Internal distribution code:

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

Datasheet for the decision of 10 January 2024

Case Number: T 1495/21 - 3.5.06

Application Number: 14735072.2

Publication Number: 3008596

IPC: G06F9/50

Language of the proceedings: EN

Title of invention:
PROVIDING DOMAIN-JOINED REMOTE APPLICATIONS IN A CLOUD ENVIRONMENT

Applicant:
Microsoft Technology Licensing, LLC

Headword:
Authenticated connection/Microsoft

Relevant legal provisions:
EPC Art. 84
RPBA 2020 Art. 13(2)

Keyword:
Claims - clarity (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 1495/21 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 10 January 2024

Appellant: (Applicant)	Microsoft Technology Licensing, LLC One Microsoft Way Redmond, WA 98052-6399 (US)
Representative:	Grünecker Patent- und Rechtsanwälte PartG mbB Leopoldstraße 4 80802 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 10 March 2021 refusing European patent application No. 14735072.2 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	T. Alecu
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division to refuse the application. All requests underlying the decision were refused for a lack of inventive step. The decision cited inter alia documents

D6: US 2013/152076 A1
D7: ANTONIO CELESTI ET AL: "Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication", 2010
D8: US 2012/233678 A1

II. With the statement of grounds of appeal the Appellant requested that the decision of the Examining Division be set aside and that a patent be granted on the basis of the main request or of one of two auxiliary requests, all as (re-)filed with the grounds of appeal. The main request and the first auxiliary request corresponded respectively to the main and second auxiliary requests underlying the decision under appeal. The second auxiliary request was based on the third auxiliary request underlying the decision under appeal, amended in response to a clarity objection so as to use wording acknowledged to be clear by the Examining Division.

III. In a communication accompanying a summons to oral proceedings, the Board indicated that it tended to confirm the decision of the Examining Division that the request lacked an inventive step.

IV. During the oral proceedings before the Board the Appellant filed a new main request in replacement of the previous main request. A discussion on claim

interpretation led the Board to conclude that all requests lacked clarity.

V. Claim 1 of the main request defines:

A public cloud computing system (101) comprising the following:

one or more processors;

system memory;

one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, causes the public cloud computing system to perform a method for provisioning private virtual machines (115) in the public cloud computing system, the method comprising the following:

an act of receiving (210), by the public cloud computing system (101), authentication information (111) for a private domain (114) from an entity (110) and an indication that one or more private virtual machines (115) from the private domain are to be provisioned on the public cloud computing system (101), the indication being received with the authentication information from the entity, the entity's private domain being accessible using the authentication information and the entity's private domain being external to the public cloud computing system;

an act of establishing (220) a virtual network (102) on the public cloud computing system, the virtual network being configured to host the

entity's one or more private virtual machines (103), each virtual machine being configured to host one or more remote applications (104);

an act of establishing (230) an authenticated connection (113) from the virtual network to the entity's private domain using the received authentication information, wherein the received authentication information includes one or more authentication credentials (112) that are used to authenticate the entity to the public cloud computing system; and

an act of providing (240) at least one of the entity's private virtual machines from the private domain on the public cloud computing system, wherein data (117) stored within the entity's private domain is accessible by at least one of the remote applications provided by the private virtual machines using the authenticated connection.

The underlined feature is the amendment in respect of the previous main request.

VI. The auxiliary requests are based on the previous main request. The Board notes though that the Appellant was prepared to file new auxiliary requests containing also the underlined feature above.

VII. Claim 1 of the first auxiliary request contains the additional clause "*wherein the one or more remote applications require access to the resources within the entity's private domain*" at the end of the text specifying "*an act of establishing (220) a virtual network [...]*".

VIII. Claim 1 of the second auxiliary request contains the additional text added to the end of the claim

wherein a virtual machine managing service is instantiated to manage the provisioning of the private virtual machines,
wherein the virtual machine managing service sends a data request for the private domain authentication information,
wherein the private domain authentication information comprises a service account that is accessible using one or more authentication credentials,
wherein the authentication information received from the entity includes the one or more authentication credentials, and
wherein the service account allows the entity to manage the at least one of the entity's private virtual machines on the public cloud.

Reasons for the Decision

The application

1. The application relates to "*provisioning private virtual machines in a public cloud and to managing private virtual machines hosted on a public cloud*" (paragraph 1 of the application as originally filed). The provisioning of private virtual machines on a public cloud allows users to connect "*to their entity-provided remote applications, especially those which require access to resources within the entity's private network*" (paragraph 29). The term "entity" as used in the application refers to the entity that requests and owns the provisioned virtual machines.

1.1 The entity is also required to provide authentication information to the public cloud. The request for provisioning can be sent together with the authentication information (paragraph 34).

1.2 Using the authentication information, an "*authenticated connection*" is established which allows the "*remote applications (and/or the VMs running the applications) to access certain portions of private data 117, services or other software on private domain 114*" (paragraph 36).

Prior art

2. Though the appeal was ultimately decided on clarity (Article 84 EPC), the discussion which led to it was initially one on inventive step. It was during this discussion that the need arose for clarifying the interpretation of the claim wording in view of a comparison with the prior art. Therefore, the Board summarises below the prior art to the relevant extent.

3. Document D6 was used by the Examining Division as a starting point for the assessment of inventive step. It relates to the migration of virtual machines between enterprise and public clouds. If the enterprise cloud runs out of resources, it may migrate services "*in the form of applications or servers, e.g., a web server, operating as virtual machines (VMs)*" to a public cloud. When resources become available, "*the VMs may migrate from the public data center back to the private data center*" (paragraph 3).

3.1 Discussing the required communication after migration, D6 states in paragraph 14: "*When VM 180 is part of a local area network (LAN) and migrates between data*

centers, the LAN is connected by LAN extension through a wide area network (WAN) or public network 170, e.g., the Internet, as part of a Layer 3 VPN. LAN extension is a technology that allows these LAN entities in different data centers to "talk" to each other by treating the underlying network as a single LAN."

3.2 To initiate the migration request from the private to the public cloud, the private cloud provides VM information and credentials (figure 2a). The corresponding paragraph 24 states: "*At 210, VM migration is initiated by server 135(2) for VM 20(5) to migrate from server 135(2) to server 160(1). As part of the migration, server 135(2) provides VM operating information as described above and migration credentials for the VM, e.g., VM 20(5). At this point, since there is a trusted relationship between the enterprise and provider clouds, the server 160(1) may accept the VM credentials*".

4. Document D7 was relied upon by the Appellant during the oral proceedings to show that the establishment of a trusted relationship was not trivial (page 96, left column, as referred to by the Appellant) and did not necessarily imply the sending of authentication credentials from one cloud to another. D7 indeed teaches a method of federating clouds where authentication is carried out using third party identity providers (figure 3, step 5, page 98 right column as referred to by the Appellant). Once federated, a cloud can provision resources on the other federated clouds.

5. The Appellant also referred to D8 to show that authentication did not necessarily imply the sending of authentication credentials from one cloud to another. In

D8 a separate authentication server is used for that purpose (see abstract).

Main request: admittance

6. The main request was filed during the oral proceedings before the Board. The amendment (in view of the previous main request) consisted in the addition of the following clause to the claimed *"act of establishing [...] an authenticated connection"*:

wherein the received authentication information includes one or more authentication credentials (112) that are used to authenticate the entity to the public cloud computing system.

7. The reason for filing it was the change of the focus in the discussion from inventive step to claim interpretation and claim clarity regarding what the "*act of establishing an authenticated connection*" might encompass. The new feature, though not explicitly claimed up to that point, had already been considered by the Board in its evaluation of claim clarity (see below), so its admittance was not detrimental to procedural economy. Considering all these circumstances, the Board decided to admit the new request (Article 13(2) RPBA 2020).

Main Request: clarity

8. Claim 1 of the main request defines inter alia

(a) an act of receiving (210), by the public cloud computing system (101), authentication information (111) for a private domain (114) from an entity (110) and an indication that one or more private

virtual machines (115) from the private domain are to be provisioned on the public cloud computing system (101), the indication being received with the authentication information from the entity, the entity's private domain being accessible using the authentication information and the entity's private domain being external to the public cloud computing system;

(b) an act of establishing (220) a virtual network (102) on the public cloud computing system, the virtual network being configured to host the entity's one or more private virtual machines (103), each virtual machine being configured to host one or more remote applications (104);

(c) an act of establishing (230) an authenticated connection (113) from the virtual network to the entity's private domain using the received authentication information, wherein the received authentication information includes one or more authentication credentials (112) that are used to authenticate the entity to the public cloud computing system; and

9. There are at least two different types of authentication to which these features appear to refer.

9.1 One is authentication of the private cloud vis-à-vis the public cloud for the purpose of provisioning virtual machines (see esp. the last three lines in the *"act of establishing an authenticate connection"* above). In this case, the private cloud must authenticate itself to the public cloud so that the public cloud knows which entity makes the request for provisioning and whether it can be allowed.

9.2 Another is authentication of the public cloud vis-à-vis the private cloud for accessing resources on the private cloud (see esp. the last four lines in the *"act of receiving [...] authentication information"*). In this case, the virtual machines, or the virtual network established on the public cloud, need to authenticate to the private cloud.

10. Though both things relate to authentication, the nature of the connection is different. In the first case, the connection is made at the resource management (provisioning) level, much as in D7, in line with the Appellant's argument regarding inventive step (see point 4 above). This would also correspond to the trusted relationship of D6 (see point 3.2 above). The authenticated connection according to the second case is established at the network level. This may be achieved by an extended LAN as per D6 (see point 3.1 above), but also in other ways such as parameterizing the private cloud to allow requests from the virtual cloud on the public domain, storing on the public cloud the names/addresses of the resources on the private cloud and the corresponding authentication information, or by a combination of such measures.

11. It is not possible to clearly derive from the claim which of these is meant, because the two aspects are mixed.

11.1 Feature (a) defining the act of receiving authentication information states that the authentication information is received together with the request for provisioning. This suggests that the authentication relates to the provision of resources in the public cloud to run the private virtual machines, although the fea-

ture also mentions the access of resources in the private domain.

11.2 Feature (b) defines the establishment of a virtual network on the public cloud. Feature (c) specifies establishing an authenticated connection between the established virtual network on the public cloud and the private domain. This hints at an authentication of the second type, of a connection at the network level.

11.3 However, confusingly, feature (c) also states (per the amendment made during the oral proceedings) that the "*authentication information includes one or more authentication credentials (112) that are used to authenticate the entity to the public cloud*", which rather refers to the first type of authentication.

12. The Appellant argued that the claim was not unclear, but merely broad. It should be taken to cover both types of authentication. The skilled person knew what an authenticated connection was and how to establish it, even if the application did not detail it. The invention did not concern the type of the authenticated connection itself, but the fact that the information was sent simultaneously with the request for provisioning. This saved network bandwidth. It was also clear what this authentication information comprised. The Appellant made reference to paragraphs 34 to 36 of the description.

13. The Board does not agree with this argument. In principle, a claim may be broad and unclear at the same time, so that the mere argument that the claimed scope is "merely broad" is not a sufficient defense to an objection that a claim is unclear. Irrespective of

breadth, it must be clear what is encompassed in the scope of the claims.

13.1 In the present case, the notion of "authentication" in itself covers a wide range of operations involving various different bits of information ("authentication information"). From this perspective, the breadth of the term "authentication information" alone might not be harmful for clarity.

13.2 However, claim 1 does not merely define the sending of "authentication information", but also an act of establishing an authenticated connection. It is the Board's opinion that it is not possible to say with sufficient certainty whether the claimed "act of establishing" an authenticated connection relates to just one of the two authentication types discussed above, to both, or possibly even to something else. Further, it is not clear, in either case, what the act of "establishing" is, effectively (see point 10 above). This clarity problem remains even if one accepts that the authentication information contains whatever is needed for the connection to be established.

13.3 The claim language therefore does not, as the Appellant suggests, merely "leave open" what type of authentication the claim relates to, but it is genuinely unclear in this regard.

13.4 The Board also notes that the ambiguity in question has a relevance for inventive step (see point 10 above as to the different possible mappings to D6).

Auxiliary requests

14. The auxiliary requests suffer from the same deficiency.

14.1 As regards claim 1 of auxiliary request 1, the added feature that the virtual machines created on the public cloud require access to the private domain does not address the clarity issue discussed above. In fact, claim 1 of auxiliary request 1 does not go substantially beyond what is already implied by claim 1 of the main request.

14.2 In claim 1 of auxiliary request 2, a "*managing service*" and a "*service account*" are introduced "*to manage the provisioning*" and to "*allow[] the entity to manage [its] private virtual machines*". Authentication information is only referred to insofar as it contains "*authentication credentials*" used to access the service account. This use of parts of the authentication information cannot clarify the use of the other parts which the Board finds unclear as explained above. Also the fact stressed by the Appellant that the second auxiliary request underlined (further) that the authentication information sent together with the provisioning request contained all the necessary information for mutual authentication does not address the clarity problem underlined above (see also 13.2 above).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde Martin Müller

Decision electronically authenticated