Internal distribution code:

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

Datasheet for the decision of 30 September 2025

Case Number: T 0405/24 - 3.5.05

Application Number: 16840343.4

Publication Number: 3395043

IPC: H04L29/06

Language of the proceedings: EN

Title of invention:
Rule-based network-threat detection for encrypted communications

Patent Proprietor:
Centripetal Limited

Opponents:
Cisco Systems GmbH
Cisco Systems, Inc.

Headword:
Correlating network-threat indicators/CENTRIPETAL

Relevant legal provisions:
EPC Art. 123(2)
RPBA 2020 Art. 12(6), 13(2)

Keywords:

Added subject-matter - auxiliary requests 1 to 7 and 9 to 15 (yes)
Admittance of non-admitted auxiliary request 8 (no): no erroneous exercise of discretion by the opposition division
Admittance of claim request filed during oral proceedings before the board - auxiliary request 2b (no): no "exceptional circumstances" justified with cogent reasons

Decisions cited:

G 0001/24, T 0367/20, T 0945/20, T 0470/21, T 2034/21, T 0193/22, T 2048/22

Catchword:

As to the applicability of the conclusions of G 1/24 to the assessment of compliance with Article 123(2) EPC, see point 1.2.3 of the Reasons.

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 0405/24 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 30 September 2025

Appellant: (Patent Proprietor)	Centripetal Limited Galway Technology Centre Mervue Business Park Galway (IE)
Representative:	MFG Patentanwälte Meyer-Wildhagen Meggle-Freund Gerhard PartG mbB Amalienstraße 62 80799 München (DE)
Respondent I: (Opponent 1)	Cisco Systems GmbH Parkring 20 85748 Garching (DE)
Respondent II: (Opponent 2)	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 (US)
Representative:	Bardehle Pagenberg Partnerschaft mbB Patentanwälte Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 29 February 2024 revoking European patent No. 3395043 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	J. Eraso Helguera
	C. Heath

Summary of Facts and Submissions

I. The appeal was filed by the proprietor against the decision of the opposition division to revoke the opposed patent under Article 101(2) and 101(3)(b) EPC for added subject-matter (Article 123(2) EPC) or extension of scope of protection (Article 123(3) EPC).

II. Oral proceedings before the board were held on 30 September 2025. The final requests of the parties were:

- The proprietor (appellant) requested, as its **main request**, that the decision under appeal be set aside and that the oppositions be rejected, or, in the alternative, that the patent be maintained in amended form on the basis of one of **sixteen auxiliary requests**, namely, auxiliary requests 1 to 8, 2b and 9 to 15. Auxiliary request 2b was filed for the first time during the oral proceedings before the board. The other claim requests underlie the decision under appeal.

- The opponents (respondents) requested that the appeal be dismissed.

At the end of those oral proceedings, the board announced its decision.

III. Claim 1 as granted (**main request**) reads as follows:

"A method comprising:

receiving, by a packet-filtering system (200) configured to filter packets in accordance with a

plurality of packet-filtering rules corresponding to a plurality of network-threat indicators, a plurality of packets;
identifying packets comprising unencrypted data, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host;
determining identified packets comprising unencrypted data that correspond to at least one of the plurality of the network-threat indicators;
generating, based on the plurality of packet-filtering rules, log data of the identified packets comprising unencrypted data that correspond to at least one of the plurality of the network-threat indicators;
identifying packets comprising encrypted data; and
correlating, based on the log data of the identified packets comprising unencrypted data that correspond to at least one of the plurality of network-threat indicators, packets comprising encrypted data that correspond to at least one of the plurality of network-threat indicators; and
routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality network-threat indicators."

Claim 1 of **auxiliary request 1** (labelled "Auxiliary Request 1") differs from claim 1 as granted in:

- the replacement of the phrase "and correlating, based on the log data" by the wording "correlating, thereby determining, based on the log data"

- the insertion of the phrase "comprising encrypted data" right before the wording "to a proxy system".

Claim 1 of **auxiliary request 2** (labelled "Auxiliary Request 2") differs from claim 1 as granted in:

- the insertion of the phrase "determining, by" right before the term "correlating"
- the insertion of the phrase "comprising encrypted data" right before the phrase "to a proxy system".

Claim 1 of **auxiliary request 3** (labelled "Auxiliary Request 3") differs from claim 1 as granted in:

- the insertion of the phrase "with the identified packets comprising unencrypted data" right before the wording "; and routing"
- the insertion of the phrase "comprising encrypted data" right before the phrase "to a proxy system".

Claim 1 of **auxiliary request 4** (labelled "Auxiliary Request 4") differs from claim 1 of auxiliary request 3 in:

- the insertion of the phrase "that correspond to at least one of the plurality of network-threat indicators" right after the phrase "with the identified packets comprising unencrypted data".

Claim 1 of **auxiliary request 5** (labelled "Auxiliary Request 5") differs from claim 1 of auxiliary request 4 in:

- the deletion of the term "and" right before the term "correlating"

- the insertion of the phrase "to determine whether the identified packets comprising encrypted data correspond to at least one of the plurality of network-threat indicators" right after the phrase "that correspond to at least one of the plurality of network-threat indicators".

Claim 1 of **auxiliary request 6** (labelled "Auxiliary Request 6") differs from claim 1 as granted in:

- the deletion of the term "and" right before the term "correlating",
- the insertion of the phrase "filtering the packets comprising encrypted data that correspond to at least one of the plurality of network-threat indicators;" right before the wording "and routing"
- the insertion of the word "the" right before the phrase "filtered packets to a proxy system".

Claim 1 of **auxiliary request 7** (labelled "Auxiliary Request 7") differs from claim 1 as granted in:

- the replacement of the wording "and correlating" by the phrase "correlating packets comprising encrypted data with one or more packets comprising unencrypted data previously determined to comprise data corresponding to at least one of the plurality of network threat indicators, including correlating",
- the insertion of the phrase ", thereby determining that the packets comprising encrypted data correspond to the at least one of the plurality of network threat indicators" right before the wording "; and routing"
- the insertion of the wording "comprising encrypted data" right before the phrase "to a proxy system".

Claim 1 of **auxiliary request 8** (labelled "New Auxiliary Request 2a") differs from claim 1 as granted in:

- the replacement of the phrase "and correlating" by the phrase "determining that the packets comprising encrypted data comprise data corresponding to the network-threat indicators, by correlating the packets comprising encrypted data with one or more packets comprising unencrypted data previously determined to comprise data corresponding to at least one of the plurality of network threat indicators; correlating"
- the replacement of the phrase "filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality network-threat indicators" by the phrase "filtered packets, being the determined identified packets, to a proxy system based on the determination that the filtered packets comprise unencrypted data that corresponds to at least one of the plurality of network-threat indicators".

Claim 1 of **auxiliary request 2b** (labelled "New Auxiliary Request 2b") differs from claim 1 as granted in:

- the insertion of the phrase "with one or more packets comprising unencrypted data previously determined to comprise data corresponding to at least one of the plurality of network threat indicators" right before the phrase "; and routing"
- the replacement of the phrase "filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality network-threat indicators" by the wording "filtered packets, being

the determined identified packets comprising unencrypted data, to a proxy system based on the determination that the filtered packets comprise unencrypted data that corresponds to at least one of the plurality of network-threat indicators".

Claim 1 of **auxiliary request 9** (labelled "Auxiliary Request 8") differs from claim 1 as granted in:

- the insertion of the phrase "determining that the packets comprising encrypted data correspond to at least one of the plurality of network-threat indicators by" right before the term "correlating"
- the insertion of the phrase "with one or more of the identified packets comprising unencrypted data previously determined to comprise data" right before "that correspond to at least one of the plurality of network-threat indicators"
- the insertion of the phrase "comprising encrypted data" right before the phrase "to a proxy system".

Claim 1 of **auxiliary request 10** (labelled "Auxiliary Request 9") differs from claim 1 of auxiliary request 7 in:

- the insertion of the phrase ", wherein
  the plurality of packet-filtering rules indicate:
  one or more network addresses for which encrypted communications should be established via the proxy system, and
  one or more network addresses for which encrypted communications should not be established via the proxy system; and
  the packet-filtering system is configured to route the one or more of the packets comprising unencrypted data to the proxy system based on a

determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications should be established via the proxy system"

at the end of the claim.

Claim 1 of **auxiliary request 11** (labelled "Auxiliary Request 10") differs from claim 1 of auxiliary request 6 in:

- the insertion of the phrase "thereby determining," right before the phrase "based on the log data".

Claim 1 of **auxiliary request 12** (labelled "Auxiliary Request 11") differs from claim 1 as granted in:

- the insertion of the phrase ", wherein at least one of the plurality of network-threat indicators comprises a domain name" right before the expression "; identifying packets"
- the insertion of the phrase ", wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server" right after the phrase "a second host"
- the deletion of "and" right before "correlating"
- the insertion of the wording ", wherein the correlating comprises determining that the one or more handshake messages comprise the domain name; responsive to determining that the one or more handshake messages comprise the domain name, at least one of dropping or logging the packets

comprising unencrypted data" right before the phrase "; and routing".

Claim 1 of **auxiliary request 13** (labelled "Auxiliary Request 12") differs from claim 1 as granted in:

- the insertion of the phrase ", wherein at least one of the plurality of network-threat indicators comprises a domain name" right before "; identifying packets"
- the insertion of the phrase ", wherein the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, wherein the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server" right after the phrase "a second host"
- the replacement of the phrase "; and routing" by the phrase ", wherein the correlating comprises determining that the one or more handshake messages comprise the domain name, and wherein the correlating comprises determining that the at least one hello message or certificate message comprises the domain name; routing"
- the addition of the wording "; and responsive to determining that the one or more handshake messages comprise the domain name, at least one of dropping or logging the packets comprising unencrypted data" at the end of the claim.

Claim 1 of **auxiliary request 14** (labelled "Auxiliary Request 13") differs from claim 1 as granted in:

- the deletion of the word "and" right before the term "correlating"
- the addition of ", wherein
  at least one of the plurality network-threat indicators comprise a domain name; and
  the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name: system, DNS, query or a reply to the DNS query; and
  the method further comprising: determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name, wherein:
  the identified packets comprising unencrypted data that correspond to at least one of the plurality of the network-threat indicators comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query; and
  the correlating further comprises determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses"

at the end of the claim.

Claim 1 of **auxiliary request 15** (labelled "Auxiliary Request 14") differs from claim 1 as granted in:

- the deletion of the word "and" right before the term "correlating"
- the insertion of the phrase
  "wherein the packets comprising unencrypted data comprise a certificate message for an encrypted communication session;
  the method further comprises at least one of

dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules;"

right before the wording "and routing".

Reasons for the Decision

1.1 MAIN REQUEST (PATENT AS GRANTED)

Claim 1 as granted comprises the following limiting features (outline based on the one used in the decision under appeal):

1. A method comprising:
1.1 receiving, by a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules corresponding to a plurality of network-threat indicators, a plurality of packets;
1.2 identifying packets comprising unencrypted data,
1.2.1 wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host;

1.3 determining identified packets comprising unencrypted data that correspond to at least one of the plurality of the network-threat indicators;

1.4 generating, based on the plurality of packet-filtering rules, log data of the identified packets comprising unencrypted data that correspond to at least one of the plurality of the network-threat indicators;

1.5 identifying packets comprising encrypted data;

1.6 correlating, based on the log data of the identified packets comprising unencrypted data that correspond to at least one of the plurality of network-threat indicators, packets comprising encrypted data that correspond to at least one of the plurality of network-threat indicators;

1.7 routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality [of] network-threat indicators.

1.2 Claim 1 - added subject-matter (Articles 100(c) and 123(2) EPC)

1.2.1 The board agrees with the opposition division and the respondents that granted claim 1 contains added subject-matter. **Feature 1.7** bears no limitation in respect of the type of "filtered packets" being "routed" to the "proxy system".

Original claim 7, cited by the appellant as providing basis for this feature, rather discloses that the one or more "network-threat indicators" comprise a domain

name and that the "packet-filtering system" is configured to route the one or more of the packets to the "proxy system" based on a determination that at least one of the first host or the second host corresponds to the domain name (board's emphasis). The action of "routing" in the original context (see Fig. 3A, step #9) thus relates to packets comprising unencrypted data (or copies thereof) being sent from "host 106" to "host 142". Those packets are "redirected" to proxy 112 instead. However, once the "SSL/TLS" connection between host 106 and proxy 112 is established (see Fig. 3B, step #17) and the subsequent packets comprise encrypted data, the packet-filtering system does not perform any further "routing" or "redirection". Rather, as indicated in Reasons 27 of the decision under appeal, those packets comprising encrypted data are just either "logged" or "dropped" (see Fig. 3B, steps #19 and #27 and paragraphs [37] and [46] of the application as filed).

1.2.2 The appellant argued that "routing filtered packets to a proxy system" in the context of claim 1 was to be broadly construed, i.e. it should not be narrowly interpreted as "network-layer routing" only. Rather, it should include any kind of "sending", "forwarding" or "logging". The unit "RG1" in step #19 of Fig. 3B at the very least "forwarded" to the proxy device "PD1" those packets (comprising encrypted data) which were not "dropped" but "logged". Thus, when applying the conclusions of **G 1/24**, i.e. in particular that the description and the drawings shall always be "consulted" to interpret a claim, to the present case, the skilled person in the field of data communications would have understood that such "forwarding" was providing a basis for the "routing" action of feature 1.7. In other words, as the appellant argued,

if multiple technically sensible interpretations of a certain claim feature exist, the one which is supported by the patent description should prevail.

1.2.3 This argument is flawed right from the outset. First, even if the Order of the **G 1/24** (related to assessing compliance with Articles 52 to 57 EPC only) could indeed be extrapolated to the assessment of compliance with Article 123(2) EPC, there is no indication in **G 1/24** that "consulting" or "referring to" the description and drawings could translate to adopting a claim interpretation which ensures that the disputed feature is originally disclosed and thus necessarily complies with Article 123(2) EPC. Such an approach which inherently assumes that there may be only one "correct" interpretation of a claim feature, namely the one derivable from the original description as its intended meaning (which is apparently advocated e.g. by **T 367/20-3.2.03**, Reasons 1.3.9 and 1.3.16 in the event of "mutually exclusive" interpretations or by the recent decision **T 2048/22-3.3.02**, Reasons 1.2.1 and 1.2.2 in the case of claim ambiguities), would not lead to an objective assessment of compliance with Article 123(2) EPC and thus jeopardise legal certainty. It would be tantamount to interpreting a claim feature such that, in the end, virtually no violation of Article 123(2) EPC within the meaning of the well-established "gold standard" could arise. Rather, there is a significant body of case law holding that *all technically reasonable* interpretations of a disputed claim feature are to be taken into account when assessing compliance with Article 123(2) EPC (see e.g. **T 945/20-3.4.02**, Reasons 2.4; **T 470/21-3.3.05**, Reasons 2.1; **T 2034/21-3.3.04**, Reasons 11; **T 193/22-3.3.06**, Reasons 3.5).

Second, even assuming *arguendo* that the "forwarding" of logged packets (comprising encrypted data) to the proxy device "PD1" in step #19 constituted a specific instance of the more general "routing filtered packets to a proxy system", this would still fail to justify the claimed generalisation, which also encompasses, *inter alia*, network-layer routing of filtered packets not being necessarily logged.

1.3 Thus, the ground for opposition under Article 100(c) EPC in conjunction with Article 123(2) EPC prejudices the maintenance of the patent as granted.

2. AUXILIARY REQUESTS 1 TO 7 AND 9 TO 15

Claim 1 of each of **auxiliary requests 1 to 7 and 9 to 15** differs from claim 1 as granted, *inter alia*, in:

1.7' routing, by the packet-filtering system, filtered packets comprising encrypted data to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality [of] network-threat indicators [**auxiliary requests 1 to 5, 7, 9 and 10**].

1.7" routing, by the packet-filtering system, the filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to at least one of the plurality [of] network-threat indicators [**auxiliary requests 6 and 11**].

On the other hand, **feature 1.7** remains unamended in claim 1 of each of **auxiliary requests 12 to 15.**

2.1 Claim 1 - added subject-matter (Article 123(2) EPC)

2.1.1 None of **features 1.7, 1.7' and 1.7"** reflects the original disclosure in respect of "routing" of packets (see point 1.2 above).

2.1.2 It follows that auxiliary requests 1 to 7 and 9 to 15 (labelled "Auxiliary Request 1" to "Auxiliary Request 7" and "Auxiliary Request 8" to "Auxiliary Request 14") are not allowable under Article 123(2) EPC, either.

3. AUXILIARY REQUEST 8

Claim 1 of **auxiliary request 8** (labelled "New Auxiliary Request 2a") differs from claim 1 as granted in the following:

- feature 1.6 explicitly requires, *inter alia*, "correlating the packets comprising encrypted data with one or more packets comprising unencrypted data previously determined to comprise data corresponding to at least one of the plurality of network threat indicators" (board's emphasis),

- feature 1.7 requires "routing (...) filtered packets being the determined identified packets, to a proxy system based on the determination that the filtered packets comprise unencrypted data that corresponds to at least one of the plurality of network-threat indicators" (board's emphasis).

3.1 Admittance into the appeal proceedings (Article 12(6), first sentence, RPBA)

3.1.1 Auxiliary request 8 (labelled "New Auxiliary Request 2a") was filed as "auxiliary request 2a" during the oral proceedings before the opposition division and was not admitted into the opposition proceedings for being late-filed and, *inter alia*, not being *prima facie* compliant with Article 123(2) EPC.

3.1.2 In accordance with Article 12(6), first sentence, RPBA, the board shall not admit *requests*, facts, objections or evidence which were not admitted in the proceedings leading to the decision under appeal, unless the decision not to admit them suffered from an error in the use of discretion or unless the circumstances of the appeal case justify their admittance.

3.1.3 The board holds that the opposition division correctly exercised its discretion not to admit this claim request, for the following reasons:

(a) First, the opposition division assessed, *inter alia*, "*prima facie* allowability" of auxiliary request 8, which is a well-established criterion as regards admittance considerations in first-instance proceedings.

(b) Second, the opposition division's finding that the objections under Article 123(2) EPC regarding **feature 1.6** of claim 1 still applied (see the decision under appeal, Reasons 45) was not unreasonable. Even when reviewing the opposition division's assessment in substance, the board in fact agrees with this objection as anticipated in its preliminary opinion on the main request and further confirmed after discussion during the oral proceedings before the board. This is because, contrary to the original application, feature 1.6

does not specify with which other data the "packet comprising encrypted data" are actually correlated and it cannot be implied that the "packet comprising encrypted data" should be necessarily correlated with the (previously identified) "packets comprising unencrypted data corresponding to the network-threat indicators". As with feature 1.7 (see point 1.2.2 above), the appellant's arguments rooted in the application of **G 1/24** fail to convince the board that the application as filed discloses feature 1.6 in its breadth.

3.1.4 The board sees therefore no reason to overrule the opposition division's discretionary decision.

3.2 Consequently, the board did not admit auxiliary request 8 (labelled "New Auxiliary Request 2a") into the appeal proceedings (Article 12(6), first sentence, RPBA).

4. AUXILIARY REQUEST 2b

Claim 1 of **auxiliary request 2b** (labelled "New Auxiliary Request 2b") likewise differs from claim 1 as granted in further limitations to features 1.6 and 1.7. In particular:

- **feature 1.6** also requires, albeit with a wording different from the one of claim 1 of auxiliary request 8, "correlating the packets comprising encrypted data with one or more packets comprising unencrypted data previously determined to comprise data corresponding to at least one of the plurality of network threat indicators" (emphasis added),

- **feature 1.7** also requires, with a wording slightly different from the one of claim 1 of auxiliary request 8, that the "filtered packets" comprise "unencrypted data" (emphasis added).

4.1 Admittance into the appeal proceedings (Article 13(2) RPBA)

4.1.1 The claims of auxiliary request 2b (labelled "Auxiliary Request 2b") were filed *after* notification of the board's communication under Article 15(1) RPBA. Hence, the admittance of this request is governed by Article 13(2) RPBA, according to which any amendment to a party's appeal case is, in principle, not taken into account, unless there are exceptional circumstances, which have been justified with cogent reasons by the party concerned.

4.1.2 As to the admissibility of auxiliary request 2b, the appellant submitted that the opposition division had concluded that the auxiliary requests on file had been caught in an "inescapable trap" between the requirements of Articles 123(2) and (3) EPC. Thus, the appellant had no guidance or instructions as to how to amend the claims in appeal. Nor did the appellant know how the board would interpret claim 1 or which objections would apply. It was thus necessary to hear the board before making further amendments. Only during the oral proceedings did the appellant learn how the board interpreted feature 1.6. Besides, claim 1 of auxiliary request 2b was clear and overcame what had been discussed about feature 1.7, since there was now a clear limitation to packets comprising "unencrypted data".

4.1.3 In the board's view, the above are no "cogent reasons" justifying "exceptional circumstances":

(a) First, the question of added matter in connection with features 1.6 and 1.7 had been discussed exhaustively already in the opposition proceedings. The board has neither denied nor confirmed the opposition division's stance on the existence of an "inescapable trap" because it had and has no bearing in the examination of the appeal. Yet, however adverse the opposition division's conclusions, the appellant could have filed auxiliary request 2b already during the opposition proceedings. Second and indeed decisively, the board at no point has deviated from its preliminary opinion during the oral proceedings before the board. It may well be that the appellant has better understood the board's position as a result of the debate that took place during the hearing. But this is the very purpose of every hearing, rather than an "exceptional circumstance". If the appellant's position was correct, every substantive discussion during an oral hearing could qualify as an exceptional circumstance in that it allowed a party to obtain a better understanding of the board's position, even if identical to the one as expressed in the preliminary opinion. If at all, the opposite is true: A change of opinion of the board due to a better understanding of a party's arguments during an oral hearing may be a legitimate reason for a party to react. Third, it is not the board's duty - particularly in *inter partes* proceedings - to provide any kind of "guidance or instructions" to the parties about how to best defend their respective cases.

4.2 Thus, the board did not admit auxiliary request 2b (labelled "New Auxiliary Request 2b") into the appeal proceedings (Article 13(2) RPBA).

5. Since there is no allowable claim request on file, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated