is cryptographically signed.

Claim 1 of the auxiliary requests further differs from D1 in the claimed alternatives from which the "physical and operative parameters" of the cryptographic token are to be selected.

7.1 The appellant argues that the invention solves the problem of "provid[ing] an improved approach for determining the level of trust in a digital certificate" (see grounds of appeal, page 5, paragraph 3).

7.2 The board considers that this formulation is unsuitable for defining the objective technical problem solved by the invention, firstly because, as argued above, the concept of "trust" has no clear, if any, technical meaning, secondly because the level of trust is not "determined" in a technical sense, and, thirdly and foremost, because it is not clear in what manner the invention "improves" the way of "determining the level of trust".

7.3 The board rather takes the view that the three differences address three separate and independent problems. Feature a) concerns the question of how the policy enforcement known from D1 is implemented, feature b) the question of which parameters may affect "trust", and feature c) the question of ensuring the integrity of the policy-relevant information itself.

8. Regarding difference c), the board considers that digital signatures are an obvious solution to the given problem. It is known from D1 to sign the user's identity with the user's public key so as to enable verification that a public key belongs to the asserted user. The board deems natural the desire to validate the token information in the same way, so as to make sure that the policy enforcement cannot be bypassed by forging the token information. To this end, the skilled person would find it obvious to provide a digital signature of the token information, too.

9. Regarding difference a), the board considers that the use of thresholding is an obvious way of arriving at a binary decision. For example, if keys were trusted the more the longer they are, the "trust level" associated with a key would be effectively the key length. If, then, a policy requirement was a minimum key length (see D1, page 3, lines 14-15) it would be obvious for the skilled person to evaluate whether the key length exceeded the minimum length threshold and allow or disallow the requested action accordingly.

10. By way of difference b), the invention proposes a policy - or, rather, a set of policy criteria - different from those disclosed in D1.

10.1 The board agrees with the examining division that the choice of policy may be a matter of agreement between "the two parties" (see decision, reasons 4.4), although it may also be a unilateral decision of the challenger (as disclosed in the application, paragraph 33). The board also agrees with the decision that the choice of policy, in itself, does not contribute to the technical character of the invention.

10.2 If one were to introduce the policy that a certain action should only be carried out with a particular kind of tamper-resistant token, then this choice itself would not solve a technical problem. In particular, the security advantage of tamper resistance is achieved by the token rather than the policy decision to require it. Coming up with a new policy thus does not solve a technical problem but expresses the wish to exploit a known advantage.

10.3 It is noted in passing that a policy need not imply any specific technical advantage. For instance, if one were to decide that only cryptographic tokens of a particular manufacturer were to be trusted (as listed in claim 1 of the auxiliary requests), then this might in itself express some form of "trust" in that manufacturer but leaves open what technical properties it might have to guarantee so as to earn and maintain that trust.

10.4 For the foregoing reasons, established jurisprudence of the boards of appeal (in particular T 641/00 COMVIK; headnote 2) provides that the details of the chosen policy may legitimately appear in the formulation of the problem to be solved rather than the solution. For claim 1 this would be the problem of modifying D1 so as to take into account "physical parameters of the cryptographic token" (main request) or "physical and operative parameters [...] selected from the group" as defined in claim 1 (auxiliary requests).

10.5 Given that D1 already discloses the definition of policies in certificates and their enforcement by the challenger, it would be obvious for the skilled person to modify D1 so as to take into account other or additional policy parameters.

10.6 Therefore, the board comes to the conclusion that claim 1 of all three pending requests lacks an inventive step over D1, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated