Internal distribution code:

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

Datasheet for the decision of 9 January 2018

Case Number: T 1307/15 - 3.5.06

Application Number: 10186372.8

Publication Number: 2333689

IPC: G06F21/00, H04L9/32, H04L12/24, H04L29/08, H04L29/06

Language of the proceedings: EN

Title of invention:
Apparatus and methods for protecting network resources

Applicant:
PowerCloud Systems, Inc.

Headword:
Replacement certificates/POWERCLOUD

Relevant legal provisions:
EPC Art. 56, 84

Keyword:
Claims - clarity (no)
Inventive step (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 1307/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 January 2018

Appellant: (Applicant)	PowerCloud Systems, Inc. 3333 Coyote Hill Road Palo Alto, CA 94304 (US)
Representative:	Gill Jennings & Every LLP The Broadgate Tower 20 Primrose Street London EC2A 2ES (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 3 February 2015 refusing European patent application No. 10186372.8 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 is against the decision of the examining division, with reasons dispatched on 3 February 2015, to refuse European patent application No. 10 186 372.8 for lack of inventive step over

D2: US 2005/069136 A1 and
D7: Adams C *et al.*, "Understanding Public-key Cryptography; Concepts, Standards and Deployment Considerations", Macmillan Technical Publishing, excerpt comprising pages 2-72 and 188-197, 1999.

II. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1-15 according to a main or one of five auxiliary requests as filed with the grounds of appeal, in combination with the application documents on file.

III. In the annex to the summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step over the prior art on file, Article 56 EPC. Objections under Articles 83, 84 and 123(2) EPC were also raised.

IV. In response to the summons, by a letter dated 8 December 2017, the appellant filed amended claims 1-10 according to a new main request and withdrew all auxiliary requests.

V. Independent claims 1 and 7 read as follows:

"1. A method of protecting network resources of an organization, the method comprising:
maintaining (200) a root certificate (150) of a first cryptographic infrastructure;

maintaining (200) a root certificate (170a) of a second cryptographic infrastructure associated with the organization;

issuing (204), to each client device enabler (120) of a plurality of client device enablers configured to provision client computing devices (132) in communication with a network associated with the organization, an initial client certificate (158) within the first cryptographic infrastructure;

issuing (202), to each authenticator of a plurality of authenticators (130a-m) within the network associated with the organization, an initial intermediate Certificate Authority, CA, certificate (172a) within the second cryptographic infrastructure;

after mutual authentication of a first client device enabler (120) of the plurality of client device enablers with a first authenticator of the plurality of authenticators (130a-m) using a first initial client certificate (158) corresponding to the first client device enabler, configuring (212), by the first client device enabler, a first client computing device for operation within the network associated with the organization;

receiving (222), from the first authenticator, a request for a replacement intermediate CA certificate responsive to the first authenticator issuing (218) to the first client computing device (132) a client certificate (176a) within the second cryptographic infrastructure using the initial intermediate CA certificate;

issuing (222), to the first authenticator, the replacement intermediate CA certificate within the second cryptographic infrastructure to the given authenticator responsive to receiving the request;

issuing (222), to the first client device enabler (120), a replacement client certificate within the first cryptographic infrastructure; and

after mutual authentication of the first client device enabler (120) with the first authenticator using the replacement client certificate, configuring (212), by the first client device enabler (120), a second client computing device for operation within the network associated with the organization.

7. A system comprising:

a plurality of authenticators (130a-m) within a network associated with an organization;

a plurality of client device enablers configured to provision client computing devices (132) in communication with the network associated with the organization; and

a server (110) adapted to store a root certificate (150) of a first cryptographic infrastructure and a root certificate (170a) of a second cryptographic infrastructure associated with the organization, the server configured to:

issue (204), to each client device enabler (120) of the plurality of client device enablers, an initial client certificate (158) within the first cryptographic infrastructure, wherein, after mutual authentication of a first client device enabler (120) of the plurality of client device enablers with a first authenticator of the plurality of authenticators (130am) using a first initial client certificate (158) corresponding to the first client device enabler, the first client device enabler configures (212) a first client computing device for operation within the network associated with the organization;

issue (202), to each authenticator of the plurality of authenticators (130a-m) within the network

associated with the organization, an initial intermediate Certificate Authority, CA, certificate within the second cryptographic infrastructure;

receive (222), from the first authenticator of the plurality of authenticators (130am), a request for a replacement intermediate CA certificate responsive to the first authenticator issuing (218) the first client computing device (132) a client certificate (176a) within the second cryptographic infrastructure using the initial intermediate CA certificate;

issue (222), to the first authenticator, the replacement intermediate CA certificate within the second cryptographic infrastructure responsive to receiving the request;

issue (222), to the first client device enabler (120), a replacement client certificate within the first cryptographic infrastructure, wherein, after mutual authentication of the first client device enabler (120) with the first authenticator using the replacement client certificate, the first client device enabler (120) configures (212) a second client computing device for operation within the network associated with the organization."

VI. By letter dated 3 January 2018, the appellant informed the board that it did not intend to attend the scheduled oral proceedings, which were thus held in its absence.

VII. At the end of those proceedings, the chairman announced the board's decision.

Reasons for the Decision

Decision in the appellant's absence

1. The appellant was duly summoned, but did not appear at the oral proceedings, which were thus held without it, Rule 115(2) EPC. Under Article 15(3) RPBA, the board is not obliged to delay any step in the proceedings, including its decision, by reason only of the appellant's absence at the oral proceedings and will treat it as relying only on its written case.

The invention

2. The application is concerned with protecting an organization's networked resources against unauthorized access by client devices (see figure 1, numbers 132 and 140; description, page 1, paragraph 1). More specifically, the application relates to the initial authorization of new client devices (this is called "provisioning"; see paragraph 6) and the potential withdrawal of authorizations should an involved device be "lost, stolen", "otherwise missing" or "compromised" (see paragraphs 14 and 15).

2.1 In the architecture being considered, client devices request access to an organization's network via one of several "access points" (see figure 1, numbers 130a-130m) or other "authenticators" (see paragraphs 28 and 29). The access is then controlled by interaction between the authenticator and a "client device enabler (CDE)", a piece of hardware connected to, or software running on, the client device (see paragraphs 30 and 35, and figure 1, number 120).

2.2 The application discloses the use of several separate public key infrastructures (PKIs), all rooted in the same server (see figure 1, number 110, and paragraphs 37 to 39). A "global" PKI is employed for provisioning all devices involved in the access control - especially the authenticators and the CDEs - before it is known what organizations they will be used by (see figure 1, number 150, and paragraphs 9, 41, 44, 45 and 48). In addition, a "per-organization" PKI is provided to protect the network of each individual organization (A to N; see paragraphs 11 and 77). These are claimed, respectively, as "first" and "second cryptographic infrastructure[s]".

2.3 When a client is to be "provisioned" for use in an organization's network, the authenticator and the corresponding CDE mutually authenticate each other using certificates issued under the global PKI (see paragraphs 22, 41 and 48; see figure 1, numbers 154, 156 and 158; and figure 2, numbers 202, 204 and 214). If that is successful, the authenticator will use an organization-specific "intermediate CA certificate" to generate an organization-specific certificate for the client (see paragraph 23, and figure 1, number 172a, and figure 2, number 218).

2.4 The application mentions that both the authenticator's intermediate CA certificate and the provisioning CDE's "global" certificate are replaced or updated "after use" (paragraphs 15 and 89). This is meant to simplify "corrective action" if "an authenticator or CDE is lost, stolen or compromised" (see paragraph 15). It is said to be sufficient in such a case to remove devices (or certificates) from a whitelist and move them to a blacklist to prevent the client from accessing the

protected network (see paragraphs 14, 15, 52-56, and 72).

Article 123(2) EPC

3. The objection under Article 123(2) EPC raised in the summons (see point 3) has become irrelevant because the feature it related to (certificates with "limited" or "predetermined number of uses") is not contained in present claims 1-10.

Article 83 EPC

4. The objection under Article 83 EPC raised in the summons (see point 5) related to the question of how client certificates are validated or invalidated by means of whitelists and blacklists. As neither the invalidation of certificates nor the use of whitelists or blacklists is now claimed, this issue has become irrelevant, too.

Clarity, Article 84 EPC, and claim construction

5. It is not explicitly claimed in claim 1 which device is to carry out the "maintaining" and "issuing" steps. More specifically, claim 1 refers to a mutual authentication between a "client device enabler" and an "authenticator", and specifies that the "first client device enabler" "configur[es] a first client computing device", but leaves open whether the maintaining and issuing steps are carried out by one of the mentioned devices or by another one. This renders claim 1 unclear, Article 84 EPC. However, in view of system claim 7 it is clear that the intended meaning is for

the server to carry out both steps. The board will adopt this interpretation in this decision.

6. The method of claim 1 specifies steps of "configuring (212)" a "first" and "a second client device for operation within the network of [an] organization" to take place "after mutual authentication" of a "first client device enabler" and a "first authenticator". The use of the preposition "after" raises the question whether or not the mutual authentication step is meant to be part of the claimed method. This renders claim 1 unclear, Article 84 EPC.

6.1 Likewise, system claim 7 specifies that the "server" is configured to issue certificates to each client device enabler, "wherein, after mutual authentication", the "first client device enabler configures [...] a first client computing device". Given that system claim 7 only specifies the server carrying out any steps, it is unclear whether or not the "wherein" clauses are meant to limit the devices involved in the mutual authentication. Claim 7 is thus unclear, too.

6.2 The board notes that the method of claim 1 is already spread over at least two devices, the claimed steps of "maintaining" and "issuing" certificates being carried out by the server and the steps of "configuring" by the "first client device enabler", so it would seem logical to assume that the mutual authentication, carried out by the first client device enabler and a first authenticator, is also meant to be claimed. The same applies, *mutatis mutandis*, to system claim 7.

6.3 In the following, the board will therefore interpret claims 1 and 7 as implying that the mutual authentication is part of the claimed invention.

7. Both independent claims refer to "replacement" certificates.

7.1 It is clear that the replacement certificates are meant to "replace" earlier certificates at the authenticator or CDE in question, in particular so that the replacement certificate is used in the process of configuring the second client computing device (see the appellant's letter of 8 December 2017, page 2, penultimate paragraph). However, this does not mean that a client certificate issued "using" an earlier "intermediate CA certificate" becomes invalid, let alone make clear what consequence such an invalidation might have.

7.2 Moreover, the claims do not exclude the possibility that the earlier certificates can be used more than once. In any event, they fail to specify the delay between the request for and the issuance of replacement certificates and do not prohibit the use of the earlier certificate in the meantime.

8. The board also notes that the invention covers only one replacement of *initial* certificates by *replacement* certificates, rather than, as apparently intended, the repeated replacement of issued certificates on request and after use. Again, the board will, for the appellant's benefit, interpret the claims according to their intended meaning.

The prior art

9. D2 relates to the management of PKI architectures and certificates (see e.g. abstract and paragraph 67). It is disclosed that, based on a "root certificate", "intermediate root certificates" with a shorter period

of validity can be issued and possibly renewed (paragraphs 111, 117 and 124). An architecture with two "certification authorities" (CAs) is disclosed, one "internal" to an enterprise and one "external" to it (see figure 5, numbers 60 and 61, and paragraphs 138 and 139). It is disclosed that the internal CA holds "intermediate root certificates" used for the local issuance of new certificates (*loc. cit.*).

10. D7 discloses background information on PKIs. Among other things, it mentions (page 35, paragraph 3) that the validity of certificates may be so short that they are effectively single-use certificates. At the same time, it states that short validity is impractical since it causes a tremendous load on the certification authority.

Inventive step

11. The decision under appeal found that the then claimed invention differed from D2 in that "each time a given authenticator issues [...] a client certificate [...], [it] requests [...] and is [...] issued [...] a replacement intermediate CA certificate" (see reasons 14.2 and 14.3). However, the claims were "silent with respect to what happens [...] when an intermediate CA certificate is being 'replaced'" and, in particular, as to whether "the private key corresponding to the replaced intermediate CA certificate is deleted or prevented from being used" or whether "the replaced intermediate CA certificate is actually revoked" (see reasons 14.6). Thus, the claims covered the possibility that "multiple intermediate certificates" were "simultaneously valid", which caused "an increased load on the authenticator without clearly

derivable benefits", so that the distinguishing features did not make an inventive contribution to the prior art, and especially not to D2 (see reasons 14.7).

12. The appellant gave a similar summary of the decision under appeal (see the grounds of appeal, especially points 15 to 19, but also 26, 30 and 32). In particular its arguments in favour of the claimed invention in the grounds of appeal were limited to the issue of whether the established distinguishing feature - in a nutshell: the repeated issuance of replacement certificates - had a technical effect and was non-obvious over the available prior art (see especially points 26, 30, 32, 37, 41 to 43, 49 and 63).

13. Present claims 1 and 7 now specify the issuance of two replacement certificates: apart from the replacement intermediate CA certificate issued within the "second cryptographic infrastructure", as already claimed before, a replacement client certificate is issued within the "first cryptographic infrastructure".

14. In its letter of 8 December 2017, the appellant stated that "the revocation of certificates should be an extremely rare event" which might "never happen in the entire life cycle of an individual authenticator or client device enabler" and that it would therefore be "an unfair characterisation of the invention to limit it to the rare circumstances in which certificates are actually revoked" (appellant's letter of 8 December 2017, page 3, penultimate paragraph). The claimed features "provide the effect of limiting the impact of a compromised authenticator (or client device enabler)" by "improv[ing] the ability of an administrator to invalidate client certificates generated after an

authenticator or client device enabler has been lost, stolen or otherwise compromised" (see *loc. cit.*, and the grounds of appeal, point 41).

15. The board appreciates that the replacement of a certificate will not cause its revocation or the revocation of any client certificate issued on its basis, but that, rather, certificates may be revoked only "in the rare event" that a device has been "lost, stolen, or otherwise compromised". Hence, the board accepts that the invention need not be limited to that rare event actually taking place.

15.1 At the same time, for it to be possible to argue, as the appellant does, that the invention provides protection against precisely such a rare event, the invention must be *capable of addressing* it if and when it is detected or reported.

15.2 However, the claims not only fail to specify what happens in the case of a security breach, which means their subject-matter is not capable of addressing such a breach, but also do not specify any means that would enable the administrator to do so.

15.3 The description states that the "number of client certificates issued under each" CDE client certificate and authenticator intermediate CA certificate "is minimized" so that "the impact of revoking or blacklisting them is minimized" (see paragraph 15). It is not claimed, however, how this effect is achieved.

15.4 One possibility seems to be that the administrator is able to identify which client certificates were issued after a security breach, so that only those ones would have to be "blacklisted" (in addition, apparently, to

the latest certificate issued to the compromised CDE or authenticator itself). The claimed-subject matter does not, however, contain a feature that would enable the administrator to do this. In particular, the claims do not specify that the client certificates (or, in fact, any certificates) are time-stamped.

15.5 An alternative possibility might be that a compromised authenticator can only issue a single client certificate and will not be issued with a replacement intermediate CA certificate when requesting one. This might limit the impact of the security breach to a single instance, rather than there being a potentially unlimited number, even without any blacklisting. However, again, the claimed subject-matter does not contain any feature that would support this interpretation. Neither does the claim guarantee that any certificate is used only once (see point 7 above), nor does it imply that a compromised authenticator might not be issued with a replacement certificate.

16. The board therefore concludes that the distinguishing feature in question (see points 10 and 11), the repeated request for and issuance of replacement certificates cannot, on its own, be accepted as having the alleged "technical advantage" of "improving resistance to security breaches" (see the appellant's letter of 8 December 2017, page 3, penultimate paragraph). Moreover, the mere *potential* to improve a system's resistance to security breaches, in particular where it may rely on a *person* (an administrator) invalidating certificates, is not a technical effect.

17. Also, the board considers that the repeated re-issuance of certificates in the claimed invention is an obvious implementation of the known practice of issuing short-

term certificates (e.g., see D7, page 35, paragraph 3). The additionally claimed fact that new certificates are *requested and eventually issued after use* does not, *per se*, have any non-trivial technical effect on the claimed invention, but must be considered to be an obvious alternative implementation of (known) short-time certificates.

18. The board concludes that the only distinguishing feature in question must be considered to lack inventive step over the prior art D2 and D7, Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated