

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO. LTD.
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

Case No. IPR2025-00482
Patent No. 11,405,429

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. Introduction 1

II. Overview of the '429 Patent 1

III. Level of Ordinary Skill in the Art.....3

IV. Claim Construction 4

V. The Petition fails to establish “a secure execution environment, separately
secure from [a] secure modem subsystem” as all challenged claims
require. 5

 A. Overview of the Petition’s theory 5

 B. The Petition fails to provide any plausible theory for how the
alleged “secure execution environment” is “separately secure
from” the alleged “secure modem subsystem” as all claims
require. 9

VI. Conclusion 13

PATENT OWNER'S EXHIBIT LIST

No.	Description
2001	DocketNavigator statistics regarding motions to stay pending IPR decided by Judge Gilstrap
2002	August 9, 2024 Docket Control Order in <i>Headwater v. Samsung</i> , Case No. 2:24-CV-00228-JRG-RSP (E.D. Tex.)
2003	DocketNavigator statistics regarding average time to trial in the Eastern District of Texas
2004	Headwater's July 12, 2024 Infringement Contentions in <i>Headwater v. Samsung</i> , Case No. 2:24-CV-00228-JRG-RSP (E.D. Tex.)
2005	Samsung's September 12, 2024 Invalidity Contentions in <i>Headwater v. Samsung</i> , Case No. 2:24-CV-00228-JRG-RSP (E.D. Tex.)
2006	Declaration of Erik de la Iglesia in Support of Patent Owner's Preliminary Response to Petition
2007	<i>Curriculum vitae</i> of Erik de la Iglesia

I. Introduction

The Board should deny institution of *inter partes* review (“IPR”) of U.S. Patent No. 11,405,429 (“the ’429 patent”), because the Petition fails to apply or even address the plain meaning of the claims.

Specifically, all challenged claims recite “a secure execution environment, separately secure from [a] secure modem subsystem.” The Petition relies on two references, Schmidt and De Beer, for this limitation, alleging that both the secure execution environment and secure modem subsystem components are (1) secure and (2) separate from one another. The claim does not, however, recite “a secure execution environment that is *separate* from [a] secure modem subsystem,” it requires “a secure execution environment, *separately secure* from [a] secure modem subsystem.” In the prior art, the alleged “secure modem subsystem” is *directly responsible* for the security of the alleged “secure execution environment” (such that their security is anything but “separate”), and the Petition provides no plausible explanation as to how these two components would be *separately* secure from one another.

II. Overview of the ’429 Patent

At a high level, the ’429 patent is directed to a method of operating an end-user device that involves two secure control channels, one of which is used for communicating service policy settings that are stored in a secure environment for

later enforcement.

More specifically, the only independent claim (Claim 1) recites:

- [1.1] A method of operating a wireless end-user device, the method comprising:
- [1.2] connecting from *a secure modem subsystem* to a wireless cellular network;
- [1.3] connecting a first secure control channel from the secure modem subsystem through the wireless cellular network to a network service controller;
- [1.4] connecting a second secure control channel from *a secure execution environment, separately secure from the secure modem subsystem*, through the secure modem subsystem and the wireless cellular network to the network service controller;
- [1.5] receiving at the secure execution environment, via the second secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more service policy settings;
- [1.6] storing the one or more service policy settings in a secure memory partition accessible only from the secure execution environment; and
- [1.7] enforcing, at least in part from the secure execution environment, a network service profile comprising the one or more service policy settings, to control the wireless end-user device use of a service on the wireless cellular network.

Ex. 1001, Claim 1.¹

As shown above, the claim recites a “secure execution environment” that must be “*separately secure* from the secure modem subsystem.” The specification explains that this separate security between, for example, protected device assisted service execution partition 114 and modem execution partition 124 may be provided via a “separate hardware security function” from modem execution partition 124. *See* Ex. 1001, 5:1-6:60 & FIG. 1; *id.* at 6:12-16 (“[T]he protected DAS partition 114 is a protected execution on the main device that is supported by certain configurations in the host (e.g., a secure virtual execution environment or a *separate hardware security function*).”).

III. Level of Ordinary Skill in the Art

The Petition proposes that a POSITA in the field of the '429 patent would have “(1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication network device applications and software. Additional education could substitute for industry experience, and *vice versa*.” Pet. 2-3 (internal citation omitted). For purposes of this Preliminary Response, Patent Owner does not challenge that definition.

¹ The Petition’s claim numbering is used throughout this preliminary response. All emphases in quotations is added by Patent Owner unless otherwise specified.

IV. Claim Construction

“Petitioner submits that no formal claim constructions are necessary....” Pet.

2. For purposes of this Preliminary Response, Patent Owner agrees and applies the plain meaning of the claim language.

Patent Owner does note however, as explained in further detail below, that the Petition ignores the plain meaning of the claim language “a secure execution environment, separately secure from the secure modem subsystem.” The Petition seems to contend that this limitation is satisfied as long as these two components (the secure execution environment and the secure modem subsystem) are both (1) secure and (2) separate from one another. *See* Pet. 48 (alleging that this requirement is satisfied because the prior art discloses “*separate* trusted” subsystems and “protected, *separate* section environments.” Pet. 48 (emphases in original).

Patent Owner submits that Petitioner’s interpretation in this regard rewrites “separately secure from” to merely mean “separate from,” such that the claim language as understood by Petitioner would read: “a secure execution environment, separate from the secure modem subsystem.” The claim *already* recites that both the claimed execution environment and the claimed secure modem subsystem are “secure.” *See* Ex. 1001, Claim 1 (reciting a “*secure* modem subsystem” and a “*secure* execution environment”). Thus, in order for “secure” in “separately secure” to have meaning, the claim’s recitation of “separately secure” requires separateness

of the security of the secure modem subsystem and the secure execution environment, and cannot be satisfied merely based on an allegation that the two secure components be conceptually “separate” from one another.

V. The Petition fails to establish “a secure execution environment, separately secure from [a] secure modem subsystem” as all challenged claims require.

A. Overview of the Petition’s theory

Claim 1 of the ’429 patent requires a “secure execution environment” that is “*separately secure*” from a “secure modem subsystem.”

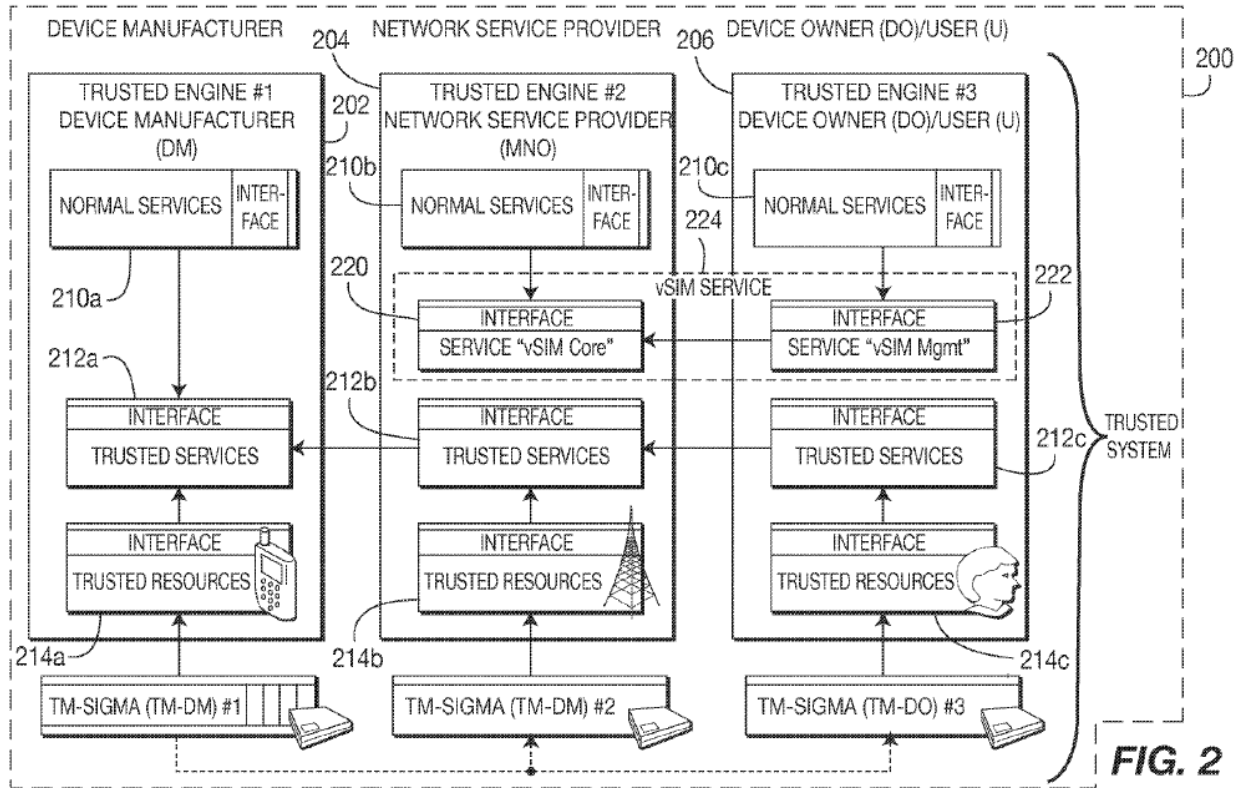
The Petition’s mapping of the claim language to the prior art is arguably difficult to follow, largely owing to the large amount of abbreviations used in the Petition, as well as the exemplary, non-committal nature of the Petition’s analysis. *See, e.g.*, Pet. 43 (alleging that the prior art discloses “a SEE (e.g, TSS-MNO/TM-SIGMA), separately secure from the secure modem subsystem, through the secure modem subsystem (e.g., TSS_DM with TX/RX)”). However, Patent Owner provides the following summary of its understanding of the Petition’s theory, based on statements by Petitioner’s expert and the Petition’s annotations of prior art figures.

The Petition contends that the “secure execution environment” of the claims is met by Schmidt’s “TSS-MNO.” *See* Pet. 44 (providing an annotated figure with “secure execution environment” annotated in green), 48 (referencing “SDD’s SEE

(TS-MNO/TM_SIGMA)"); Ex. 1003 at ¶233 (referencing "SDD's secure execution environment (TSS-MNO)").² TSS-MNO appears to be an abbreviation for "trusted subsystem – mobile network operator," because Schmidt describes the TSS-MNO as a "mobile network operator-trusted subsystem... configured to store and provide credentials related to a mobile network operator." Ex. 1005, [0005]; *see also* Pet. 6 (the Petition describing TSS-MNO as a trusted subsystem "that operate[s] on behalf of... the network service provider").

Schmidt's TSS-MNO (i.e., the alleged "secure execution environment") is depicted by "TRUSTED ENGINE #2" along with "the underlying TM-SIGMA (TM-DM) #2" in Schmidt's FIG. 2, reproduced below.

² The Petition's mapping of the claim language to the prior art may appear difficult to discern, due to the volume of abbreviations used in the Petition, as well as the exemplary, non-committal nature of the Petition's analysis. *See, e.g.*, Pet. 43 (alleging that the prior art discloses "a SEE (e.g., TSS-MNO/TM-SIGMA), separately secure from the secure modem subsystem, through the secure modem subsystem (e.g., TSS_DM with TX/RX)"). However, the Petition's theory is clarified by the corresponding expert declaration as well as various annotations of prior art figures included with the Petition.



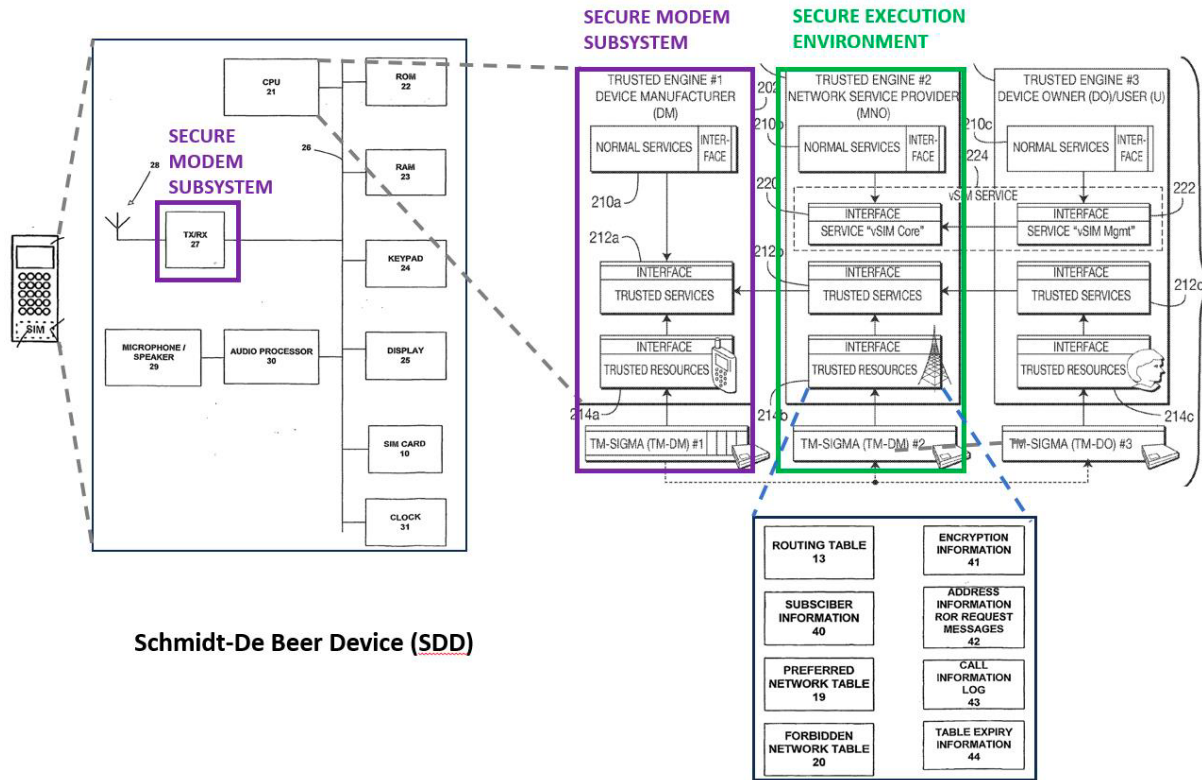
Ex. 1005, FIG. 2; *see also* Pet. 44, 53 (specifically identifying these elements as constituting the “secure execution environment”).

For the “secure modem subsystem” limitation, the Petition relies on Schmidt in combination with De Beer. Specifically, the Petition proposes that a modem including transceiver (TX/RX) circuitry 27 from De Beer’s FIG. 2, in combination with Schmidt’s TSS-DM (“TRUSTED ENGINE #1” from Schmidt’s FIG. 2 along with the underlying “TM_SIGMA (TM-DM) #1”), would allegedly constitute the “secure modem subsystem” as claimed. *See* Pet. at 34-35 (providing an annotation showing the “secure modem subsystem” as including those elements); *id.* at 31 (“SDD’s wireless modem (including the transceiver components) and TSS-DM

together serve as a secure modem subsystem that facilitates the device's network communications."); Ex. 1003, ¶233 (specifying that "the secure modem subsystem" includes "SDD's transceiver circuitry operating in conjunction with TSS-DM").

In this context, "TSS-DM" is an abbreviation for "trusted subsystem – device manufacturer," because Schmidt makes clear that "TSS-DM" is a reference to "a device manufacturer-trusted subsystem... configured to store and provide credentials related to a manufacture[r] of the [mobile trusted platform]." Ex. 1005, [0005]; *see also* Pet. 6 (describing the TSS-DM as a trusted subsystem "that operate[s] on behalf of the device manufacturer").

The Petition's annotated diagrams showing these elements of the proposed combined system—with the "secure execution environment" being mapped to the mobile network operator subsystem (TSS-MNO), and the "secure modem subsystem" being mapped to transceiver circuitry (TX/RX) in addition to the device manufacturer subsystem (TSS-DM)—is reproduced below.



Pet. 35 (Petition’s annotations of portions of Figures 1-2 of Ex. 1005, and Figure 2 of Ex. 1006).

B. The Petition fails to provide any plausible theory for how the alleged “secure execution environment” is “separately secure from” the alleged “secure modem subsystem” as all claims require.

As explained above, the Petition equates the claimed “secure execution environment” to be the TSS-MNO (a trusted execution environment related to a network service provider), and the “secure modem subsystem” to be transceiver circuitry in combination with the TSS-DM (which is a trusted subsystem related to device manufacturer). The Petition further contends that the TSS-MNO (the alleged “secure execution environment”) is “separately secure from” the TSS-DM (the

alleged “secure modem subsystem”) as claim 1 of the ’429 patent would require. Pet. 43, 48.

However, as explained by Patent Owner’s expert Erik de la Iglesia, the security of these two components is not “separate” because the TSS-DM “provides *all* security sensitive resources for [the] device” (Ex. 1005 ¶32), such that the TSS-MNO *cannot* be “separately secure from” the alleged secure modem subsystem (TSS-DM plus transceiver circuitry); indeed, the security of the TSS-MNO is highly reliant on the security of the TSS-DM. *See* Ex. 2006 ¶¶31-35.

As Mr. de la Iglesia explains, the TSS-DM *also* “controls *all* internal and external communications” within the device, which “necessarily includes all communications to and from the TSS-MNO subsystem (as well as communications within that subsystem).” Ex. 2006 ¶32 (citing Ex. 1005, [0032]) (emphasis in original). Accordingly, a POSITA would recognize that the security of the components the Petition alleges to be the secure execution environment (TSS-MNO) and secure modem subsystem (TSS-DM plus TX/RX circuitry) “is highly integrated and that the TSS-DM is responsible for securing the TSS-MNO, such that a POSITA would not understand these two systems to be *separately* secure from one another under the plain meaning of that term.” Ex. 2006 ¶32.

The Petition’s explanation of why the two alleged components would be “separately secure” from one another is sparse, but the Petition seems to imply two

distinct theories. **First**, the Petition appears to imply that if two subsystems are both (1) secure and (2) separate from one another, then those two subsystems are by definition “separately secure.” See Pet. 48 (alleging the TSS-MNO to be “separately secure from” the transceiver circuitry plus TSS-DM because they are “separate from” one another and “*each* is a separate secure/trusted execution environment”) (emphasis in original).

Regarding this first theory, however, the Petition improperly rewrites “a secure execution environment, *separately secure from* the secure modem subsystem” to mean “a secure execution environment, ~~*separately secure from*~~ the secure modem subsystem.” Of course, as discussed above in Section IV, the claim *already* recites that both the “execution environment” and “modem subsystem” are “secure.” See Ex. 1001 at claim 1 (reciting “a *secure* execution environment” and “a *secure* modem subsystem”) (emphases added). Thus, under the theory of the Petition, the “separately secure from” language could be satisfied so long as each *secure* component were “separate from” one another.

However, a POSITA would not interpret the claim in this manner, because “the claim does not merely require that the two systems be ‘separate’ and ‘secure,’ but instead requires that they be *separately secure* such that the security of one is separate from the security of the other.” Ex. 2006 ¶33. And this plain meaning understanding of the claim language “is certainly not [satisfied] here,” because “the

TSS-DM is responsible for controlling all communications to, from, and within the TSS-MNO” (Ex. 2006 ¶33), in addition to “providing all security sensitive resources for [the] device” (Ex. 2006 ¶34, quoting Ex. 1005, [0032]).

Second, the Petition implies that the two subsystems (TSS-MNO and TSS-DM in combination with transceiver circuitry) “are separately secure because *each*... ‘is [also] configured to sign and encrypt any given data.’” Pet. 48. But as explained by Mr. de la Iglesia, the fact that communications use encryption does not mean that one is “separately secure from” the other given that the TSS-DM provides *all* security sensitive resources for the device and controls *all* internal and external communications within the device. Ex. 2006 ¶34 (quoting Ex. 1005, [0032]).

At most, each subsystem’s use of encryption mechanisms would imply that *communications from* each subsystem might be independently secured, but would not show that the TSS-MNO itself is “separately secure from” the TSS-DM and transceiver. Again, the separateness of the security of the TSS-MNO from the TSS-DM *cannot* be satisfied here given the “extraordinarily high level of security independence” of the TSS-MNO on the TSS-DM as explicitly disclosed in Schmidt itself and confirmed by Mr. de la Iglesia. *See* Ex. 2006 ¶34.

Accordingly, the Petition fails to set forth a reasonable likelihood of prevailing as to its sole challenge to claim 1 of the ’429 patent. And because claim 1 of the ’429 patent is the *only* independent claim of the patent, the Petition fails to

set forth a reasonable likelihood of success as to any challenged claim, such that institution should be denied.

VI. Conclusion

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition.

Date: May 27, 2025

Respectfully submitted,

/James A. Milkey/

Reza Mirzaie, Reg. No. 69,138

Marc A. Fenster, *pro hac vice* forthcoming

Dale Chang, Reg. No. 61,476

Neil A. Rubin, Reg. No. 67,030

Philip X. Wang, Reg. No. 74,621

James A. Milkey, Reg. No. 79,503

RUSS, AUGUST & KABAT

12424 Wilshire Blvd., 12th Floor

Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATION REGARDING WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Patent Owner certifies that there are 2,331 words in the paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: May 27, 2025

/James A. Milkey/

Reza Mirzaie, Reg. No. 69,138

Marc A. Fenster, *pro hac vice* forthcoming

Dale Chang, Reg. No. 61,476

Neil A. Rubin, Reg. No. 67,030

Philip X. Wang, Reg. No. 74,621

James A. Milkey, Reg. No. 79,503

RUSS, AUGUST & KABAT

12424 Wilshire Blvd., 12th Floor

Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e)(1))

The undersigned hereby certifies that the above document was served on May 27, 2025, by filing this document through the Patent Trial and Appeal Case Tracking System (PTACTS) as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
IPR39843-0185IP1@fr.com
PTABInbound@fr.com

Date: May 27, 2025

/James A. Milkey/
Reza Mirzaie, Reg. No. 69,138
Marc A. Fenster, *pro hac vice* forthcoming
Dale Chang, Reg. No. 61,476
Neil A. Rubin, Reg. No. 67,030
Philip X. Wang, Reg. No. 74,621
James A. Milkey, Reg. No. 79,503
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner