Internal distribution code:

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

Datasheet for the decision of 2 February 2017

Case Number: T 1524/10 - 3.5.01

Application Number: 07122559.3

Publication Number: 1933264

IPC: G06Q10/00

Language of the proceedings: EN

Title of invention:
Policy enforcement via attestations

Applicant:
Oracle International Corporation

Headword:
Policy enforcement / ORACLE

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - changing access rights depending on user's behaviour (no - not technical)

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 1524/10 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 2 February 2017

Appellant: (Applicant)	Oracle International Corporation 500 Oracle Parkway, M/S 5 op 7 Redwood Shores, CA 94065 (US)
Representative:	D Young & Co LLP 120 Holborn London EC1N 2DY (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 18 March 2010 refusing European patent application No. 07122559.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	P. Scriven
	P. Schmitz

Summary of Facts and Submissions

I. This is an appeal against the Examining Division's decision to refuse European patent application 07122559. The Examining Division considered that claim 1 of the sole request then pending comprised subject-matter extending beyond the content of the application as originally filed, and that claim 11 lacked novelty in the light of Document D1.

D1: *Security Assertion Markup Language (SAML) V2.0 Technical Overview, Working Draft 08, 12 September 2005, available from https://www.oasis-open.org/committees/documents.php?wg_abbrev=security (see https://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf)*

II. In the statement setting out the grounds of appeal, the appellant requested that the Examining Division's decision be set aside and a patent be granted on the basis of the text underlying the appealed decision, and that oral proceedings be held before any final decision was taken.

III. The Board communicated its provisional view of the case. Inter alia, the Board indicated that the subject-matter of claim 1 seemed to lack inventive step in the light of D1, on the basis that it defined an obvious implementation (using a plug-in to the operating system) of non-technical steps.

IV. With its letter of response, dated 6 October 2015, the appellant filed a single substantive request, and maintained the request for oral proceedings.

V. The Board arranged for oral proceedings to be held. With the summons, the Board sent a further communication indicating a number of issues that the appellant should be ready to discuss, in particular, the issue of inventive step in the light of D1.

VI. With its letter of response dated 21 December 2016, the appellant submitted a new main request, and maintained the previous request as an auxiliary request.

VII. During oral proceedings before the Board, the appellant submitted a new main request, and made a final formulation of requests as follows:

that the decision under appeal be set aside and that a patent be granted on the basis of
- claim 1 of the main request as submitted during oral proceedings before the Board, with further claims still to be adapted thereto; or
- on the basis of auxiliary request 1, filed with the letter dated 6 October 2015; or
- on the basis of auxiliary request 2, filed with the letter dated 21 December 2016.

VIII. Claim 1 according to the main request reads as follows.

A computer-implemented security method
comprising a policy-based attestation service
to provide enhanced security to resources

accessible to an operating system, wherein the policy-based attestation service is implemented as a plug-in to the operating system, the method comprising the policy-based attestation service performing the step of:
monitoring an environment where a given set of resources are accessible, wherein access to the resources is governed by access permissions;
detecting (110) a principal operating under an identity within the environment being monitored by the policy-based attestation service, wherein the principal is initially authenticated to the environment;
identifying (120) a condition occurring within the environment by using policy limitations that define conditions the policy-based attestation service is to monitor within the environment, the conditions associated with operations taken by the principal operating within the environment whereby operations taken by the principal may trigger a condition defined by the policy limitations;
obtaining (130) an attestation in response to identifying the condition, wherein the attestation defines a policy for dynamically altering access permission of the principal with respect to the resources that the principal can access within the environment; and
enforcing (140) the policy in response to the attestation against the principal when the principal attempts to access the multiple resources within the environment so as to restrict access to resources that would otherwise have been available to the

principal.

IX. Claim 1 according to the first auxiliary request reads as follows.

A computer-implemented security method to provide enhanced security to resources accessible to an operating system, implemented by a policy-based attestation service as a plug-in to the operating system, the policy-based attestation service having access to policy limitations for identify [sic] a condition occurring within an environment where resources are available, access to the resources being governed by access permissions assigned based on a role designation, the method comprising the policy based attestation service:
detecting (110), by monitoring the environment, a principal operating under an identity within the environment, wherein the principal is authenticated to the environment and is able to assume one or more role designations while operating within the environment;
identifying (120) a condition occurring within the environment by using the policy limitations, the condition being associated with just the principal or with the principal and also with another principal operating within the environment;
obtaining (130) an attestation in response to identifying the condition, wherein the attestation defines a policy for dynamically altering access permissions of the principal

with respect to multiple resources that the principal can access within the environment; and
enforcing (140) the policy defined by the attestation against the principal when the principal attempts to access the multiple resources within the environment.

X. Claim 1 according to the second auxiliary request reads as follows.

A computer-implemented security method to provide enhanced security to resources accessible to an operating system, implemented as a plug-in to the operating system, the method comprising:
detecting (110) a principal operating under an identity within an environment where a given set of resources are available and wherein the principal is authenticated to the environment, by monitoring the environment;
identifying (120) a condition occurring within the environment by using global policy limitations of a global policy that defines the condition, the condition associated with operations taken by the principal operating within the environment;
obtaining (130) an attestation in response to identifying the condition, wherein the attestation defines a policy for dynamically altering access permission of the principal with respect to multiple resources that the principal can access within the environment; and

enforcing (140) the policy in response to the attestation against the principal when the principal attempts to access the multiple resources within the environment.

XI. The appellant's arguments regarding the procedure before the Board can be summarised as follows.

The communication sent with the summons to oral proceedings indicated possible issues of clarity and inventive step but did not substantiate any actual objection.

The Examining Division objected to claim 11 on the grounds of lack of novelty, but not to claim 1. During the whole procedure, no objection of lack of novelty had been directed at claim 1, and present claim 11 had been amended to correspond.

New objections raised during oral proceedings would be prejudicial to the appellant. A decision on such a basis could not be taken if the appellant were unrepresented. In consequence the appellant's interests might best be served by not attending.

XII. The appellant submitted arguments concerning the nature of the invention, which can be summarised as follows.

The invention concerned the configuration of a system to identify conditions and react with appropriate changes. It was not concerned with any particular reasons for which permissions might be altered.

The main purpose was to improve computer security. That

was a technical matter. An administrator might set rules for access, but could only set rules supported by the underlying computer systems.

In the prior art, once a user was logged in, his access permissions were mostly fixed for the whole session (see paragraph 0005 of the published application). There was no prior art indicating systems how those were implemented that did not fall under the term "mostly".

A user changing file properties from read-only to read-write would not count as a condition within the terms of the claim.

The objective technical problem was how to enable the automatic determination of conditions occurring within the environment that might result in changes to access permissions.

XIII. The appellant submitted specific arguments comparing the invention with the disclosure in section 3.4.2 of D1. These can be summarised as follows.

The example shown in Figure 11 of D1 disclosed only the steps of obtaining an attestation and of enforcing a policy, but none of the other features defined in claim 1.

The invention addressed the problem of applying additional access restrictions during a session. Any change in permissions in D1 would involve starting a new session.

The first action in D1 is the principal's attempt to access a resource. That was the final action in claim 1.

The invention was devised by a security architect. It was described at the same level as D1, although D1 had better examples of use.

The claim defined the invention in general terms, but there were enough details to distinguish it from D1: the use of a plug-in to the operating system, the enhancement of security of resources accessible from the operating system, the principal being authenticated and, therefore, already logged on, and the monitoring of the environment and identification of condition associated with operations performed by the user.

The term "policy" was used in the same sense in D1 as in the claims. It meant something akin to configuration file, something that could be changed on the fly rather than something that was hard wired.

Section 3.4.2 of D1 disclosed a method in which a principal tried to access a resource and in which policies were enforced. However, there was no indication that resources were accessible to an operating system, that the principle was authenticated in the environment, or that there was anything like the identification of a condition described by a policy and dependent upon user behaviour. Line 565 in section 3.4.2 indicated that the user was authenticated, but did not indicate how that was done.

When the PEP in Section 3.4.2 deferred access pending a decision, that was not the implementation of a policy. Such behaviour was hard coded, and could not be in accordance with a policy, because a policy had to be an explicit description.

Reasons for the Decision

Procedural matters

1. The Board's communication accompanying the summons to oral proceedings stated, in paragraph 2, that the appellant "should be prepared to discuss inventive step, particularly in the light of D1 ...". The appellant essentially argued that if claim 1 were to be objected to at the oral proceedings, this would be a new objection because neither the examining division nor the Board had ever substantiated such an objection.

2. However, the Board had set out its provisional view that the subject-matter of the pending claim 1 lacked inventive step in the light of D1 in its first communication. With the summons, it indicated that the issue would be further discussed, in particular with an eye to which features were technical.

3. The Board is satisfied that the appellant was aware of its provisional view and of the issues of technicality and novelty over D1. All this, moreover, was further discussed in the oral proceedings.

4. The Board also notes that it is not obliged to send a communication with a summons to oral proceedings, but generally does so in order to help the appellant prepare. At the time of arranging oral proceedings, it may appear that questions in certain areas are likely to arise and the Board considers it good practise to inform the appellant. Moreover, the Board is not obliged to delay its decision due to a failure to

attend (Article 15(3) RPBA). Section III.B 2.7.3 of the Case Law of the Boards of Appeal of the European Patent Office, 8th Edition, is instructive on this matter.

Background

5. A computer user may be allowed to access some resources (a printer, a public document, ...) but not allowed to access others (a confidential report, ...). Other users may have different access rights. As the application explains it (paragraph 0005 of the published application), once a user has been authenticated, what he may access and what he may not access mostly remains fixed.

6. However, the user might do something that would cause suspicion. He might have access to a number of confidential documents, but if he were to access all of them quickly, one after another, that might indicate that he is planning some nefarious act. He might be planning on passing copies to unauthorised persons. He might be a spy or a whistle-blower.

7. Under such circumstances, it might be desirable to reduce the user's access to confidential documents, pending investigation.

8. The invention caters for this desire. Broadly stated, when the system detects that some particular circumstance has arisen in connection with a user's actions, it obtains and applies a new, more restricted, access policy.

The disclosure of D1

9. Section 3.4.2 of D1 discloses a method of using of a particular markup-language (XACML) for controlling access to resources. A user requests access (step 1 in Figure 11 and the preceding text) and information is obtained about the user and possible other parties to the request (step 2). This information might be sent with the request, or it might be obtained elsewhere. Other necessary information is gathered (step 3) and on the basis of all this information, the request is evaluated for compliance with one or more policies (steps 4 and 5). A decision to grant or withhold access is then made and enforced (steps 6 and 7).

10. The appellant submitted the following arguments with regard to D1.

- Neither a plug-in nor resources accessible to an operating system were disclosed.

- The principal was not authenticated.

- There was no identification of a condition defined by a policy. In particular, the detection of an attempt to access a resource and deferring access pending a decision, which was hard coded in D1, could not be seen as the identification of a condition defined in a policy, because a policy was a changeable configuration.

11. The Board agrees that D1 mentions neither an operating system nor a plug-in, but cannot agree that the principal is unauthenticated. According to section

3.4.2, line 565, "it is common to consider when and how a user authenticated" as one of the considerations in allowing or withholding access. That is, the time and method of authentication are taken into account for subsequent decisions on access to resources. The Board understands this as saying that the access control method works for users that have been authenticated.

Main request, interpretation of claim 1

12. Before the method of claim 1 starts, a principal is already authenticated (she is "operating under an identity"). Operations taken by this principal are monitored, in order that the occurrence of some predefined condition can be recognised. When the condition arises, a new access policy is obtained and applied to that principal, so as to restrict access. All that is done by a plug-in to the operating system.

13. This exposition of the claim derives from the following explanations, given by the appellant during oral proceedings before the board.

The principal "operating under an identity" meant that she was already authenticated, and this was important in order to distinguish the invention from the common situation in which changes of access might result from a user logging in.

The term "policy limitations that define conditions the policy-based attestation service is to monitor" could have been more clearly formulated, but the intention was that the condition to be identified was not hard coded but was set out in something akin to a configuration file. Thus, the condition was not fixed,

but could be changed by modifying the definition.

The step of "obtaining ... an attestation ... [that] defines a policy ..." meant that a new definition of access permissions was obtained.

14. The Board is not persuaded that the term *policy*, as used in the application, necessarily refers to a set of conditions explicitly defined; but the claim does cover this interpretation.

Main request, inventive step

15. Thus the invention of claim 1 differs from D1 in that it is implemented by a plug-in to an operating system and in that the monitoring is for a condition which is defined by a changeable policy definition.

16. The technical effect, as the appellant explained it, was to increase security. A user might be authenticated on the basis of a password, and so be allowed to access certain files. With the invention, in addition to the password, patterns of access could be spotted and some remedial action taken. As the Board understands it, an example might be a user too frequently visiting websites that the network's owner dislikes, with a restriction on access while some investigation is carried out.

17. The appellant further argued that the invention was technical in virtue of being generic. The specification of a rule that restricted access to certain banking resources might be formulated by a banker, but only a technically-skilled person could conceive of a machine that could be used with any rule, irrespective of the

rule's motivation, which could be technical or not.

18. The Board rejects the appellant's argument regarding the invention's generic nature. The claim does not define a method that can detect any condition defined by rules. It defines a method that detects one condition defined by rules, and that condition may well be non-technical. Indeed, the appellant's example of a user accessing sensitive documents in an unusual way, is a non-technical condition.

19. As a consequence, the Board does not see the identification of a condition that arises from a user's behaviour and the application of more restricted rules of access as a technical difference over D1. The only technical distinction is in the implementation as a plug-in to the operating system. The technical problem is, therefore, how to implement this access control scheme.

20. In the Board's view, an operating system of some sort is implicit in D1; but the plug-in is not. The effect of the plug-in is to make the system of access control accessible to various applications, so that individual applications need not provide their own. The skilled person, seeking that effect would want to provide something at the level of the operating system so that all applications could use it; indeed, he would consider making it obligatory. The realisation as a plug-in means that it can be included or not, as the operator desires; and that seems a natural option to include.

21. The Board, therefore, judges that at least some of the alternatives that fall within the definition of claim 1 do not involve an inventive step (Article 56 EPC).

Accordingly, the main request is not allowed.

First auxiliary request, claim 1, inventive step

22. This request differs from the main in that access is based on roles. That is, a user who has the role of *editor* can do more with a document than a user who has the role of *reader*; a user who is an *administrator* can do more than one who is a *visitor.*

23. The Board does not see the user's role as a technical issue. As a result, there are no technical differences over D1 that are not already defined in the main request.

24. Consequently, this request is not allowed.

Second auxiliary request, claim 1, inventive step

25. The subject-matter of this claim is broader than in the main request, and, therefore, lacks inventive step for the same reason.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated