

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

K.MIZRA LLC,
Plaintiff,

v.

GOOGLE LLC,
Defendant.

§
§
§
§
§
§
§
§
§
§

Case No. 1:25-cv-00236-ADA

JURY TRIAL DEMANDED

GOOGLE’S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

	Page
INTRODUCTION	1
BACKGROUND OF THE ASSERTED PATENTS.....	1
AGREED TO CONSTRUCTION	2
ARGUMENT	2
A. Term 1: “protected network” (all asserted claims)	2
B. Term 2: “trusted computing base” (all asserted claims)	4
C. Term 3: “valid digitally signed attestation of cleanliness” (all asserted claims).....	10
D. Term 4: “includes at least one of an . . . and an . . .” (’705 Patent, all asserted claims).....	11
E. Term 5: “quarantine” or “quarantining” (all asserted claims)	13
F. Term 6: “quarantine server” (all asserted claims).....	16
G. Term 7: “a remediation host configured to provide data usable to remedy the insecure condition” (all asserted claims)	17
CONCLUSION.....	20

TABLE OF AUTHORITIES

	Page
CASES	
<i>ArcelorMittal France v. AK Steel Corp.</i> , 700 F.3d 1314 (Fed. Cir. 2012).....	15
<i>Azurity Pharms., Inc. v. Alkem Lab’ys Ltd.</i> , 133 F.4th 1359 (Fed. Cir. 2025)	8
<i>Biomedino, LLC v. Waters Techs. Corp.</i> , 490 F.3d 946 (Fed. Cir. 2007).....	19
<i>Cirba Inc. v. VMware, Inc.</i> , 2022 WL 608185 (D. Del. 2022)	12
<i>Diebold Nixdorf, Inc. v. ITC</i> , 899 F.3d 1291 (Fed. Cir. 2018).....	18, 20
<i>Egenera, Inc. v. Cisco Sys., Inc.</i> , 972 F.3d 1367 (Fed. Cir. 2020).....	18
<i>Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.</i> , 815 F.3d 1314 (Fed. Cir. 2016).....	1
<i>Eye Therapies, LLC v. Slayback Pharma, LLC</i> , 141 F.4th 1264 (Fed. Cir. 2025)	4
<i>Fenner Invs., Ltd. v. Cellco P’ship</i> , 778 F.3d 1320 (Fed. Cir. 2015).....	5
<i>Google LLC v. EcoFactor, Inc.</i> , 92 F.4th 1049 (Fed. Cir. 2024)	4
<i>Int’l Rectifier Corp. v. IXYS Corp.</i> , 361 F.3d 1363 (Fed. Cir. 2004).....	16
<i>Intel Corp. v. Qualcomm Inc.</i> , 21 F.4th 801 (Fed. Cir. 2021)	3
<i>Media Rights Techs., Inc. v. Capital One Fin. Corp.</i> , 800 F.3d 1366 (Fed. Cir. 2015).....	20

TABLE OF AUTHORITIES
(continued)

	Page
<i>Micropairing Techs. v. Gen. Motors</i> , 2022 WL 2442167 (W.D. Tex. 2022).....	12, 13
<i>MTD Prods. Inc. v. Iancu</i> , 933 F.3d 1336 (Fed. Cir. 2019).....	19
<i>Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.</i> , 831 F.3d 1350 (Fed. Cir. 2016).....	13
<i>Noah Sys., Inc. v. Intuit Inc.</i> , 675 F.3d 1302 (Fed. Cir. 2012).....	20
<i>NovaPlast Corp. v. Inplant, LLC</i> , 2023 WL 4760466 (D.N.J. 2023)	12
<i>O2 Micro Int'l Ltd. v. Beyond Innov. Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008).....	3
<i>Optis Cellular Tech., LLC v. Apple Inc.</i> , 139 F.4th 1363 (Fed. Cir. 2025)	18, 19
<i>Parallel Networks, LLC v. Abercrombie & Fitch Co.</i> , 704 F.3d 958 (Fed. Cir. 2013).....	5
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005).....	3, 16
<i>Rain Computing, Inc. v. Samsung Elecs. Am., Inc.</i> , 989 F.3d 1002 (Fed. Cir. 2021).....	19, 20
<i>Retractable Techs., Inc. v. Becton, Dickinson & Co.</i> , 653 F.3d 1296 (Fed. Cir. 2011).....	6
<i>Ruckus Wireless, Inc. v. Innovative Wireless Solutions, LLC</i> , 824 F.3d 999 (Fed. Cir. 2016).....	14, 15
<i>SIMO Holdings Inc. v. Hong Kong Network Tech</i> , 983 F.3d 1367 (Fed. Cir. 2021).....	11
<i>SuperGuide Corp. v. DirecTV Enters., Inc.</i> , 358 F.3d 870 (Fed. Cir. 2004).....	12, 13

TABLE OF AUTHORITIES
(continued)

	Page
<i>Vitronics Corp. v. Conceptronic, Inc.</i> , 90 F.3d 1576 (Fed. Cir. 1996).....	9
<i>Williamson v. Citrix Online, LLC</i> , 792 F.3d 1339 (Fed. Cir. 2015).....	17, 18
<i>WSOU Investments LLC v. Google LLC</i> , 2023 WL 6531525 (Fed. Cir. 2023).....	19
OTHER AUTHORITIES	
Antonin Scalia & Bryan A. Garner, <i>Reading Law: The Interpretation of Legal</i> <i>Texts</i> § 19 (2012)	11
William Strunk, Jr. & E.B. White, <i>The Elements of Style</i> (4th ed. 2000).....	12

TABLES OF EXHIBITS

Exhibit No.	Description
1	Barbara Fraser et al., <i>RFC 2196, Site Security Handbook</i> , RFC Editor (Sept. 1997), available at https://www.rfceditor.org/info/rfc2196
2	<i>RFC Errata: RFC 2196, Site Security Handbook</i> , September 1997, RFC Editor, available at https://www.rfceditor.org/errata/eid482.RFC 2196
3	U.S. Gen. Accounting Office, GAO-04-467, <i>Information Security: Technologies to Secure Federal Systems</i> (Mar. 2004), available at https://www.gao.gov/products/gao-04-467
4	U.S. Patent No. 6,345,299 (filed Nov. 26, 1997) (issued Feb. 5, 2002)
5	Pl.'s K.Mizra's Op. Cl. Constr. Br., <i>K.Mizra LLC v. HPE</i> , No. 2:21-cv-305, Dkt. 117 (E.D. Texas)
6	File History for U.S. Patent 8,234,705 (KMIZ-GOOGLE_000058-000513)
7	U.S. Patent Application No. 2005/0033987 A1 (filed Aug. 8, 2003) (published Feb. 10, 2005)
8	Martin Abadi & Ted Wobber, <i>A Logical Account of NGSCB</i> , in <i>Proceedings of Formal Techniques for Networked and Distributed Systems (Forte '04)</i> , Springer-Verlag (Sept. 2004), available at https://www.microsoft.com/enus/research/publication/a-logicalaccount-of-ngscb/ (“Abadi”)
9	Claim Construction Order, <i>K.Mizra LLC v. HPE</i> , No. 2:21-cv-305, Dkt. 132 (E.D. Tex. Nov. 21, 2023)
10	Antonin Scalia & Bryan A. Garner, <i>Reading Law: The Interpretation of Legal Texts</i> (2012)
11	William Strunk, Jr. & E.B. White, <i>The Elements of Style</i> (4th ed. 2000)
12	<i>Quarantine</i> , Webster's Third New International Dictionary, Merriam-Webster Inc., at 1859 (2002)
13	<i>Quarantine</i> , Random House Webster's Unabridged Dictionary, Random House, at 1579 (2nd ed. 2001)
14	U.S. Patent Application No. 2002/0199116 A1 (filed June 25, 2001) (published Dec. 26, 2002)

Exhibit No.	Description
15	Kevin Eustice et al., <i>Securing Nomads: The Case for Quarantine, Examination, and Decontamination, in NSPW '03: Proceedings of the 2003 Workshop on New Security Paradigms</i> (2004) (“Eustice”)
16	Declaration of Sachin M. Patel and Appendices, dated August 26, 2025
17	<i>Host</i> , Comprehensive Dictionary of Electrical Engineering, at 312 (1999)
18	<i>Host</i> , Microsoft Computer Dictionary, at 256 (5th ed. 2002)

TABLE OF ABBREVIATIONS

Abbreviation	Description
K.Mizra	Plaintiff K.Mizra LLC
Google	Defendant Google LLC
'705 Patent	U.S. Patent No. 8,234,705
'048 Patent	U.S. Patent No. 9,516,048
asserted patents	The '705 and '048 Patents
asserted claims	Claims 12, 13, 16, and 19 of the '705 Patent and claims 10, 11, 14, 17, and 18 of the '048 Patent
K.Mizra-HPE matter	<i>K.Mizra LLC v. HPE</i> , No. 2:21-cv-305 (E.D. Texas)
skilled artisan or POSITA	Person of ordinary skill in the art

* *Emphasis added unless otherwise indicated.*

** *Internal citations and quotations omitted unless otherwise indicated.*

*** *Citations to one specification refer to both specifications except where otherwise indicated.*

INTRODUCTION

The seven disputed terms fall into three classes: terms requiring clarification following other litigations involving the same patents; terms with specific meanings compelled by the intrinsic evidence and confirmed by extrinsic evidence; and one term drafted in means-plus-function that lacks corresponding structure.¹ K.Mizra denies that any claim construction is necessary, using alleged “plain meaning” to broaden the claims’ scope beyond their ordinary meaning and the description in the specification. As explained below, Google’s proposed constructions adhere to the fundamental rule that “a word describing patented technology takes its definition from the context in which it was used by the inventor.” *Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.*, 815 F.3d 1314, 1320 (Fed. Cir. 2016).

BACKGROUND OF THE ASSERTED PATENTS

The asserted patents, addressing techniques for network security, share nearly identical specifications and claims. The asserted patents generally disclose receiving a request from a host to connect to a “protected network” and determining whether to “quarantine” the host. ’705 Patent, 3:8-11; ’048 Patent, 12:11-13. The asserted claims determine whether to quarantine the first host by “contacting a trusted computing base associated with a trusted platform module within the first host” and then receiving “a digitally signed attestation of cleanliness” from the trusted computing base. ’705 Patent, claims 12, 19; ’048 Patent, claims 10, 17. If quarantined, the host receives only limited access to the protected network to remedy a condition causing the quarantine. ’705 Patent, 3:11-20. Figures 10B and 14 show the network environment where infected hosts are quarantined and the process for isolating the hosts.

¹ Terms 1-7 are presented in Sections A-G in an order following the Court’s Standing Order Governing Proceedings – Patent Cases (OGP).

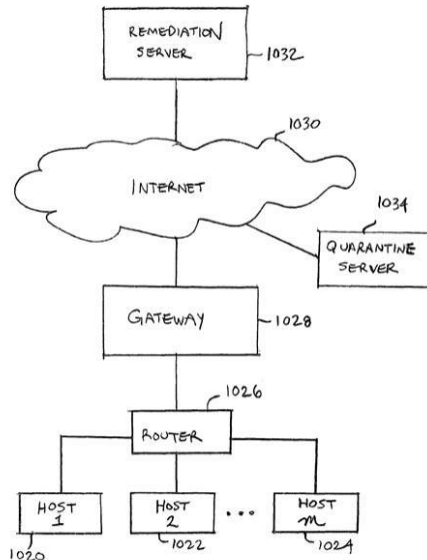


FIG. 10B

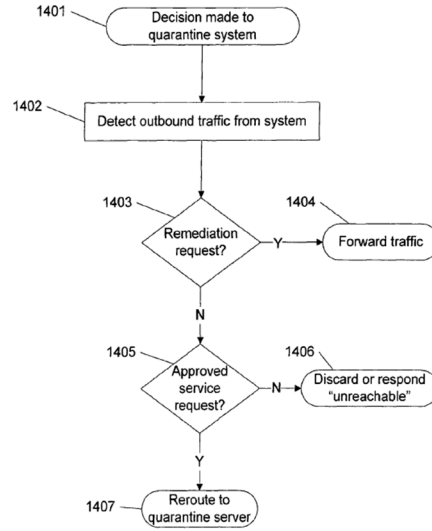


Figure 14

Id., Figs. 10B & 14.

AGREED TO CONSTRUCTION

K.Mizra and Google agree to the construction of the following term:

Term	Agreed To Construction
“trusted platform module” (all asserted claims)	a secure cryptoprocessor that can store cryptographic keys and that implements the Trusted Platform Module specification from the Trusted Computing Group.

ARGUMENT

A. Term 1: “protected network” (all asserted claims)

Google’s Construction	K.Mizra’s Construction
private network, distinct from public networks like the Internet	Plain and ordinary meaning

“Protected Network” Requires A Construction To Assist The Jury. The asserted claims recite “protecting a network” that detects “an insecure condition on a first host that has connected or is attempting to connect to *a protected network.*” ’705 Patent, claims 12, 19; ’048 Patent, claims 10, 17. The claim language itself demonstrates that “protected network” must be something more than just a “network.” Google construes the term consistent with its ordinary meaning: a “private network, distinct from public networks like the Internet.” By contrast, K.Mizra attempts to read out the recited word “protected” by disputing Google’s construction without stating what it

contends the term means. Construing “protected network” is therefore necessary to assist the jury because when “the ordinary meaning . . . does not resolve the parties’ dispute,” courts must “determine what claim scope is appropriate in the context of the patents-in-suit.” *O2 Micro Int’l Ltd. v. Beyond Innov. Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008).

Intrinsic Evidence Establishes That Google’s Construction Reflects The Ordinary Meaning. The intrinsic evidence confirms that a “protected network” is distinct from the “Internet and/or another public” network. First, the fact that the claims “did not just say [‘network’] but instead said [‘protected network’] provides a strong reason to avoid the disfavored result of rendering the word [protected] superfluous.” *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 810 (Fed. Cir. 2021); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (“[T]he claim in this case refers to ‘steel baffles,’ which strongly implies that the term ‘baffles’ does not inherently mean objects made of steel.”).

Second, the specification demonstrates that a “protected network” is distinct from public networks. When addressing Figure 10B, the patent describes “a network environment” comprising “a gateway, router, firewall, or other device configured to provide and control access ***between a protected network and the Internet and/or another public*** or private ***network.***” ’705 Patent, 11:57-67. Figure 10B (reproduced above) explicitly provides that the Internet (1030) is a separate feature from the protected network, which includes the gateway 1028, router 1026, and so forth. The specification also repeatedly distinguishes between the claimed “protected network” and other networks like the Internet, explaining that “[c]ontact may be made with an anti-contagion source (302) ***via a network such as the Internet.***” *Id.*, 4:56-57. Likewise, the patent teaches that the “client system 420 includes a communication interface 422, such as a network interface card, configured to send/receive communications ***via a network, such as the Internet.***” *Id.*, 6:66-7:2.

Contemporaneous Evidence Confirms That Skilled Artisans Understood That A “Private Network” Is Distinct From Public Networks. Claims are construed as understood “at the time of the invention,” in this case, the effective filing date. *Eye Therapies, LLC v. Slayback Pharma, LLC*, 141 F.4th 1264, 1268 (Fed. Cir. 2025). Contemporaneous extrinsic evidence reflecting the POSITA’s objective understanding of “protected network” further supports Google’s construction:

- The RFC Site Security Handbook, which was a guide for developing computer security procedures, explained: “Firewalls help to place limitations on the amount and type of communication that takes place between the **protected network** and the [sic] **another network** (e.g., **the Internet**, or another piece of the site’s network).” Ex. 1 at 21; *see generally* Ex. 2.
- The U.S. General Accounting Office’s Report on Information Security explained: “Typically, a firewall is a network device or host with two or more network interfaces—one connected to the **protected** internal **network** and the other connected to **unprotected networks, such as the Internet**.” Ex. 3 at 15.
- U.S. Patent No. 6,345,299 disclosed: “The firewall node 12 protects communications between an **unprotected public network 14** (e.g., **the Internet**) and a **private protected network 16**.” Ex. 4 at 1:37-39.

This objective evidence explains both what a “protected network” does and does not include, aligning with the established principle that “[c]laim construction is the judicial statement of what is and is not covered by the technical terms and other words of the claims.” *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1055 (Fed. Cir. 2024).

B. Term 2: “trusted computing base” (all asserted claims)

Google’s Construction	K.Mizra’s Construction
hardware or software within the first host that provides security to the host	hardware or software that has been designed to be a part of the mechanism that provides security to a computer system

“Trusted Computing Base” Requires Clarification In Light Of Prior Litigation And The Intrinsic And Extrinsic Evidence. The intrinsic evidence—the claims, the specification, and the prosecution history—conclusively shows the “trusted computing base” must be “within the first host.” The asserted claims recite “a trusted computing base associated with a trusted platform

module within the first host.” *See* ’705 Patent, claim 12, 19; ’048 Patent, claim 10, 17. Here, K.Mizra recycles its previously-litigated construction, arguing that the trusted computing base “can be located *anywhere* based on the plain language of the claim.” Ex. 5 at 6 (original emphasis). To the contrary, the intrinsic and extrinsic evidence disclose a trusted computing base *within the first host*. There is no dispute that the claim language “associated with a trusted platform module” modifies “a trusted computing base.” But also, in context, the claim language “within the first host” further modifies the whole (“a trusted computing base associated with a trusted platform module”), not the part (“a trusted platform module”). Claim terms “are not construed in the abstract, but in the context in which the term was presented and used by the patentee, as it would have been understood by a person of ordinary skill in the field of the invention on reading the patent documents in light of the entire specification and prosecution history.” *Fenner Invs., Ltd. v. Cellco P’ship*, 778 F.3d 1320, 1322-23 (Fed. Cir. 2015). Google’s construction honors this principle.

The Specification And Prosecution History Demonstrate That K.Mizra Attempts To Rewrite The Claim Language. In prior litigation, K.Mizra insisted that the “trusted computing base can be located within *any* computer, provided that it is associated with the trusted platform module within the first host.” Ex. 5 at 6 (original emphasis). The Court should reject K.Mizra’s misreading of “associated with” because it redrafts the asserted claims to have a trusted computing base “within *any* computer.” Rejecting a similar approach, the Federal Circuit reasoned:

If [patentee’s] position were adopted, it would permit the broad term “associated with” to effectively rewrite the patent. Notwithstanding the potential breadth of the phrase “associated with,” it is clear that the patent teaches an applet containing both the data and the functionality when the applet is generated.

Parallel Networks, LLC v. Abercrombie & Fitch Co., 704 F.3d 958, 968 (Fed. Cir. 2013). The same reasoning and outcome follows here.

The specification does not disclose a “trusted platform module,” instead providing examples of a “trusted computing/code base.” There is no dispute that the “trusted platform module” is within the “first host.” The examples of “trusted computing/code base” confirm that, like the trusted platform module, the trusted computing base must be within the first host. *See* ’705 Patent, 13:64-14:12. The specification describes examples indicating that each computer’s “trusted computing/code base” is *within a computer* being queried. Based on the claim language, that computer is “the first host.” *See id.*, 13:64-67 (acknowledging “[a] computer” and “a trusted computing base *within a computer*”), 14:7-9 (“*Trusted code bases* may . . . execute antivirus scans of *the remainder of the computer.*”), 14:10-12 (“[T]rusted code bases may digitally sign assertions about the . . . *state of their computers.*”); 14:1-7 (“*a trusted computing base within a computer* is the Paladium [sic] security initiative under development by Microsoft” and “is described in various TCG specifications”). If the applicant intended the “trusted computing/code base” to be on “any” or “another” computer instead of “within the first host,” the inventor knew how to say so. *See, e.g., id.*, 8:19-20 (“In some embodiments, all requests are assumed to be authentic without the use of *any authenticator.*”), 10:25-26 (“*Any order* may be used.”), 16:60-63 (“In some embodiments, a user is requested and/or required to authorize in advance use of an authorized and/or *any unauthorized backdoor* for purposes of inoculation.”), 10:11-13 (“In one example, an indirect source may be a peer, such as *another computer* that has downloaded the content.”). The applicant expressed no such limitation. The specification “only disclose[s] embodiments that are expressly limited to” the trusted computing base able to check the remainder of the computer, be a part of “a computer,” or sign assertions on the “state of [its] computer[],” *i.e.*, within the first host. *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1305 (Fed. Cir. 2011) (“[A] construction of ‘body’ that limits the term to a one-

piece body is required *to tether the claims to what the specifications* indicate the inventor actually invented.”). Google’s construction reflects the way skilled artisans would have understood the term: “hardware or software within the first host that provides security to the host.”

During prosecution of the ’705 Patent, the applicant intended that the “trusted computing base” to be within the first host, where it indicated “a trusted platform module” to be a part that modifies “a trusted computing base associated with a trusted platform module,” a whole. *See, e.g.*, Ex. 6 at 248 (“Liang does not anticipate a trusted platform module, nor *a trusted computing base associated with a trusted platform module.*”). The examiner rejected the pending claims because:

As per claim 9, Liang discloses “a system for protecting a network, comprising: a processor configured to”: “detect an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that [sic] on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21), “*wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host*” (col. 8, lines 49-53, send a query to client device requesting confirmation)[.]

Id. at 272 (first emphasis in original). Appealing this rejection, the applicant asserted that “Liang does not teach ‘wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host’ because Liang does not teach either a trusted computing base or a trusted platform module.” *Id.* at 247 (underline in original). Then acknowledging that “[t]rusted computing base’ and ‘trusted platform module are terms of art with specific meanings,” the application stated: “A given piece of *hardware or software* is a part of the *TCB* if and only if it has been designed to be a part of the mechanism that *provides its security to the computer system.*” *Id.* at 248.

K.Mizra cannot rewrite the asserted claims, when the applicant during prosecution failed to correct the examiner’s understanding that “within the first host” modifies “a trusted computing base associated with a trusted platform module.” After all, “[a]ny explanation, elaboration, or

qualification presented by the inventor during patent examination is relevant, for the role of claim construction is *to capture the scope of the actual invention* that is disclosed, described, and patented.” *Azurity Pharms., Inc. v. Alkem Lab’ys Ltd.*, 133 F.4th 1359, 1366 (Fed. Cir. 2025). After amending the asserted claims to include “a trusted computing base associated with a trusted platform module within the first host,” *see* Ex. 6 at 373-83, the applicant argued that the prior art “does not anticipate [(1)] a trusted platform module, nor [(2)] *a trusted computing base associated with a trusted platform module*,” *id.* at 248. The applicant explicitly distinguished “a trusted platform module” from “a trusted computing base associated with a trusted platform module,” clarifying that a “trusted platform module” is the *component* of the *whole* “trusted computing base associated with a trusted platform module.” *Id.* The applicant also clarified the type of “trusted computing base” not taught by prior art: “a trusted computing base *associated with a trusted platform module*.” *Id.* at 247-48. Moreover, the applicant repeatedly used the phrase “a trusted computing base associated with a trusted platform module,” without mentioning “within the first host,” *see id.* at 248 (arguing that prior art “does not anticipate . . . *a trusted computing base associated with a trusted platform module*”); *id.* at 249 (“Clearly, [prior art] does not disclose the detail in the claim, i.e. ‘*a trusted computing base associated with a trusted platform module*’”), indicating that the latter claim language is meant to modify the former, the *whole* “trusted computing base associated with a trusted platform module.”

Upon further examination, the examiner demonstrated the understanding that “a trusted computing base associated with a trusted platform module” was to be “within a first client.” The examiner observed that the prior art “discloses detecting an insecure condition in a client computing device.” Ex. 6 at 227. The examiner then relied on an additional reference, Yan, when rejecting claim 9 of the application (claim 12 of the ’705 Patent). *Id.* at 227-28. Yan discloses

that, “[t]he Trusted Computing Platform Alliance (TCPA) formed in 1999 by Intel, HP/Compaq, IBM, Microsoft, and other companies, proposes *a new computing platform* for this century that will initially provide improved trust in the *Personal Computer (PC) platform* with eventual trust provided by the Trusted Mobile Computing Platform (TMCP).” Ex. 7 at [0003]; *see also* Ex. 6 at 228 (citing Yan at [0003]). The examiner’s combination requires “detecting an insecure condition *in a client computing device*” (i.e., within a first host), as well as “contacting a trusted computing base associated with a trusted platform module” (also in the first host), respectively. Ex. 6 at 227-28. Based on the applicant’s and examiner’s understanding of the application, the Court should adopt Google’s construction that “trusted computing base” relates to “hardware or software” “that provides security to the host.” *See Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) (“[The prosecution] history contains the complete record of all the proceedings before the Patent and Trademark Office, *including any express representations made by the applicant regarding the scope of the claims.*”). And that the “trusted computing base associated with a trusted platform module” is “*within the first host.*” *See id.*; *see also* Ex. 6 at 247-49.

Extrinsic Evidence Reveals That At The Time Of Invention, The Trusted Computing Base And Its Associated Trusted Platform Module Were Within The First Host. Microsoft’s Palladium security initiative is a trusted computing base that resides on the computer for which it provides security. *See, e.g.*, ’705 Patent, 14:1-7. Like the specification, a contemporaneous 2004 paper (“Abadi”), describes Palladium as being located on a particular computer: “NGSCB (‘Next-Generation Secure *Computing Base*’, formerly known as ‘Palladium’) integrates hardware and software components that aim to help in protecting data and processes against software attacks. . . . The software includes new, trusted operating system components.” Ex. 8 at 1. Accordingly, like the trusted computing base claimed in the asserted claims, Abadi acknowledges that Palladium

also was located on and used to protect the first host. Thus, contemporaneous art further supports that the trusted computing base is “within the first host.”

C. Term 3: “valid digitally signed attestation of cleanliness” (all asserted claims)

Google’s Construction	K.Mizra’s Construction
Plain and ordinary meaning, wherein the plain and ordinary meaning is that the “attestation of cleanliness” is digitally signed by and received from the “trusted computing base”	Plain and ordinary meaning

The Term “Valid Digitally Signed Attestation Of Cleanliness” Requires Clarification In Light Of Prior Litigation And The Intrinsic Evidence. In the K.Mizra-HPE matter, Judge Gilstrap construed “attestation of cleanliness” to have its ordinary meaning, holding that “the ‘attestation of cleanliness’ *must be received* from the ‘trusted computing base’ in the patent claims at issue.” Ex. 9 at 11. Judge Gilstrap’s construction is included here as part of the construction for the larger limitation reciting “valid digitally signed attestation of cleanliness.” Construction of this larger limitation term is necessary to avoid juror confusion regarding the role and functionality of the “trusted computing base.” Consistent with Judge Gilstrap’s construction, the intrinsic evidence establishes Google’s proposed construction.

The phrase “valid digitally signed” modifies “attestation of cleanliness,” requiring that the “attestation of cleanliness” be digitally signed by and received from the “trusted computing base.” Claim 12, for example, first recites “contacting a trusted computing base” and requires “receiving a response” from the trusting computing base. ’705 Patent, claims 12, 19. The claim then recites that the “response” from the trusted computing base contains a “valid digitally signed attestation of cleanliness” that, in turn, contains two conditions. *Id.* The attestation includes an ascertainment by the trusted computing base that “the first host is not infested” and “the presence of a patch or a patch level associated with a software component on the first host.” *Id.* The specification is in accord, stating that “trusted code bases *may digitally sign assertions* about the cleanliness (e.g. infestation status) and/or state of their computers.” *Id.*, 14:10-12.

Google’s clarification that the “attestation of cleanliness” is digitally signed by and received from the “trusted computing base” is a natural extension of Judge Gilstrap’s clarification and would assist the jury’s understanding of the claim language.

D. Term 4: “includes at least one of an . . . and an . . .” (’705 Patent, all asserted claims)

Google’s Construction	K.Mizra’s Construction
includes at least one of an . . . and at least one of an . . .	Plain and ordinary meaning

Google’s Construction Is A Straightforward Application Of Settled Principles To The Plain Claim Language. Google’s construction of this term adheres to the Federal Circuit’s recent guidance in *SIMO Holdings Inc. v. Hong Kong Network Tech*:

Our holding in *SuperGuide* reflects a more general grammatical principle applicable to a modifier coming before a series. “When there is a straightforward, parallel construction that involves all nouns or verbs in a series, a prepositive or postpositive modifier normally applies to the entire series.” Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* § 19, 147 (2012). ***As SuperGuide makes clear, the principle has particular force when the term joining the items in a series is “and.”***

983 F.3d 1367, 1377 (Fed. Cir. 2021); *see also* Ex. 10 at 147. The Federal Circuit further explained that when “at least one of” is “at the start of a list of items joined together by ‘and[,]’” the phrase “applie[s] to ***each item in the list***, not to the list considered as a whole.” *Id.* at 1376.

Claims 12 and 19 of the ’705 Patent recite: “the valid digitally signed attestation of cleanliness ***includes at least one of an*** attestation that the trusted computing base has ascertained that the first host is not infested, ***and an*** attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.” Accordingly, the phrase “at least one of” modifies a list of items (*e.g.*, types of attestations) with parallel articles (*e.g.*, an) joined together by the conjunctive “and.” “[B]ecause the list uses ‘and’ rather than ‘or,’ the phrase is properly understood as if ‘of’ or ‘at least one of’ appears before ***each*** item.” *Id.* at 1376-77; *see also* Ex. 11 at 27; *SuperGuide Corp. v. DirecTV Enters., Inc.*,

358 F.3d 870, 886 (Fed. Cir. 2004) (“The phrase ‘at least one of’ precedes a series of categories of criteria, and the patentee used the term ‘and’ to separate the categories of criteria, which connotes a conjunctive list.”). A straightforward application of these principles here requires “**at least one of** an attestation that the trusted computing base has ascertained that the first host is not infested,” and “[**at least one of**] an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.”

Judge Gilliland’s decision in *Micropairing Techs. v. Gen. Motors* fully accords with this construction. In *Micropairing*, the Court explained “that the phrase ‘at least one of [A], [B], and [C]’ is conjunctive,” reasoning that the “Federal Circuit has also held that the term ‘and’ should be given its plain and ordinary meaning (*i.e.*, ‘and’ not ‘or’) unless ‘the specification compels a disjunctive construction,’ for example, when the term ‘conjoins mutually exclusive possibilities.’” 2022 WL 2442167, at *14-15 (W.D. Tex. 2022). Other courts also reach the same determination. In *Cirba Inc. v. VMware, Inc.*, the court construed “at least one of a compatibility score, and a number of transfers” to be “**at least one** compatibility score and **at least one of** a number of transfers.” 2022 WL 608185, at *8 (D. Del. 2022) (Stark, J.). Similarly, in *NovaPlast Corp. v. Inplant, LLC*, the court “recogniz[ed] that the phrase ‘at least one of’ requires one or more of each item in a conjunctive list.” 2023 WL 4760466, at *11 (D.N.J. 2023).

The Specification Cements That Google’s Construction Covers The Ordinary Meaning.

The specification supports Google’s interpretation and does not compel a disjunctive construction. The specification states that the “trusted code bases may digitally sign assertions about the cleanliness (e.g. infestation status) **and/or** state of their computers.” ’705 Patent, 14:10-12. The inventors thus knew how to disclose embodiments requiring either one or both types of the claimed assertions. This is true throughout the patent. *See id.*, 14:12-19 (“In some embodiments, the query

for cleanliness (1302) *may be responded to by anti-contagion software*, such as antivirus software, with assertions about the currency of a scan”); *id.*, 14:19-22 (“In some embodiments, an *operating system may respond with information associated with its patch level*, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness.”).

The patent also uses permissive language of “may digitally sign” and “may respond” as relating to each item of the series. There is otherwise no restrictive language mandating mutual exclusivity between the two. As in *SuperGuide*, “nothing in the specification rebuts the presumption that the [] patentee intended the plain and ordinary meaning of this language.” 358 F.3d at 887. In fact, the patent owner knew how to claim the disjunctive form of a similar limitation, claiming, in the related ’048 Patent, “at least one attestation *selected from the group consisting of* an attestation that the trusted computing base has ascertained that the first host is not infested, *and* an attestation that the trusted computing base has ascertained the presence of a patch or a patch level” ’048 Patent, claims 10, 17; *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1357 (Fed. Cir. 2016) (“A Markush group lists *specified alternatives* . . . in the form: a member selected *from the group consisting of A, B, and C.*”). As Judge Gilliland explained, “the patentee had multiple options available to use disjunctive language if that was intended,” including “at least one *selected from the group of A and B*” and, indeed, the patentee knew to do that in other claims. *Micropairing*, 2022 WL 2442167, at *15. The same reasoning applies with equal force to this case and requires the same result: this limitation is written in the conjunctive.

E. Term 5: “quarantine” or “quarantining” (all asserted claims)

Google’s Construction	K.Mizra’s Construction
isolating from the protected network	Plain and ordinary meaning

“Quarantine” Or “Quarantining” Requires Construction To Avoid Juror Confusion When Applied In The Context Of Protected Networks. The term “quarantine” or “quarantining”

appears in all asserted claims. For example, claim 12 of the '705 Patent recites: “A system for protecting a network, comprising: a processor configured to: . . . when it is determined that the response does not include a valid digitally signed attestation of cleanliness, *quarantine* the first host.” The Court should adopt Google’s construction to prevent juror confusion, which K.Mizra appears to anticipate by failing to provide any construction of the term “quarantine” or “quarantining” to the context of protected networks. Unlike K.Mizra’s non-construction, Google’s construction helps the jury understand the term in the context of the asserted patents.

The Specification Demonstrates That To “Quarantine” Is To “Isolate.” Consistent with the claim language, the specification supports Google’s construction that “quarantine” or “quarantining” relates to isolating from the protected network. As an initial matter, the asserted patents share similar titles, “Contagion *Isolation* and Inoculation” and “Contagion *Isolation* and Inoculation *via Quarantine*,” respectively. Patent titles “aid in claim construction.” *Ruckus Wireless, Inc. v. Innovative Wireless Solutions, LLC*, 824 F.3d 999, 1003 n.2 (Fed. Cir. 2016). The '705 Patent specification explains:

Contagion *isolation* and inoculation is disclosed. In some embodiments, a request is received from a host, e.g., via a network interface, to connect to a protected network. ***It is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided only limited access to the protected network.*** In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed.

'705 Patent, 3:8-16, Abstract (same). The specification indicates that the “quarantined host” is isolated or quarantined from the protected network except for accessing a remediation server. *See id.*, 12:3-7 (“In some embodiments, a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch, more current threat definition, etc.”). The claims make clear that the term “quarantine” or “quarantining” relates to isolating from the protected network, *see, e.g., id.*, claim 12 (“*quarantine*

the first host”), claim 19 (“**quarantining** the first host”); *see also* ’048 Patent, claim 17 (same). Moreover, the asserted patents make clear that the invention seeks to secure the protected network by isolating the host from the network: “**Contagion isolation** and inoculation is disclosed. In some embodiments, a request is received from a *host*, *e.g.*, via a network interface, **to connect to a protected network**. It is determined whether the host is **required to be quarantined**.” ’705 Patent, 3:8-11.

Extrinsic Evidence Supports Google’s Construction. First, contemporaneous dictionary definitions support Google’s construction that “quarantine” means to “isolate.” Webster’s Third New International Dictionary defines “quarantine” as to “**isolate** as a precaution against contagious disease: detain in quarantine” or “to exclude by quarantine.” Ex. 12 at 1859. Likewise, Random House Webster’s Unabridged Dictionary defines “quarantine” as “a **strict isolation** imposed to prevent the spread of disease.” Ex. 13 at 1579.

Second, the prior art demonstrates how skilled artisans used “quarantine” interchangeably with “isolate” at the time of invention. “Prior art can help to demonstrate how a disputed term is used by those skilled in the art.” *ArcelorMittal France v. AK Steel Corp.*, 700 F.3d 1314, 1321 (Fed. Cir. 2012). For example:

- U.S. Patent Publication 2002/0199116 A1 teaches a “system and method for network virus exclusion of the present invention **isolates** virus-susceptible clients and virus-infected clients from a server of a network . . . to effectively place those clients in **quarantine**.” Ex. 14 at [0015].
- In a 2004 article, “*Securing Nomads: The Case for Quarantine, Examination, and Decontamination*,” researchers stated that their model “protects machines by logically **isolating them**, examining them for known vulnerabilities or malicious software, and then repairing, or otherwise mitigating, discovered problems. **We refer to these processes as quarantine**, examination, and decontamination.” Ex. 15 at 125 (explaining the “goal of the quarantine stage is to isolate potential clients”).

The prior art here demonstrates that at the time of invention, POSITAs were using “quarantine” or “quarantining” consistent with Google’s construction, *i.e.*, isolating from the protected network.

F. Term 6: “quarantine server” (all asserted claims)

Google’s Construction	K.Mizra’s Construction
server to which a quarantined host’s network traffic is redirected	Plain and ordinary meaning

“Quarantine Server” Requires Construction To Assist the Jury. The claimed invention’s purpose as captured in the claim language and tracking the term’s usage in the specification support Google’s construction that a “quarantine server” is a “server to which a quarantined host’s network traffic is redirected.” Google’s construction also clarifies for the jury that the specifically claimed “quarantine server” is different from other generic servers. The applicant’s deliberate choice to draft the asserted claims to include a “quarantine server,” as opposed to just a “server” or any other type of “server” has a consequence. “Had the inventor meant ‘[server],’ he could have used that word. However, we must consider the word that the inventor actually chose.” *Int’l Rectifier Corp. v. IXYS Corp.*, 361 F.3d 1363, 1374 (Fed. Cir. 2004). On its face, “*quarantine* server” makes clear that it requires something more than just any “server.” See ’705 Patent, claims 12, 19.

The specification “is the single best guide to the meaning of a disputed term.” *Phillips*, 415 F.3d at 1315. Here, consistent with the claim language, the specification and Figure 14 distinguish the quarantine server’s purpose from other types of servers. The patent explains that when outbound traffic from a quarantined device is determined to be “associated with a remediation request (1403)” —such as “contact with a verified remediation site” or “an internal ISP site” —“the traffic is routed or forwarded to its destination,” such as a remediation server. ’705 Patent at 14:50-63. A “remediation server” is where the quarantined host may be able “to download a patch, more current threat definition, etc.” *Id.* at 12:5-7. By contrast, if non-remediation “outbound traffic” is detected during quarantine, then the network traffic is “re-routed to a special *quarantine server* (1407), such as an ISP web server that provides information and links to assist in remediation.” *Id.*, 14:65-15:1. Figure 14 (reproduced above) demonstrates that

the “quarantine server” receives redirected traffic from a quarantined host.

The asserted patents consistently stress the quarantine server’s purpose of redirecting network traffic from a quarantined host. The patent explains that “a device such as a router may forward *outbound traffic* from a *quarantined computer* to a *quarantine server*.” *Id.*, 15:63-65, Fig. 16. The patent also teaches that “requests to connection to a host *other than the remediation server 1032* are *redirected* to a *quarantine server 1034* configured to provide a notice and/or other information and/or instructions to a user of the quarantined host.” *Id.*, 12:7-12. And Figure 10B illustrates that the “quarantine server” and remediation server are separate, further reinforcing how traffic is redirected when appropriate.

G. Term 7: “a remediation host configured to provide data usable to remedy the insecure condition” (all asserted claims)

Google’s Proposed Construction	K.Mizra’s Construction
Subject to 35 U.S.C. § 112(f). <u>Function</u> : “provide data usable to remedy the insecure condition” <u>Structure</u> : Indefinite	Plain and ordinary meaning

All the asserted claims recite the limitation “[1] a remediation host [2] configured to [3] provide data usable to remedy the insecure condition.” ’705 Patent, claims 12, 19 (bracketed numbers added); ’048 Patent, claims 10, 17. This limitation invokes § 112, ¶ 6 and is indefinite for failure to disclose sufficient corresponding structure.

The Claims Establish Section 112, ¶ 6 Applies. The rebuttable presumption against § 112, ¶ 6 is overcome when, as here, the claim “fails to recite sufficiently definite structure,” or “recites function without reciting sufficient structure for performing that function.” *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348-51 (Fed. Cir. 2015). The limitation “[1] a remediation host [2] configured to [3] provide data usable to remedy the insecure condition” is written “in a format consistent with traditional means-plus function claim limitations” by “replac[ing] the term ‘means’ with the term [remediation host] and recit[ing] [] functions” to be performed. *Id.* at 1350.

Starting with the phrase “a remediation host,” this is a nonce term that lacks definite structure because it is “not adopted into use generally.” *Egenera, Inc. v. Cisco Sys., Inc.*, 972 F.3d 1367, 1373 (Fed. Cir. 2020) (applying § 112, ¶ 6 to “logic to modify”). Instead, the phrase “remediation host” was specifically “invented . . . for one occasion only”—it exists solely in the asserted patents and their patent family. *Id.* Indeed, the phrase “remediation host” does not appear in any other patent or patent application outside the family of the asserted patents. Ex. 16. It was “coined for the purposes of the patents-in-suit.” *Diebold Nixdorf, Inc. v. ITC*, 899 F.3d 1291, 1302 (Fed. Cir. 2018) (applying § 112, ¶ 6 to “symbol generator”).

The individual words in “remediation host” further demonstrate the means-plus-function format. Contemporaneous dictionary definitions establish that “host” is a verbal construct that serves as shorthand for any computer that can perform a function. The Comprehensive Dictionary of Electrical Engineering defines “host” as “a computer that is the one responsible for **performing a certain computation or function.**” Ex. 17 at 312. Similarly, the Microsoft Computer Dictionary explains that a “host” “**provides services, such as news, mail, or data,** to computers that connect to it.” Ex. 18 at 256. The term “host” thus is no different than traditional nonce terms such as “device,” “module,” and “unit”—all of which merely serve as “placeholders” for anything that can perform a functionality. *Optis Cellular Tech., LLC v. Apple Inc.*, 139 F.4th 1363, 1382 (Fed. Cir. 2025). The same holds true here. Moreover, using the modifier “remediation” before “host” fails to connote any structure. “Remediation” is “simply an adjective describing” the function of “host” and “not a structure or material capable of performing the identified function.” *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007). Such prefixes that “merely describe[] the function[s]” “do[] not impart structure.” *Rain Computing, Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1006 (Fed. Cir. 2021).

Turning to the phrase “configured to,” the Federal Circuit repeatedly holds that “claim language reciting what [a term] is ‘configured to’ do is functional.” *MTD Prods. Inc. v. Iancu*, 933 F.3d 1336, 1343 (Fed. Cir. 2019). Terms such as “configured to” are “functional and do not supply a ‘sufficiently definite’ structure.” *Optis*, 139 F.4th at 1382.

And the last phrase “provid[ing] data usable to remedy the insecure condition” is entirely functional and devoid of structure. Such “purely functional claim language reciting what the [remediation host] is configured to do provides no structure.” *Rain*, 989 F.3d at 1006. Indeed, the phrase “provid[ing] data usable to remedy the insecure condition” is effectively identical to the “remediation” prefix because “both describe the same purely functional characteristics of an undefined and uncertain [remediation host].” *WSOU Investments LLC v. Google LLC*, 2023 WL 6531525, at *4 (Fed. Cir. 2023). This renders the “claim limitation self-referential” and fails to impart any structure. *Id.* In short, the limitation describes the function (*i.e.*, remediates), but not the structure or how the function is performed.

The Specification Reinforces That The Term Is Means-Plus-Function. The closest the specification comes to discussing a “remediation host” is referencing “remediation host name” without providing any structure. ’705 Patent, 16:10-31. The specification merely states that a “remediation host name may include a host name as appropriate to the reason for a quarantine, such as a *host providing anti-contagion software, or a host providing security updates, or a host internal to (or partnered with) an ISP.*” *Id.*, 16:19-23. The patent’s repeated use of “providing” following “host” demonstrates the functional characterization of host in this passage and fails to provide any definite structure. This is precisely what *Williamson* contemplates by directing that § 112, ¶ 6 applies when the term recites function without reciting sufficient structure for performing that function. Moreover, the usage of “host” in other contexts, such as “infected hosts,”

“quarantined host,” and “requesting host” (*id.*, 2:26, 12:25, 6:45), confirms that “host” is a generic placeholder for something “performing a certain computation or function,” Ex. 17 at 312.

The Specification Fails To Disclose Corresponding Structure. The inquiry next turns to “whether the specification discloses sufficient structure that corresponds to the claimed function.” *Diebold*, 899 F.3d at 1303. The specification fails to provide **any** structure—let alone sufficient structure—to perform the claimed function of “provid[ing] data usable to remedy the insecure condition.” The specification provides no disclosure of how a “remediation host” provides anti-contagion software or security updates as described in column 16. ’705 Patent, 16:19-23; ’048 Patent, 16:46-50. “If the function [of remediating] is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification **disclose the algorithm** that the computer performs to accomplish that function.” *Rain*, 989 F.3d at 1007. Here, the specification fails to disclose any algorithm. Nor does the specification provide any other disclosed structure for carrying out that specific function of remediating. At bottom, “[n]othing in the written description . . . adds sufficiently to the meaning of the term’s structure; it only describes the term’s function and interactions with other parts in the system.” *Media Rights Techs., Inc. v. Capital One Fin. Corp.*, 800 F.3d 1366, 1373 (Fed. Cir. 2015). “This type of purely functional language, which simply restates the function associated with the means-plus-function limitation, is insufficient to provide the required corresponding structure.” *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1317 (Fed. Cir. 2012). This term is indefinite.

CONCLUSION

Google respectfully requests that this Court adopt Google’s proposed constructions.

Dated: August 26, 2025

Respectfully submitted,

By: Shaun W. Hassett, with permission for
Tharan Gregory Lanier
Tharan Gregory Lanier (*Admitted Pro Hac Vice*)
tgranier@jonesday.com
Evan McLean (*Admitted Pro Hac Vice*)
emclean@jonesday.com
JONES DAY
1755 Embarcadero Road
Palo Alto, CA 94303
Telephone: +1.650.739.3939
Facsimile: +1.650.739.3900

Michael A. Lavine (*Admitted Pro Hac Vice*)
mlavine@jonesday.com
JONES DAY
555 California Street, 26th Floor
San Francisco, CA 94104
Telephone: +1.415.626.3939
Facsimile: +1.415.875.5700

Sachin M. Patel (*Admitted Pro Hac Vice*)
smpatel@jonesday.com
JONES DAY
110 North Wacker Drive, Suite 4800
Chicago, IL 60606
Telephone: +1.312.782.3939
Facsimile: +1.312.782.8585

Michael E. Jones
TX State Bar No. 10929400
mikejones@potterminton.com
Shaun W. Hassett
TX State Bar No. 24074372
shaunhassett@potterminton.com
POTTER MINTON
102 N. College Ave., Suite 900
Tyler, TX 75702
Telephone: +1.903.597.8311
Facsimile: +1.903.593.0846

Counsel for Defendant Google LLC