Internal distribution code:

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

Datasheet for the decision of 28 May 2025

Case Number:	T 0588/22 - 3.5.06
Application Number:	13715758.2
Publication Number:	2820584
IPC:	G06F21/00, H04L29/06
Language of the proceedings:	EN

Title of invention:
SYSTEM AND METHOD FOR ACCESS DECISION EVALUATION FOR BUILDING AUTOMATION AND CONTROL SYSTEMS

Patent Proprietor:
Signify Holding B.V.

Opponent:
Molnia, David

Headword:
Access decision evaluation for building automation and control systems/SIGNIFY HOLDING

Relevant legal provisions:
EPC Art. 123(2), 56
RPBA Art. 13(2)
EPC R. 139

This datasheet is not part of the Decisior
It can be changed at any time and without notic

Keyword:

Amendments - added subject-matter (no)
Inventive step - (no) - (yes)
Amendment to appeal case - taken into account (yes)
Correction of error in document(s) - (yes)

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

Case Number: T 0588/22 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 28 May 2025

Appellant:
(Opponent)

Molnia, David
Theatinerstraße 16
80333 Munich (DE)

Representative:

Molnia, David
Molnia Ho PartG mbB
Theatinerstraße 16
80333 München (DE)

Respondent:
(Patent Proprietor)

Signify Holding B.V.
High Tech Campus 48
5656 AE Eindhoven (NL)

Representative:

van Eeuwijk, Alexander Henricus Waltherus
Signify Netherlands B.V.
Intellectual Property
High Tech Campus 7
5656 AE Eindhoven (NL)

Decision under appeal:

Interlocutory decision of the Opposition Division of the European Patent Office posted on 23 December 2021 concerning maintenance of the European Patent No. 2820584 in amended form.

Composition of the Board:

Chairman M. Müller
Members: A. Teale
K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. This is an appeal by the opponent (appellant) against the interlocutory decision, dispatched with reasons on 23 December 2021, that European patent EP 2 820 584 according to a first auxiliary request, received on 13 September 2021, and the invention to which it related met the requirements of the EPC. The patent according to the main request, the patent as granted, was found not to comply with Article 100(c) EPC regarding added subject-matter.

II. The notice of opposition, received on 10 January 2020, was based on the grounds for opposition under Article 100(a) EPC (novelty and inventive step) and 100(c) EPC (added subject-matter).

III. A notice of appeal and the appeal fee were received on 2 March 2022, the appellant requesting that the decision be set aside and the patent revoked. The appellant also made an auxiliary request for oral proceedings.

IV. In a statement of grounds of appeal, received on 2 May 2022, the appellant requested that the decision be set aside and the patent revoked. The appellant argued that the claimed subject-matter lacked novelty and inventive step in view of D1 or D2, these documents being as follows:

D1:	US 7 002 468 B2
D2:	US 2005/0144186 A1.

V. With a response to the appeal, received on 15 September 2022, the respondent (proprietor) submitted (as document D5) a labelling scheme for the features of the independent claims of auxiliary request 1. The respondent requested that the appeal be dismissed and, as an auxiliary request, oral proceedings. As further auxiliary requests, the respondent stated that they defended the patent according to auxiliary requests 2 to 4 in the decision, received on 13 September 2021. The respondent did not defend the patent as granted.

VI. The appellant made a further submission, received on 12 October 2023.

VII. In a communication dated 12 December 2024 the board set out its preliminary opinion on the appeal as follows. The subject-matter of claims 1 and 7 according to auxiliary request 1 seemed to involve an inventive step, Article 56 EPC, starting from D1 or D2. The board however had doubts whether claims 9 and 11 involved an inventive step starting from either D1 or D2. Neither auxiliary request 2 nor 3, nor their combination in 4, seemed capable, if admitted, of lending inventive step to the claims, in particular claims 9 and 11.

VIII. The respondent, with a submission, received on 14 February 2025, submitted a new auxiliary request 5 and a correspondingly amended description. The appellant did not make any substantive submissions in response.

IX. At the oral proceedings, held on 28 May 2025, the respondent submitted a corrected version of auxiliary request 5. The appellant requested that the decision under appeal be set aside and that the patent be revoked. The respondent requested that the appeal be dismissed and, as an auxiliary request, that the decision under appeal be set aside and the patent be maintained according to one of auxiliary requests 2 to 4 (received on 13 September 2021) or according to auxiliary request 5 (submitted in the oral proceedings). The board admitted auxiliary request 5 into the proceedings. At the end of the oral proceedings the board announced its decision.

X. The patent is being considered in the following form:

Description (auxiliary requests 1 to 4): paragraphs 1 to 18 and 20 to 77 of the patent specification and paragraph 19, received in the oral proceedings before the opposition decision.

Description (auxiliary request 5): paragraphs 2 to 18, 20 to 28 and 33 to 77 of the patent specification and paragraphs 1 and 19 filed with the letter of 14 February 2025.

Claims (received on 13 September 2021):
auxiliary request 1: 1 to 12.
auxiliary request 2: 1 to 12.
auxiliary request 3: 1 to 9.
auxiliary request 4: 1 to 9.

Claims (received on 28 May 2025):
auxiliary request 5: 1 to 8.

Drawings (all requests):
Pages 16 to 19 (figures 1 to 6) of the patent specification.

XI. The independent claims 1 and 7 of auxiliary request 5, which are the same as those of auxiliary request 1, read as follows, the labelling of the features of claim

1 having been submitted as D5 by the respondent with the submission of 15 September 2022:

"1.1 Method for access decision evaluation in a building automation and control system, the method comprising:

1.2 sending, from an accessing device (10) to an accessed device (20), an access request,

1.3 sending, from the accessed device (20) to a central decision evaluation apparatus (30), an evaluation request asking if the access request is granted or denied,

1.4 evaluating, at the central decision evaluation apparatus(30), the evaluation request using one or more central access control policies in order to reach a decision on if the access request is granted or denied,

1.5 deriving, at the central decision evaluation apparatus(30), from one or more central access control policies that was used for evaluation a device specific access policy,

1.6 sending, from the central decision evaluation apparatus(30) to the accessed device (20), the decision and the device specific access policy,

1.7 storing, at the accessed device (20), the device specific access policy; and

1.8.01 sending, from the accessing device (10) to the accessed device (20), a subsequent access request,

1.8.02 evaluating, at the accessed device (20), if the subsequent access request matches with the device specific access policy stored in the accessed device (20), if so,

1.8.03 deciding, at the accessed device (20), if the subsequent access request is granted or denied based on the device specific access policy."

"7. Access decision evaluation system in a building control system, the access decision evaluation system comprising: an accessing device (10), an accessed device (20) comprising a local memory (22) storing one or more device specific access policies, a matching point (24) and a policy decision point (26), and a central decision evaluation apparatus (30) comprising a database (33) of one or more central access control policies, an access policy decision point (34) and an access policy deriver (36), wherein the accessing device (10) is arranged to send an access request to the accessed device (20), and characterized in that the matching point (24) of the accessed device (20) is arranged to evaluate the access request to see if the access request matches with one of the one or more device specific access policies stored in the local memory (22), if so, the policy decision point(26) of the accessed device (20) is arranged to decide if the access request is granted or denied based on the matched device specific access policy, if not so, the accessed device (20) is arranged to send an evaluation request asking if the access request is granted or denied to the central decision evaluation apparatus (30), wherein the access policy decision point (34) of the central decision evaluation apparatus (30) is arranged to evaluate the evaluation request using one or more central access control policies in order to reach a decision on if the access request is granted or denied, wherein the access policy deriver (36) of the central decision evaluation apparatus (30) is arranged to derive from the one or more central access control policies that was used for the evaluation a derived device specific access policy, and wherein the central decision evaluation apparatus (30) is arranged to send the decision and the derived device specific access policy to the accessed device (20)."

XII. Independent claim 9 of auxiliary request 1 reads as follows:

"Central decision evaluation apparatus (30) in an access decision evaluation system comprising an accessing device (10), an accessed device (20) and the central decision evaluation apparatus (30), the central decision evaluation apparatus (30) comprising: a database (33) of one or more central access control policies, an access policy decision point (34) arranged to evaluate an evaluation request from the accessed device (20) using one or more central access control policies stored in the database (33) in order to reach a decision on if an access request being sent from the accessing device (10) to the accessed device (20) is granted or denied, and characterised in that the central decision evaluation apparatus (30) further comprises: an access policy deriver (36) arranged to derive from the one or more central access control policies that was used for the evaluation a device specific access policy, wherein the central decision evaluation apparatus (30) is arranged to send the decision and the device specific access policy to the accessed device (20) to enable the accessed device (20) to store the device specific access policy and thereby decide if a subsequent access request is granted or denied based on the device specific access policy."

XIII. Claim 9 of auxiliary request 2 differs from that of the previous request in the additional feature of the device-specific access policy "only comprising the relevant rules valid for the accessed device (20)". Claim 7 of auxiliary request 3 differs from claim 9 of the previous request in the following additional feature at the end: "wherein the access policy deriver (36) is further arranged to derive the device specific access policy with context attributes as variable to enable the accessed device (20) to evaluate subsequent access requests from the accessing device (10) under different contexts." Claim 7 of auxiliary request 4 differs from claim 7 of the previous request in combining the amendments of auxiliary requests 2 and 3. The claims according to auxiliary request 5 do not comprise an independent claim to a "central decision evaluation apparatus" or an "accessed device".

Reasons for the Decision

1. Admissibility of the appeal

In view of the facts set out at points I, III and IV above, the appeal fulfils the admissibility requirements under the EPC and is consequently admissible.

2. The admittance of auxiliary request 5, Article 13(2) RPBA

2.1 At the oral proceedings the appellant opponent objected for the first time to the admittance of auxiliary request 5, which resulted from deleting claims 9 to 12 of auxiliary request 1, on the basis that this request could have been filed earlier. The deletions responded to objections already raised by the opponent before the opposition division, namely that claims 9 and 11 were broader than 1 and 7. For instance, claim 11 did not set out a building automation and control system. These objections had been repeated in the statement of grounds of appeal; see [31,33,34]. Hence the new request should have been filed at the latest in response to the grounds of appeal. Only the deletion of claim 11 could be seen as a response to the grounds of appeal.

2.2 The respondent argued that objections concerning the access policy in claim 9 possibly being non-technical and the "central decision evaluation apparatus" in claim 11 covering any apparatus had only been raised by the board in its provisional opinion; see points 10.7.6, 10.7.7 and 10.7.12. Auxiliary request 5 was thus a timely response to the board's provisional opinion. The deletion of claims 9 to 12 had not shifted the focus of the proceedings, and there had been no reason to delete claims 9 and 11 before, since the appealed decision had treated all four independent claims as having essentially the same scope; see points 42-43.

2.3 The board finds that auxiliary request 5, in which claims 9 to 12 have been deleted vis-à-vis auxiliary request 1, constitutes an amendment to the respondent's case, Article 13(2) RPBA. The appellant had not objected to claim 9 on the basis of non-technicity, an objection raised by the board for the first time in its provisional opinion. The new request was thus a timely reaction to the provisional opinion which moreover simplified the case. The Board considers this to represent exceptional circumstances under Article 13(2) RPBA in accordance with established case law of the Boards (see Case Law of the Boards of Appeal of the EPO V.A.4.2.2 d) and 4.5.5 g)).

2.4 Consequently the board admitted auxiliary request 5.

3. The correction of auxiliary request 5

3.1 In the oral proceedings the board pointed out that, although the "track changes" version of auxiliary request 5 designated the last paragraph of the claims as claim 8, the numbering was missing in the "clean" version. The appellant submitted a corrected version of the claims with "8." added to the last paragraph, which the appellant did not object to.

3.2 The board allows the correction of claim 8 as an error of transcription, Rule 139 EPC, since the error and its correction are both immediately evident.

4. Summary of the invention

4.1 In the following the references are to the application as originally filed.

4.2 The invention relates to a building automation and control system (BACS) comprising access decision evaluation, i.e. deciding whether a certain device should be allowed to communicate with or otherwise interact with another device in the system; see page 1, lines 9 to 20, and page 3, lines 21 to 29.

4.3 The invention is aimed at improving the information security of such systems, in particular access control in the sense of authentication (who you are) and authorisation (what you are permitted to do); see page 3, lines 17 to 20. One limitation on improving access control is the delay (latency) such measures introduce between a user giving a command and the system reacting. The invention seeks to reduce latency by combining an initially centralised approach, which offers high scalability, with a subsequently distributed approach, which offers reduced latency; see page 2, line 23, to page 3, line 10. This has been referred to in this case as the "hybrid" approach.

4.4 As illustrated in figure 5, an "accessing device" (10) (defined on page 4, lines 4 to 8), for instance a smartphone, sends an "access request" (20) to an "accessed device" (defined on page 4, lines 9 to 13), for instance a lighting device or electronic lock. The accessed device in turn sends an "evaluation request" to a "central decision evaluation apparatus" (30) which decides, based on one or more "central access control policies", whether the access request is to be granted or denied. Figure 6 shows a sequence diagram of the information flows in the system. "Policies" are defined as a "set of criteria for the provision of access to resources"; see page 3, lines 30 to 31.

4.5 The central decision evaluation apparatus derives a device-specific access policy from one or more central access control policies and sends this, together with its grant/deny access decision, to the accessed device, the "device-specific access policy" being stored in the accessed device.

4.6 When the accessing device subsequently sends an access request to the accessed device, the latter checks whether the access request matches a stored device-specific access policy and, if so, decides whether to grant or deny the request, based on the stored device-specific access policy without reference to the central decision evaluation apparatus.

4.7 A key difference between the "distributed approach" to access control, shown in figures 1 and 2, and the "centralised approach", illustrated in figures 3 and 4, is that the latter has a separate central decision evaluation apparatus (30). The "hybrid" approach of the invention, shown in figures 5 and 6, combines the "distributed" and "centralised" approaches (see page 10, line 1, to page 14, line 15) in that it initially uses the "centralised" approach, but then switches to the "distributed approach".

4.8 Auxiliary request 2 adds the feature that the device-specific access policy only comprises rules valid for the accessed device, as disclosed on page 11, lines 29 to 33. Auxiliary request 3 refers to "context attributes". These are defined in the paragraph bridging pages 3 and 4 as, for example, location, time, and situation (emergency/normal); see also page 5, lines 1 to 5. Auxiliary request 4 combines the amendments in the previous two requests.

5. The four independent claims of auxiliary requests 1-4

5.1 According to the appellant, independent claims 9 and 11 do not set out the "hybrid approach". The respondent has disputed this.

5.2 The claims of auxiliary request 1 comprise an independent method claim 1 and a (with the exception of the term "automation") corresponding independent apparatus claim 7, both referring to a building control system and three key system components: an accessing device (10), an accessed device (20) and a central decision evaluation apparatus (30).

5.3 The two further independent apparatus claims are understood by the board to be broader than claim 7 in that they each only set out one key system component: a central decision evaluation apparatus (claim 9) and an accessed device (claim 11). Although claims 9 and 11 contain the expression "in an access evaluation system", the board understands this as merely *suitable for use* (emphasis by the board) in such a system. It is noted that otherwise claims 9 and 11 would essentially set out the same subject-matter as claim 7. Regarding claim 9, the board does not regard the fact that the access request was sent *from the accessing device* to the accessed device as limiting the features of the central decision evaluation apparatus, since it merely receives an evaluation request from the accessed device.

5.4 The discussion in this case has focussed on claims 1 and 9 of auxiliary request 1. For the purposes of a decision in this case there is no need to further consider claim 11, setting out an accessed device.

6. The board's understanding of the invention

6.1 The meaning of "access control"

According to page 8, lines 7 to 16, authentication, in particular mutual authentication between the accessing device (10) and the accessed device (20), is the first step of "access control". This establishes, amongst other things, the identity of the accessing device. Based on the identity of the accessing device, its privileges (authorizations) can be determined and access requests accordingly granted or denied. Authentication is not set out in the claims, but the board understands it to have implicitly already happened before access requests are processed.

6.2 The limitative effect in claim 1 of all requests of a method "for" access decision evaluation in a building automation and control system

6.2.1 The appellant has argued that the subject-matter of claim 1 is not limited by the expression "in a building automation and control system" and covers other methods, including that known from D1. The respondent has disagreed.

6.2.2 The board appreciates that the term "building automation and control system" is a rather broad, albeit a well-established one, but accepts the respondent's argument that a building automation and control system must be construed as comprising a plurality of distributed devices, such as locks and lighting devices being addressed by a plurality of addressing devices; see page 4, lines 9 to 13, of the application.

6.2.3 Hence the context in which the method is carried out, explicitly set out in claim 1, namely "in a building automation and control system", is indeed limiting on the method. So too are the terms "access decision evaluation".

6.3 The limitative effect in claim 7 of auxiliary requests 1, 2 and 5 and claim 6 of auxiliary requests 3 and 4 of the expression "in a building control system"

6.3.1 The expression "in a building control system" is understood as limiting the independent system claim, in the sense of requiring that the system be suitable for this purpose. It also requires that there can be a plurality N of accessing devices (such as smartphones) accessing a plurality M of accessed devices (such as locks).

6.3.2 The board notes that claims 9 and 11 (auxiliary requests 1 and 2) and 7 and 8 (auxiliary requests 3 and 4) do not set out either a building automation control system or a building control system.

6.4 The meaning of an "access control policy"

The description defines the expression "access control policy" as a "set of criteria for the provision of access to resources"; see page 3, lines 30 to 31. The board understands the expression broadly to mean any information forming the basis for a decision to either grant or deny an access request. The criteria embodied by a policy could be purely commercial in nature and not technical. For instance, a policy could deny access to accessing devices from a certain manufacturer or country. This is particularly relevant to the assessment of claim 9 of auxiliary requests 1 to 4.

6.5 The meaning of a "device-specific access policy"

6.5.1 According to page 5, lines 13 to 18, the accessed device has a fixed amount of memory for storing a limited number of device-specific access policies. These are collectively referred to as a "device-specific access policy".

6.5.2 In the oral proceedings the respondent argued that the device-specific access policy, set out in all independent claims of all requests, could be a list of the identities of accessing devices to which access was to be granted. The board can find no disclosure of such a device-specific access policy in the patent, nor have the claims been restricted to this case.

6.5.3 Generally speaking, the term "device-specific" could be understood to relate to either the "accessing device", or the "accessed device", or indeed to both, as a policy sets out which accessing device is granted access to which accessed device. However, in view of the context of access control and the aim of achieving decentralised access control, the board considers that the "device-specific" access policy must be construed as the access policy to be enforced by a specific accessed device vis-à-vis one or more accessing devices.

6.6 The meaning of "matching point" and "policy decision point"

Claim 7 of auxiliary requests 1, 2 and 5 and claim 6 of auxiliary requests 3 and 4 refer to a "matching point" (24) and a "policy decision point" (26). In this context, the board understands a "point" to be a "unit".

7. Added subject-matter, Article 123(2) EPC

7.1 According to the appealed decision, the patent amended according to auxiliary request 1 complied with Article 123(2) EPC; see point 13.

7.2 The appellant has not raised any objections under Article 123(2) EPC against auxiliary requests 1 to 5.

7.3 In particular, concerning auxiliary request 5, the board also sees no reason to object under Article

123(2) EPC and finds that the patent amended according to auxiliary request 5 satisfies Article 123(2) EPC.

8. Document D1 (US 7 002 468 B2)

8.1 D1 relates to controlling access by a portable medical monitoring device via a communications link to a medical monitoring system, so that only a "properly authorized" patient can use the system, thereby incurring costs; see column 1, lines 50 to 53.

8.2 The system is illustrated in figure 2. For access by a medical monitoring device system (52), comprising a medical monitoring device (54) and a base station (56), to be "properly authorized", a formal check is done on access data entered into the medical monitoring device system (52) (see figure 2; keypad 66 and column 4, lines 61 to 67), and the patient's health-care-benefit payer (74), referred to as a "third-party source" (72) must agree (also referred to as "authorizing" and "signing off"; see column 1, lines 31 to 34, column 2, lines 7 to 12, column 4, lines 33 to 48, and column 6, lines 47 to 50. Access to the system may further depend on data in a variety of databases (71) accessible by the central unit 58; see column 2, lines 13 to 17, and column 4, lines 33 to 36. A sub-process (30) may also make a local copy at the central unit (58), i.e. cache, a third party's database of authorisation information; see column 5, lines 52 to 61.

8.3 If the formal check of the access data is successful, then the medical monitoring device system (52) establishes a connection with the central unit (58) and the two co-operatively determine whether the monitoring device is to be granted access, termed "activating" the medical monitoring device; see column 5, lines 21 to

37. The "activation determination process" (see figure 1; 26) comprises obtaining third-party authorization (30) from third-party sources (72), such as a financial source (74) or a medical professional (76) (see column 6, lines 22 to 34), and/or databases (71); see column 5, lines 55 to 60. Based on the results of the activation determination process, the activation decision is typically made at the central unit (58); see column 6, lines 58 to 62. In the case of activation, an "activation signal" is sent by the central unit (58) to the medical monitoring device system (52) to activate it; see column 7, lines 1 to 6.

8.4 The board regards the "medical monitoring system 52" in D1 as an accessing device in the sense of the claims. The part of the central unit (58) in figure 2 communicating with the medical monitoring system (52) (referred to as the "left" part in the following) is regarded as an "accessed device", and the rest of the central unit (58) communicating with the third-party sources (72,74,76,78) is regarded as a "central decision evaluation apparatus" in the sense of the claims.

8.5 In the board's view, "activation" in D1 falls under the granting of "access" in the claims. In D1 "access" refers to ensuring that only authorized patients can connect their monitoring device (figure 2; 54) to the hospital's monitoring system and incur charges; see column 1, lines 50 to 66, and column 7, lines 1 to 6.

8.6 Where is the activation decision made in D1?

8.6.1 According to the appellant, D1 distinguished between "activation" at the central unit and "authorization" at the third party. However, while the central unit 58 typically made the final activation decision, an *access authorization* was performed by, and obtained from, one or more third parties. In the case of a single third party, known, for instance, from column 6, lines 29 to 30, the activation decision was made by *that* third party, namely the medical source (76); see also column 6, lines 22 to 25, regarding the authorization by the "financial source" 74.

8.6.2 According to the respondent, the third-party sources (72) never took a decision; they merely provided input to the base station (58), so that it could take a decision; see column 1, line 66, to column 2, line 2, column 5, lines 38 to 42, and column 7, lines 1 to 6. Considering the central unit (58) as an "accessed device", D1 did not disclose either a decision or a device-specific access policy being sent to the accessed device.

8.6.3 The board finds that the activation decision is taken in the central unit (58) (see figure 1; step 32 and column 6, lines 58-59), since activation not only involves obtaining a "sign-off" from one or more third-party sources (step 30), it also involves initially evaluating the identification data entered by the patient on their keyboard (66)(step 28).

8.7 Does D1 disclose a device-specific access policy?

8.7.1 The appellant has argued that D1 does not disclose the copying of a complete database to a local copy in the central unit (58); see column 5, line 55, to column 6, line 2, and column 6, lines 18 to 22. The local copy was consequently comparable to a device-specific access policy in the claims.

8.7.2 The respondent has argued that only updates to the third-party database were added to the local copy; see column 5, line 62, to column 6, line 2.

8.7.3 The board finds that the updating of a local copy of a third-party database in the central unit does not involve a *device-dependent* selection of authorisation data and hence does not qualify as a device-dependent access policy.

8.7.4 In the oral proceedings the appellant also argued that D1 disclosed not granting access to faulty monitoring devices that had been taken out of service for repair; see column 6, lines 41 to 46. This constituted a device-specific access policy in the sense of the claims. Moreover, in the context of the invention, an "accessed device" could, for instance, be an electronic lock or a lighting device; see page 4, lines 9 to 13, and paragraphs [40, 51-53] of the patent.

8.7.5 The respondent argued that, according to the invention in the case of the lock, only data relating to accessing devices authorized to open that particular lock were transferred to the accessed device to form a (accessed) device-specific access policy.

8.7.6 The board regards a list of accessing devices that have been taken out of service as not specific to the accessed device in D1. Hence, again, the appellant has not established that D1 discloses a device-specific access policy being sent from a central decision evaluation apparatus to an accessed device.

8.7.7 In the terms of claim 1 of auxiliary request 5, which is the same as that of auxiliary request 1, D1 discloses a method for access decision evaluation comprising: sending, from an accessing device (52) to an accessed device (58, left part), an access request, sending, from the accessed device (58, left part) to a central decision evaluation apparatus (58, rest), an evaluation request asking if the access request is granted or denied, evaluating, at the central decision evaluation apparatus, the evaluation request using one or more central access control policies (see database 71) in order to reach a decision on whether the access request is granted or denied and sending the decision from the central decision evaluation apparatus to the accessed device. The same applies *mutatis mutandis* to claim 7 of auxiliary request 5, which is the same as that of auxiliary request 1.

8.7.8 Turning to claim 9 of auxiliary request 1, as understood by the board, D1 discloses a central decision evaluation apparatus (58, rest) suitable for use in an access decision evaluation system comprising an accessing device (52), an accessed device (58, left) and the central decision evaluation apparatus (58, right), the central decision evaluation apparatus (30) comprising: a database (71) of one or more central access control policies, an access policy decision point arranged to evaluate an evaluation request from the accessed device using one or more central access control policies stored in the database (71) in order to reach a decision on whether an access request is granted or denied.

9. Document D2 (US 2005/0144186 A1)

9.1 According to the decision (point 30), the opponent initially relied on a first "feature mapping" in D2, focussing on figures 9 and 15 and paragraphs [23-24, 56, 68, 91, 146, 167, 168, 197-198, 200-201, 231, 225 and 253]; see notice of opposition, page 13 ff. As D2 only has 256 paragraphs, it seems that this mapping relies on passages scattered throughout D2, rather than relating to a particular embodiment in D2. The opponent later changed tack and relied on a second "feature mapping" in D2, termed the "alternative mapping" in the decision; see point 34. According to the decision, this mapping focussed on figures 10 to 12 and paragraphs [167, 170, 172 and 225]. This part of D2 relates to "strategic data caching" and the subscriptions mentioned in paragraphs [164 to 172].

9.2 The appellant has argued that the role of the connection server (see figure 15; 14) in the second embodiment in D2 was most relevant to the claimed subject-matter; see paragraph [163] and figure 11. The provision of specific rules for the accessed device, set out in auxiliary requests 2 to 4, was known from paragraph [55]. The addition of context information, set out in auxiliary requests 3 and 4, was known from the time stamps in D2; see [170]. Moreover, while the security server (58)(see figure 15) was only optional, the connection server (14) was essential for enabling and managing subscriptions to particular devices, active subscriptions being key to enabling request decisions.

9.3 According to the respondent, in D2 the decision to admit a new computer was taken by the security server (58), not the connection server (14); see [115] and figure 15. The subscriptions mentioned in D2 had no bearing on granting or denying access; see [226].

9.4 The board's view on D2

9.4.1 In the board's view, D2 relates to distributed data storage and access; see title. Data is cached in the cache memories of storage devices. Communications over the network are managed by connection servers which handle *inter alia* authentication, authorization and encryption; see abstract.

9.4.2 D2 addresses the problem that computer applications often require high-bandwidth, low-latency access to data storage. Whilst this can be readily provided in a local area network (LAN), high-bandwidth and low-latency are more difficult to achieve in a wide area network (WAN), such as the internet; see [3,4].

9.4.3 The approach used in D2 is for each local computer (see [91]) to have a local cache in a local storage device (see [98]) and the remote computer (see [89]) to have a remote cache in a remote storage device; see [24,34]. Each cache is managed by a cache management application; see [38]. One cache management application may request file overhead information from another cache management application and store the result locally with a time stamp; see [39, 40].

9.4.4 When one computer requests a file, the local cache manager checks whether the file is cached locally. If not, then the cache manager requests the file from a remote cache manager; see [48]. The remote file manager searches for the file and any differential data (see [103,104]), termed "delta" and "inverse delta" files, necessary for updating the file to its current state. Sending a file in this way reduces the bandwidth required; see [50,51].

9.4.5 Figure 10 - the start of the "second mapping" - shows a network of three computers (72,74,76) and a database (DB 52) linked by a connection server (14) which ensures that communication between the computers is *inter alia* authenticated, authorized and encrypted; see [153]. The strategic cache management used in the network is illustrated in figure 11, showing two computers (72,74) linked by a WAN, so that computer 72 can access the storage device (18b) of the other computer 74; see [157]. Application 72a on the first computer makes access requests to user module 72su which manages data caching from a data module 74sd in the second computer; see [157], last sentence.

9.4.6 Figure 12 (see [163,167]) illustrates the process by which a computer checks its local cache to see whether "file overhead" information, defined in paragraph [164] as representing the file structure and file parameters of a storage device for another computer, is available and valid and, if not, sending a subscription request for file updates from the other computer (1206). The other computer checks whether the requestor is authorized (see [168]) to receive this information and, if so, registers (1212) the subscription request, from then on sending file updates (1214) to the subscribed computer. Such file access requests are also possible for file data; see [164,166]. File subscriptions optimise (i.e. reduce; see [170]) network bandwidth requirements and latency; see [165]. Consequently subsequent requests for the subscribed file can be satisfied by the local cache; see page 17, first sentence. Network bandwidth is reduced, thus also reducing latency, because the first computer no longer has to send a request for a copy or updates of a subscribed file to the second computer, since the second computer automatically sends file updates which are cached in the first computer, every time the file changes; see [170].

9.4.7 Figure 15 illustrates a computer network comprising computers (110, 120) in private networks accessing a storage device (154) via a connection server (14) in another private network (gateway 140) using a security server (58); see [198]. The security server (58) is only accessed for authentication purposes at the beginning of a session. During a session, remote computers access the gateway by communicating with the connection server (14) directly, saving bandwidth; see [199]. Subscriptions can be managed and set at the connection server (14) and its associated database (52); see [226, 2nd sentence]. The system allows a user to work securely with data stored on remote devices as if the data were stored locally on their computer; see [250]. The system can be used in the home ([252]) or in factory automation; see [253].

9.4.8 The board finds that, although the various systems known from D2 disclose access rights being determined at an accessed device, a copy of those rights then being cached at the accessing device (see, for example, figure 11 and [170], 2nd sentence) or at a central server (58) (see figure 15 and [198], lines 17 to 21), D2 does not disclose an access request being initially passed as an evaluation request by the accessed device to a central decision evaluation apparatus which decides and returns a device-specific policy to the accessed device. The systems known from D2 have a fixed location for deciding on access requests, even if copies of those rights are then transferred to the accessing device.

9.4.9 In the terms of claim 1 of auxiliary request 5, which is the same as that of auxiliary request 1, D2 discloses (see figure 15) a method for access decision evaluation in a building automation and control system (see [252,253]), the method comprising: sending, from an accessing device (110) to an accessed device (gateway 140), an access request, evaluating, at a central decision evaluation apparatus (security server 58), an evaluation request using one or more central access control policies in order to reach a decision on if an access request is granted or denied, deriving, at the central decision evaluation apparatus, from one or more central access control policies that were used for evaluation a device specific access policy, and sending, from the accessing device (110) to the accessed device (140), a subsequent access request. The same applies *mutatis mutandis* to claim 7 of auxiliary request 5, which is the same as that of auxiliary request 1.

9.4.10 In the terms of claim 9 of auxiliary request 1, D2 discloses a central decision evaluation apparatus (58) suitable for use in an access decision evaluation system comprising an accessing device (110), an accessed device (140) and the central decision evaluation apparatus (58), the central decision evaluation apparatus (58) comprising: a database of one or more central access control policies, an access policy decision point arranged to evaluate an evaluation request from the accessed device using one or more central access control policies stored in the database in order to reach a decision on whether an access request is granted or denied.

10. Inventive step, Article 56 EPC

10.1 Claim 9 of auxiliary request 1 starting from D1

10.1.1 The subject-matter of claim 9 of auxiliary request 1 differs from the disclosure of D1 in further comprising:

a. an access policy deriver arranged to derive from the one or more central access control policies that were used for the evaluation a device specific access policy,

b. wherein the central decision evaluation apparatus is arranged to send the decision and the device specific access policy to the accessed device (20).

10.1.2 In the oral proceedings the respondent argued that sending the decision and the device specific access policy to the accessed device (feature "b") had the technical effect of enabling the hybrid approach, since the accessed device could only decide itself if it had the device specific access policy. It was moreover not usual to send rules to another system element.

10.1.3 The appellant argued that the features of the central decision evaluation apparatus were not limited by its effect on another system element, namely enabling the accessed device to decide. Moreover the access policy could be based on purely financial rather than technical considerations.

10.1.4 The board finds that sending the decision and the device specific access policy to the accessed device is a necessary but insufficient condition for the presence of a technical effect in the central decision evaluation apparatus, since the criteria in a policy need not be technical. The derivation of a device-specific access policy and the taking of a decision based on it can be non-technical steps which are thus unable to lend inventive step to the claim. For instance, sending the derived policy together with the decision could merely serve the non-technical purpose of informing the accessed device about the reasons for the decision taken.

10.1.5 Hence the subject-matter of claim 9 lacks inventive step in view of D1.

10.2 Claims 1 and 7 of auxiliary request 5 starting from D1

10.2.1 These claims are the same as those of auxiliary request 1, discussed in the decision. According to point 19 of the decision, the subject-matter of claim 1 differed from the disclosure of D1 in that:

i. the method for access decision evaluation is a method in a building automation and control system (feature 1.1),

ii. the evaluation request from the accessed device to the central decision evaluation apparatus is for asking if the access is granted or denied, that the central decision evaluation apparatus evaluates the request to reach a decision and finally sends the decision to the accessed device (parts of features 1.3, 1.4, 1.6),

iii. the central decision evaluation apparatus derives a device specific access policy and sends it to the accessed device and that further the accessed device stores this device specific access policy and uses it for evaluation and deciding on a subsequent request (features 1.5, 1.6 (part), 1.7, 1.8.02, 1.8.03).

10.2.2 According to the decision, regarding difference "i", the method was defined as being for access decision evaluation in a building automation and control system. This feature could not be disregarded; the method was to be performed in the context of such a system. However, as nothing in the claim was linked to anything particular in a building automation and control system, no restriction was put on the terms and steps of the claim by the feature of a building automation and control system. The terms "accessing device" and "accessed device" were generic and not limited by the definitions in the description. Such definitions were only to be taken into account in case of ambiguity.

10.2.3 Turning to difference "ii", features 1.3, 1.4 and 1.6 of claim 1 were not disclosed in D1, since the third parties did not take a decision, but only sent their input to a final decision. In general, no single third party could take such a decision alone; the final decision was taken by the central unit 58; see e.g. column 6, lines 58-60, and step 32 in figure 1 and column 7, lines 1-6.

10.2.4 Regarding difference "iii", the decision found that D1 did not disclose the derivation of a device-specific access policy from central access policies because copying a complete database in D1 (see column 5, lines 55 to 58) was not the same as selecting a specific entry or set of entries from the database.

10.2.5 Starting from D1, the method of claim 1 and the system of claim 7 involved an inventive step, since each set out the decision being taken by the central decision evaluation apparatus, i.e. difference "ii" above.

10.2.6 The respondent has argued that D1 is not an appropriate starting point ("realistic springboard") for assessing inventive step. The board disagrees, since inventive step can be assessed starting from any prior art disclosure. The question to be answered is whether the skilled person would have arrived at the claimed subject-matter from that starting point in an obvious manner.

10.2.7 The appellant has argued, referring to figure 2 of D1, that the third party sources (72-78) were a "central decision evaluation apparatus" in the sense of claim 1. The claim only required one access policy, and this was known from the examples of financial, medical and other access policies disclosed in column 6, lines 18-46. Hence features 1.3 and 1.4 were known from D1. A local copy (71) of a third-party's authorisation database was known from column 5, line 55 to column 6, line 2, and was available to central unit 58. Claim 1 did not set out any features relating to a building automation and control system; it merely set out a method "suitable for" a building automation and control system. The objective technical problem starting from D1 was to apply the method of D1, albeit in the medical field, to other automatic activation systems.

10.2.8 The board finds that the subject-matter of claim 1 of auxiliary request 5 differs from the disclosure of D1 in the following features:

a. the method takes place in a building automation and control system;

b1. deriving, at the central decision evaluation apparatus, a device-specific access policy from one or more central access control policies that were used for evaluation;

b2. sending the device-specific access policy from the central decision evaluation apparatus to the accessed device and storing it there and

b3. sending, from the accessing device to the accessed device, a subsequent access request, evaluating, at the accessed device, whether the subsequent access request matches the device-specific access policy stored in the accessed device, if so, deciding, at the accessed device, whether the subsequent access request is granted or denied based on the device-specific access policy.

10.2.9 The board does not accept the objective technical problem proposed by the appellant. From the perspective of D1, this formulation would require the skilled person to start from a known solution in a medical context and, in a way, to look for a problem, namely an automation domain which might profit from that solution. However, a central assumption of the problem-solution approach is that the skilled person starts with a problem and looks for a solution to it. The board also notes that the appellant has not justified the proposed objective technical problem in any other way.

10.2.10 The board finds that in claim 1 features "b1" to "b3", representing the so-called "hybrid" approach, would not have been obvious to the skilled person starting from D1. More specifically, although the hybrid approach, i.e. delegating the access control decisions to the accessed devices, has a clear advantage in a building automation and control system, which the board accepts (see above, point 6.2.2) must be construed as having a large number of "accessed devices" such as locks or lighting devices, no such advantage is apparent in the system of D1 in which there is only one, central accessed device. Furthermore, the skilled person would also have no reason to try applying the solution of D1 to such a building automation and control system. Inversely, it has not been argued that, and it is not apparent to the board why, a skilled person starting from, and addressing a problem in, a generic building automation and control system would look for a solution in a medical automation system such as that of D1.

10.2.11 Hence the subject-matter of claim 1 involves an inventive step in view of D1. The same applies *mutatis mutandis* to claim 7.

10.3 Claims 1 and 7 of auxiliary request 5 starting from D2

10.3.1 These claims are the same as those of auxiliary request 1, discussed in the decision. According to the decision (point 36), the subject-matter of claim 1 differed from the disclosure of D2 in differences "ii" and "iii" (but not "i"), as follows:

i. the method for access decision evaluation is a method in a building automation and control system (feature 1.1),

ii. the evaluation request from the accessed device to the central decision evaluation apparatus is for asking if the access is granted or denied, that the central decision evaluation apparatus evaluates the request to reach a decision and finally sends the decision to the accessed device (parts of features 1.3, 1.4, 1.6).

10.3.2 Starting from D2 led to the same conclusion as for D1; apart from difference "i" above (feature 1.1), the differentiating features over the disclosure of D2 were the same.

10.3.3 In view of the above analysis, the board finds that the subject-matter of claim 1 differs from the disclosure of D2 in the following features:

a1. sending, from the accessed device to a central decision evaluation apparatus, the evaluation request asking if the access request is granted or denied,

a2. sending, from the central decision evaluation apparatus to the accessed device, the decision and the device-specific access policy, the policy being stored at the accessed device,

b. evaluating, at the accessed device, if the subsequent access request matches with the device-specific access policy stored in the accessed device and, if so, deciding, at the accessed device, whether the subsequent access request is granted or denied based on the device specific access policy.

10.3.4 The board finds that in claim 1 features "a2" and "b", relating to deriving a device-specific access policy for use by the accessed unit to decide on access requests (the so-called "hybrid" approach), would not have been obvious to the skilled person starting from D2, the same applying for analogous reasons to claim 7.

10.4 Claim 9 of auxiliary request 2 and claim 7 of auxiliary requests 3 and 4

10.4.1 The appellant has argued that auxiliary requests 2 to 4 do not add any novel or inventive features to *inter alia* claim 9. The provision of an authorisation for a specific device, set out in auxiliary requests 2 and 4, was known from D1 and D2, and the addition of context information, set out in auxiliary requests 3 and 4, was known from the time stamps in D2.

10.4.2 The respondent has argued, regarding the second auxiliary request, that the feature added to *inter alia* claim 9, namely that the device-specific access policy "only compris[es] the relevant rules for the accessed device (20)" was based on page 11, line 31, and reducing the amount of data in the policy. Regarding the third auxiliary request, the feature added *inter alia* to claim 7 that "the step of deriving the device specific access policy further comprises deriving the device specific access policy with context attributes as variable to enable the accessed device (20) to evaluate subsequent access requests from the accessing device (10) under different contexts" was based on original claims 3 and 11. As to the fourth auxiliary request, the claims contained the amendments of the two previous requests, the arguments for those requests also applied to this request.

10.4.3 The board finds that neither auxiliary request 2 nor 3, nor their combination in 4 introduces amendments lending inventive step to claim 9 of auxiliary request 2 or claim 7 of auxiliary requests 3 and 4. In auxiliary requests 2 and 4 the restriction of the device-specific access policy to only the relevant rules valid for the accessed device seems to be a usual matter for the skilled person of conserving memory space and network bandwidth and, given that the policy need not be technical, the additional feature lacks technical character and is thus unable to contribute to inventive step. Turning to auxiliary requests 3 and 4, the derivation of the device-specific access policy using context attributes as variables lacks technical character, since the policy itself need not be based on technical considerations.

10.4.4 Hence the subject-matter of claim 9 of auxiliary request 2 and claim 7 of auxiliary requests 3 and 4 does not involve an inventive step, Article 56 EPC.

11. Summary of the allowability of the respondent's substantive requests

11.1 Auxiliary requests 1 to 4 are not allowable because the subject-matter of claim 9 (auxiliary requests 1 and 2) and claim 7 (auxiliary requests 3 and 4) does not involve an inventive step, Article 56 EPC, starting from D1.

11.2 Auxiliary request 5 is allowable because the subject-matter of claims 1 and 7, the only independent claims, involves an inventive step, Article 56 EPC, starting from either D1 or D2. Moreover the patent amended according to auxiliary request 5 complies with Article 123(2) EPC regarding added subject-matter.

Order

For these reasons it is decided that:

The decision under appeal is set aside. The case is remitted to the opposition division with the order to maintain the patent as amended in the following version:

Description:
Paragraphs 2 to 18, 20 to 28 and 33 to 77 of the patent specification and paragraphs 1 and 19, filed with the letter of 14 February 2025.

Claims:
No. 1 to 8 according to auxiliary request 5, received during oral proceedings before the board of appeal on 28 May 2025.

Drawings:
Figures 1 to 6 of the patent specification.

The Registrar: The Chairman:

K. Götz-Wein M. Müller

Decision electronically authenticated