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 February 2015

Case Number: T 1670/10 - 3.5.06

Application Number: 05105665.3

Publication Number: 1610202

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Using a portable security token to facilitate public key certification for devices in a network

Applicant:
Palo Alto Research Center Incorporated

Headword:
Portable security token/PALO ALTO RESEARCH

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (yes)

Decisions cited:

Catchword:

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 1670/10 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 February 2015

Appellant: (Applicant)	Palo Alto Research Center Incorporated 3333 Coyote Hill Road Palo Alto, California 94304 (US)
Representative:	Grünecker, Kinkeldey, Stockmair & Schwanhäusser Anwaltssozietät Leopoldstrasse 4 80802 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 1 February 2010 refusing European patent application No. 05105665.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	M. Müller

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 1 February 2010, to refuse European patent application No. 05 105 665.3 on the basis that the subject-matter of claim 1 according to the main and first to third auxiliary requests did not involve an inventive step, Article 56 EPC, in view of the disclosure of the following document:

D1: US 6 601 171 B1

and the common general knowledge of the skilled person.

II. With a notice of appeal, received on 31 March 2010, the appellant filed sets of claims according to a main and first to third auxiliary requests which were the same as the claims upon which the appealed decision was based. The appellant requested that the decision be set aside and that a European patent be granted on the basis of the sets of claims according to said main and first to third auxiliary requests and the description and figures on file. The appellant also made a conditional request for oral proceedings. The appeal fee was paid on the same day.

III. In a statement of grounds of appeal, received on 11 June 2010, the appellant maintained its requests made in the notice of appeal, but only presented arguments regarding the patentability of the main request, offering to comment on the patentability of the auxiliary requests if the need arose.

IV. The application is thus being considered in the following form:

Description (all requests):
pages 1 to 18, as originally filed.
page 2a, received on 14 November 2007.

Claims (all received on 31 March 2010 and being the same as the claims upon which the decision was based):
Main request: 1 to 10
First auxiliary request: 1 to 9
Second auxiliary request: 1 to 8
Third auxiliary request: 1 to 6.

Drawings (all requests):
Pages 1/3 to 3/3.

V. Claim 1 according to the main request reads as follows:

"A method for using a portable security token (102) to facilitate public key certification for a target device (104) in a network, comprising:
bringing the portable security token in close physical proximity to the target device, thereby allowing the portable security token to communicate with the target device through a location-limited communication channel;
receiving an authenticator for the target device at the portable security token through the location-limited communication channel, wherein the authenticator is a cryptographic token that can be used in a subsequent protocol between the target device and a certification authority (CA) to prove that the cryptographic token originated from the target device;
forming a ticket by digitally signing the authenticator with a key previously agreed upon by the portable security token and the CA (106); and sending the ticket to the target device, whereby the target device can

subsequently present the ticket to the CA to prove that the target device is authorized to receive a credential from the CA."

The text of the claims according to the lower ranking requests is immaterial to this decision.

Reasons for the Decision

1. The admissibility of the appeal

The appeal fulfils the admissibility criteria under the EPC and is consequently admissible.

2. Technical summary of the invention

2.1 The application relates to certifying public encryption keys of devices in a distributed computing network. It is known to use a public key infrastructure (PKI) to solve this problem by using a "Certification Authority" (CA). The CA owns a trusted public key. The corresponding private key of the CA is used to sign the public keys of members of the network to form digital public key certificates, for instance by encrypting their hash. Hence the public key of the CA can be used by other members to verify the authenticity of the public key of a member contained in such a certificate. According to the application, establishing a fully-fledged PKI may be prohibitively costly and difficult in wireless networks.

2.2 The application therefore proposes a mechanism for distributing certificates which can be practiced in wireless networks. Figure 1 shows such a distributed computing network comprising a target device (such as a television), a portable security token (such as a cell

phone or smart card) and a certification authority (such as a wireless access point comprising a CA and an authentication server). The target device can communicate wirelessly with the token and the certification authority. The portable security token is used to facilitate public key certification for the target device in the network. In use, the token must be brought into "close physical proximity" with the target device to allow the two to communicate via a so-called "location-limited communication channel"; see the flow charts in figures 2 to 4. Examples of such communication channels ranging from a wireless connection to a wired connection are set out in paragraph [0040]. During this communication, the token receives an "authenticator" for the target device and forms a "ticket" by digitally signing the authenticator with a key previously agreed upon by the token and the CA. The authenticator is a token which the CA knows is linked to the target device, such as the target device's public key. The token sends the ticket to the target device which can then present the ticket to the CA to prove that the target device is authorized to receive a credential from the CA, for instance a digital certificate for the target device's public key.

3. Document D1

3.1 D1, the closest prior art relied upon in the decision, relates to the delegation of rights (also referred to as "permissions") in a distributed computing system; see column 3, line 7, to column 4, line 53. This involves a principal delegating specific rights to one or more deputies who themselves can delegate specific rights to further deputies in a chain of delegations. The deputization approach to delegating rights does not require that an entity impersonate another; instead,

actions taken by a principal and actions taken by its deputy can be distinguished; see column 5, lines 33 to 45. The entities in these deputization are represented by computing system tasks, such as the "user task" and "deputy system task" in figure 2. The distributed computing system comprises one or more Distributed Deputization Points (DDPs) which manage such deputizations.

3.2 Figure 2 shows the data flows occurring during deputization; see column 7, line 38, to column 9, line 17. The user first logs into the computer system by exchanging login information with a server which then acts as a "principal node" 206, i.e. a node representing the principal, i.e. one who delegates rights. A "user task" on the principal node represents the principal for delegation purposes; see column 7, lines 50 to 51. Other tasks created by software such as operating systems and application programs running on the system can act as principals; see column 7, lines 51 to 54, and column 8, lines 17 to 21. The user task sends an authentication request 212 identifying the principal to the DDP and optionally containing a credential that the principal is entitled to use that user name; see figure 2; 212. If the DDP accepts the principal as legitimate, it returns an authentication response 214 to the user task containing an indication that the principal is authenticated.

3.3 Once authenticated by the DDP, a user task, deputy (system task) or application (system task) running on the principal node (see column 8, lines 21 to 26) can send a deputy credential request 220 to the DDP, the request possibly containing the public key of the proposed deputy or identifying the deputy so that the DPP can request the deputy's public key from a

repository such as a certification authority; see column 8, lines 36 to 38. The request may also contain the public key of the proposed deputy encrypted with the principal's public key. In response to the deputy credential request 220, the DDP issues a deputy credential response 222 to the principal comprising a deputy credential containing *inter alia* the principal's identity, the delegated rights/permissions, the deputy's private key encrypted with the principal's public key, a deputy certificate and the DDP's digital signature; see figure 6, column 9, line 66, to column 10, line 58, and column 10, lines 50 to 58.

3.4 According to column 8, lines 21 to 23, a deputy may act as a principal to create its own deputy; see figure 5 and column 9, lines 47 to 57. Hence the board agrees with the appellant that this is why figure 2 shows "Deputy (system task) 216" as a possible principal (node) in addition to "User task 208" and "Application (system task) 218". As the appellant has pointed out, in D1 the entity communicating with the DPP is always a principal (node, see 206 in figure 2). A principal could delegate rights to a deputy who, in turn, could further delegate these rights; see figure 5 and column 9, lines 47 to 57. However, in doing so, the deputy acts as a principal rather than as a deputy. Hence the board accepts the appellant's argument that figure 2 does not disclose communication between the DDP and the deputy.

3.5 The embodiment shown in figure 8, like that shown in figure 2, involves an authentication request 212 and response 214 to authenticate a principal - referred to in figure 8 as the "requester" - to a DDP (step 800); see column 11, lines 33 to 37. The requester then sends a "request for rights delegation" 802 including *inter*

alia the identity of the requester 804, a specification of the rights to deputize 806 and the identity of an existing deputy 808 in a manner corresponding to the deputy credential request 220 in figure 2 (see column 8, lines 30 to 57), to the DDP. In contrast to the embodiment shown in figure 2, the principal/requester may cause (step 814) a deputy to be created to receive the delegated rights; see column 11, lines 51 to 60. If the principal/requester does not already have a public/private key pair then the DDP can obtain such a key pair from a certification authority or may itself have certification authority functionality to issue such a key pair; see column 12, lines 1 to 9. Similarly, the DPP can obtain or itself provide a public/private key pair for the deputy; see column 12, lines 15 to 19. The deputy credential certificate is formed (step 822) having the same structure as in the embodiment shown in figure 2; see figure 6 and column 12, lines 20 to 26.

4. The main request

The application according to the main request is the same as that according to the main request forming the basis of the decision.

4.1 The meaning of the expression in claim 1 "portable security token" in the context of the application

Claim 1 refers to a (hardware) portable security token (102) which, according to paragraph [0032] of the description, includes portable devices that can communicate with network devices through a so-called location-limited communication channel, examples being a cell phone, smart card, PDA, laptop computer and a hand-held remote control device. Since these examples all concern devices dedicated to and normally owned by

a single user, the board finds that the Distributed Deputization Point (DDP; figure 2; 202), which serves the many users of a distributed computer system and is thus not dedicated to any particular user, cannot be regarded as a "security token" in the sense of the application, let alone a portable one.

5. Inventive step, Article 56 EPC 1973

5.1 The reasons for the decision are based on the embodiment shown in figure 8 of D1 and described in column 11, line 18, to column 12, line 39, which extends the embodiment set out in figures 2 and 6. The reasons regard the DDP as the claimed "portable security token" and the "deputy 216" in the "principal node(s) 206" as the claimed target device to which a deputization in D1 is made. The board accepts the appellant's argument that the reasons for the decision are consequently based on an incorrect understanding of D1 in the context of the claims, in particular the identity of the "deputy" to which a "principal" delegates rights. As the appellant has argued, in D1 deputization of rights does not occur to "deputy 216". On the contrary, it is "deputy 216" that is acting as a principal to delegate rights. In D1 a principal delegates rights either to another existing entity or to an entity especially created to receive the delegated rights; see figure 8, step 814, and column 12, lines 9 to 10. Moreover, as stated above, the board finds that the DDP in D1 cannot be regarded as the "security token" set out five times in claim 1.

5.2 The board is also satisfied that there is no obvious problem or solution for the skilled person, starting from D1 and applying common general knowledge, to modify the DDP known from D1 to turn it into a

"portable security token" which, as set out in claim 1, can be brought into "close physical proximity to the target device". The board consequently finds that, already for this reason, the subject-matter of claim 1 of the main request involves an inventive step, Article 56 EPC 1973, in view of D1 and the common general knowledge of the skilled person. Thus claim 1 according to the main request overcomes the reasons given in the decision for refusing the application, and the decision must be set aside.

5.3 In view of the finding above that the reasons for the decision are based on an incorrect understanding of D1 in the context of the claims, in particular an incorrect understanding of the expression in claim 1 of the main request "portable security token", the board finds that it cannot be excluded that the search was not exhaustive and that more relevant prior art may exist.

6. Remittal, Article 111(1) EPC 1973

6.1 Remittal of the case to the first instance will not only give the first instance an opportunity to review its position on inventive step, but also to form an opinion on the following issues.

6.2 There seems to be doubt in claim 1 of the main request and thus a lack of clarity, Article 84 EPC 1973, caused by the expressions "location-limited communication channel"and "close physical proximity". Understood in the context of the examples given in paragraph [0040], which cover wired connections, wireless connections and physical computer-readable media, there is doubt as to what determines the limit of the communication channel and the meaning of "close physical proximity". In

particular, the embodiment involving physical computer-readable media does not seem to imply any limit of the communication channel or to constrain "proximity".

6.3 Claim 7 according to the main request, claim 6 of the first auxiliary request, claim 5 according to the second auxiliary request and claim 4 according to the third auxiliary request contain a passage in parentheses, making these claims unclear, Article 84 EPC 1973, since there is uncertainty as to whether the expression is to be understood as limiting or not.

6.4 In claim 1 according to the second auxiliary request the expression in line 11 "orming" should presumably read "forming", making the claim unclear, Article 84 EPC 1973.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the first instance for further prosecution.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated