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 14 December 2010

Case Number: T 1547/06 - 3.5.06

Application Number: 00962697.9

Publication Number: 1224517

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Method for computer security

Applicant:
QinetiQ Limited

Headword:
Group membership certificate/QINETIQ

Relevant legal provisions:
EPC Art. 123

Relevant legal provisions (EPC 1973):
EPC Art. 84, 56

Keyword:
"Added subject-matter - main and first auxiliary request (yes)"
"Inventive step - second auxiliary request (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1547/06 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 14 December 2010

Appellant: QinetiQ Limited
85 Buckingham Gate
London SW1E 6PD (GB)

Representative: Williams, Arthur Wyn Spencer
QinetiQ Limited
Intellectual Property
Malvern Technology Centre
St Andrews Road
Malvern
Worcestershire WR14 3PS (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 8 May 2006 refusing European patent application No. 00962697.9 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

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

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, dated 8 May 2006, to refuse the European patent application 00962697.9.

II. In the decision, the examining division referred, *inter alia*, to the following documents

D1: WO 96 17286
D2: J. Davis *et al.*, "An Implementation of MLS on Network of Workstations using X.500/509", Proc. IEEE Conf. on Performance, Computing and Communications, pp. 546-553, IEEE Press, 1997
D4: WO 98 25373

and argued that claim 1 lacked an inventive step over D1 in combination with either D2 or D4.

III. An appeal was filed by fax received on 6 July 2006 and the appeal fee was paid on the same day. A statement of grounds of appeal was filed by fax on 31 August 2006. The board takes it that the appellant requests to set aside the decision and to grant a patent on the basis of the following documents:

description, pages
1, 10-27 as published
2-9 received by fax on 20 September 2004
drawings, sheets
1/7-7/7 as published

and one of the following sets of claims as filed with the statement of grounds of appeal:

1-35 according to the main request
1-33 according to the 1st auxiliary request
1-31 according to the 2nd auxiliary request

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

"A method for computer security to control access to data held on a computer system (2) as requestable datasets (4) characterised in that the method includes:

a) allocating computer system users between a plurality of user groups (e.g. C, C/O, C/O/OU) as members thereof such that not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information (e.g. AWAC INC.) common to such members;

b) providing for each dataset an access category (e.g. 45433) selected from a plurality of such categories and associated with a criterion (e.g. UNCLASS) for access to that dataset by computer system users;

c) associating each user group (e.g. C, C/O, C/O/OU) with a respective dataset access category (e.g. 45433) such that all members of each user group (e.g. C, C/O, C/O/OU) having multiple members are associated with a dataset access category (e.g. 45433) which is common to members of that user group; and

d) *[sic]*

e) providing access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of

its membership of that user group and members of that user group being associated with a common dataset access category (e.g. 45433) which is appropriate for access to that dataset."

Claim 1 according to the first auxiliary request reads as follows:

"A method for computer security to control access to data held on a computer system (2) as requestable datasets (4) characterised in that the method includes:

a) allocating computer system users between a plurality of user groups (e.g. C, C/O, C/O/OU) as members thereof such that not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information (e.g. AWAC INC.) common to such members;

b) providing for each dataset an access category (e.g. 45433) selected from a plurality of such categories and associated with a criterion (e.g. UNCLASS) for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

c) associating each user group (e.g. C, C/O, C/O/OU) with a respective dataset access category such that all members of each user group (e.g. C, C/O, C/O/OU) having multiple members are associated with a dataset access category which is common to members of that user group and membership of a user group having multiple members is

authentically evidenced by provision of like user group information by each of such multiple members; and

d) providing access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of its membership of that user group and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access of that dataset."

Claim 1 according to the second auxiliary request reads as follows:

"A method for computer security to control access to data held on a computer system (2) as requestable datasets (4) characterised in that the method includes:

a) allocating computer system users between a plurality of user groups (e.g. C, C/O, C/O/OU) as members thereof such that not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information (e.g. AWAC INC.) common to such members;

b) providing for each dataset an access category (e.g. 45433) selected from a plurality of such categories and associated with a criterion (e.g. UNCLASS) for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

c) associating each user group (e.g. C, C/O, C/O/OU) with a respective dataset access category such that all members of each user group (e.g. C, C/O, C/O/OU) having multiple members are associated with a dataset access category which is common to members of that user group;

d) providing a respective computer-based identifying certificate means (20) for each user as authenticated evidence of that user's membership of its user group; and

e) providing access to a dataset to a member of a user group with multiple members in response to such member providing its identifying certificate means (20) and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access of that dataset."

Each request also comprises corresponding independent claims to a computer program and an apparatus.

V. With the summons to oral proceedings the board expressed its preliminary opinion that the appeal would probably have to be dismissed.

a. The board first noted that the label "D4" had been used incorrectly in the decision. During examination, the examining division had initially used D4 as defined above but later had introduced another document as "D4" as well. That document was renamed D5 by the board.

D5: US 5 220 604

The board pointed out that some of the references to "D4" in the decision (see esp. point 1.4 of the reasons, referring to columns 6 and 7 and figures 1a, 1b; and 2.4 of the *obiter dicta*, referring to columns 3, 6, 7, 10 and 11) could apparently only refer to D5, because D5 has both columns and figures 1a and 1b, whereas D4 has neither. By consequence, the refusal must be read as arguing lack of inventive step based on D1 in combination with either D2 or *D5*.

b. The board mentioned some possible deficiencies under Articles 84 EPC 1973 and Article 123 (2) EPC, and expressed its preliminary opinion that the subject matter according to claim 1 of all three requests lacked an inventive step over D1 and D5.

VI. In response to the summons, the appellant filed neither arguments nor amendments but announced that he would not be attending the oral proceedings. The board informed the appellant by fax on 8 December 2010 that the oral proceedings were nonetheless maintained.

VII. Oral proceedings were held as scheduled on 14 December 2010 in absence of the appellant.

Reasons for the Decision

Admissibility

1. The appeal is admissible as complying with the EPC admissibility requirements (see points I and III).

Interpretation of the claims and Article 84 EPC 1973

2. Claim 1 of all requests specifies that "membership of a user group" is to be "*authentically evidenced* by provision of user group identity information". The board considers dubious the notion of "authentically evidenc[ing]" and, in the following, interprets it to mean that membership is "evidenced by provision of authenticated user group identity information".

3. Claim 1 of all requests comprises a step of "*allocating* ... users between ... user groups". In the board's view, this step is supported by the description on the understanding that allocation of users to user groups is, in the context of the invention, implicit to the assignment of a distinguished name to a user (cf. p. 11, lines 4-11).

4. Under these provisos, the board has no objections under Article 84 EPC 1973 against claim 1 according to any of the requests.

Article 123 (2) EPC, All requests

5. Claim 1 of all requests comprises the features that "membership of a user group ... is ... evidenced by *provision* of user group identity information" and that

"access to a dataset" is granted "to a member of a user group ... in response to *such member providing*" either "evidence of its membership" (main and first auxiliary requests) or, more specifically, "its identifying certificate means" (second auxiliary request).

5.1 Literally, this language might suggest that the member of a user group would actively provide the required authentication when accessing a dataset, in a manner comparable to typing in a password.

5.2 This interpretation does not have verbatim support in the original application. The original claims more generally refer to users "*having* a ... certificate" (*e.g.* claim 10) or that "user group and ... data access" be *determined* "from the [user group] identifying means" (*e.g.* claim 8).

5.2.1 According to the main embodiment disclosed in the description, the "group identity information" is embedded in a user's X.509 certificate. This certificate, too, is not "provided by" but only "associated with" the user, and provided by the client computer when needed (cf. p. 4, lines 14-16; p. 10, lines 16-18; figs. 1 and 3; see also D2, sec. III.B, for more details about the X.509 authentication process).

5.3 While, therefore, the original application documents do not support the literal meaning of these features, they do support the slightly more general interpretation that the "group identity information" is available for individual users and produced when a user tries to access a certain dataset.

5.4 For what follows the board decides, in favour of the applicant, to adopt this latter interpretation rather than to consider this a violation of Article 123 (2) EPC.

6. All three requests require, according to claim 1 that "membership of a user group ... is ... evidenced by provision of *user group identity information ... common* to such members" (feature a) without defining the nature of this common group identity information.

Claim 1 of the second auxiliary request further requires that the identity information must be contained in each user's "computer-based identifying certificate means" (feature d).

Claim 1 of the first and second auxiliary requests additionally specify that dataset access categories are hierarchically organised (features b and d).

6.1 The board is satisfied that this hierarchy as claimed is disclosed in the application documents as originally filed, for instance by fig. 2 and the description on p. 16, lines 14-21.

6.2 The description appears to disclose only one specific example for evidence of a user's group membership, namely the elements of the distinguished name of the user's X.509 certificate, but indicates that generalization to "some [other] form of certificate" is intended, provided it "incorporat[es] categories of clients which correspond to different degrees of access" (p. 14, last par. and p. 16, last par.).

It would seem that the description uses synonymously the terms "client" and "user" (*e.g.* p. 13, lines 6 ff. refer to "particular clients" identified by their distinguished names; and p. 22, lines 21 ff. refer to "a user's distinguished name") and the terms "categories" and "groups" (cf. *e.g.* p. 22, lines 26-27).

On this basis, the board accepts that it is originally disclosed to provide evidence for group membership based on an unspecified certificate (esp. by p. 16, last par.).

The board is thus satisfied that claim 1 of the second auxiliary request conforms with Article 123 (2) EPC.

6.3 The board was unable to find disclosure of any "user group identity information" which would be "common to" [the] "members" of a group but *not* linked to "some form of certificate". This notion would, for instance, subsume a group identity and password that all group members would have to provide in addition to (or instead of) their individual identity and passwords, which is nowhere disclosed or implied by the application as originally filed.

The board concludes, for this reason, that claim 1 according to the main and the first auxiliary request extends beyond the contents of the application as originally filed by way of intermediate generalization, in violation of Article 123 (2) EPC.

Article 54 EPC, Second auxiliary request

7. The appellant has not challenged document D1 as a suitable starting point for the assessment of novelty and inventive step.

7.1 Document D1 discloses a method of computer security to control access to a database on a computer according to which different users - or different computer identities - can be given different access rights (*i.e.* "dataset access categories").

7.2 The access rights are organised as user permissions to perform certain operations, specifically to create, read, update, or delete data, on individual datasets in the database (cf. p. 3, lines 9-16, and p. 8, lines 3-15). This system - referred to as CRUD, for short - implies a hierarchy of access rights as claimed: For example, where system administrators have unlimited access (*i.e.* the right to create, read, update and delete certain data), employees have the right to read and update, and customers have only read access, the "access category" of system administrators is "relatively higher" than and "incorporates" the others. In passing, it is added that hierarchical access categories are also a commonly practiced way of organizing access restrictions to electronic data but also to paper documents (cf. also D2, p. 547, left col., last par.)

7.3 D1 further discloses that users identify themselves individually (cf. fig. 1) by indicating their individual password (or, if they have multiple computer identities, one of the associated passwords). After

identification, the system would establish each user's access rights.

7.4 In several places, D1 also refers to groups of users which may be given specific access rights *as a group*. For example, on page 11, lines 13-18, D1 defines a hierarchy of groups of system administrators, a few of which "hav[e] unlimited access rights" while "the majority hav[e] limited rights". Further on page 11, lines 20-26, D1 discloses that users can be divided into "client groups" each of which has "access rights limited to the needs of the client" and a dedicated client-administrator. D1 also states that "each client [would be] representing a department or external organisation" (p. 11, line 21). However, where a user belongs to any such group of users with the same access rights, no group affiliation need be explicitly established. For instance, the mere existence of client groups of users with uniformly restricted access does not imply anything other than individual user identification.

7.5 Accordingly, D1 does not disclose that each user has an associated piece of "user group identity information" which is produced to authenticate "that user's membership of its user group" when a user tries to access a certain dataset. More specifically, D1 does not disclose the corresponding use of a "computer-based identifying certificate means".

7.6 Due to these differences, claim 1 is novel over D1.

Article 56 EPC 1973, Second auxiliary request

8. D1 discloses a system with a large number of users, "in the order of 20,000" or "perhaps as many as 10,000" (p. 1, lines 12-14 and p. 8, lines 18-20). It is considered that management of individual access rights for a few 10,000 users requires considerable effort in terms of storage and maintenance, which would become even more significant should the user base grow further. This effort would apparently be a lot smaller if access rights had to be kept only for a small number of groups.

8.1 The board therefore considers as an appropriate objective technical problem solved by the invention as claimed to reduce the effort of managing the access rights. This would appear to correspond to a main advantage of user groups according to the application (p. 4, lines 1-6).

8.2 Document D5, in a similar context of resource access control, discloses that the list of all "principals" (*e.g.* users, see col. 3, line 2) can become "quite lengthy" when the user base grows (*e.g.* up to 100,000; cf. col. 9, line 67 - col. 10, line 9). D5 then proceeds to state that "fast and manageable access" may be achieved by providing groups of "principals, who are considered equivalent for security related purposes" and have the same access rights (col. 10, lines 2-12).

8.3 The skilled person, setting out to solve the objective technical problem just defined, would find an express solution in D5 and would therefore not hesitate to incorporate the pertinent teaching of D5 into D1.

8.4 D5 further discloses that membership of individual users in a group may be specifically certified (cf. col. 10, lines 37-39 and 50-65). This certificate must be "furnished" to establish group membership (cf. col. 10, line 66 - col. 11, line 5). The certificates of all users of some group G have in common at least the reference to "G" (cf. again col. 10, lines 57-60).

8.5 In the terms used in claim 1, hence, D5 clearly discloses to provide a "computer-based identifying certificate means for each user as authenticated evidence of that user's membership of its user group", comprising "user group information ... common to" all members of a given group, and that this information is produced when a user tries to access certain datasets.

8.6 Therefore, the board concludes that the skilled person starting from D1 would, by incorporating the teaching of D5, arrive at the subject-matter of claim 1 according to the second auxiliary request without an inventive step, in violation of Article 56 EPC 1973.

9. As there is no allowable request, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The registrar: The Chairman:

B. Atienza Vivancos D. H. Rees