

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

OKTA, INC.,
Petitioner,

v.

THALES DIS FRANCE SAS,
Patent Owner.

Case IPR2026-00278
Patent No. 11,387,982

PATENT OWNER'S PRELIMINARY RESPONSE

Table of Contents

List of Exhibits.....	iii
I. INTRODUCTION	1
II. TECHNOLOGY BACKGROUND.....	3
A. Authentication Using Mutable Context Data.....	3
B. Asserted References	4
1. Starner (EX1004)	4
2. Leskovec (EX1007)	5
III. THE ’982 PATENT.....	6
A. Overview of the ’982 Patent and Independent Claim 1	6
B. Prosecution History Summary	8
IV. THE PETITION FAILS TO ESTABLISH A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE OBVIOUS.....	10
A. Petitioner Fails to Establish All Claim Limitations	10
1. Petitioner Improperly Relies on Declarant Assumptions for Missing Limitation “wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet.” [1.6.2].....	11
2. Starner and Leskovec Fail to Teach Generating a <i>Hash</i> Distance [1.5]	13
3. Starner and Leskovec Fail to Teach, “wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet” [1.6.3]	16

B.	Deficiencies of the Starner Leskovec Combination Cannot be Overcome	19
V.	CONCLUSION.....	21

List of Exhibits

Exhibit	Description
2001	Prosecution History of U.S. Patent Application No. 16/958,252.
2002	Administrative Instructions under the Patent Cooperation Treaty, Part 8, Instructions Relating to Observations by Third Parties, Section 801, Third Party Observation System, https://www.wipo.int/en/web/pct-system/texts/ai/s801#_801_a (captured May 5, 2026).
2003	Thales Group United States - About Us, https://www.thalesgroup.com/en/worldwide/united-states/about-us (captured May 5, 2026).
2004	Thales Defense and Security Inc. – Manufacturing, https://www.thalesdsi.com/manufacturing/ (captured May 5, 2026).
2005	International Patent Application Publication No. WO 2019/129422.
2006	Jonathan Vanian, <i>This Enterprise Software Unicorn Just Filed to Go Public</i> , Fortune Magazine (Mar. 13, 2017), https://fortune.com/2017/03/13/okta-cybersecurity-public/ .
2007	Agam Shah, <i>Made-in-China Servers Attracting More Buyers</i> , CIO (Mar. 9, 2016), https://www.cio.de/article/3686856/made-in-china-servers-attracting-more-buyers-4.html .

I. INTRODUCTION

The '982 Patent relates to novel and inventive systems and methods for efficient, secure user authentication using context data while reducing bandwidth usage tied to context-based authentication processes. EX1001 at 1:38–51, 3:4–5. The Petition fails to establish a reasonable likelihood of prevailing on any of its obviousness grounds as it does not specify where each claim element is found in the prior art, does not provide a proper motivation for modifying its primary reference, and does not establish a reasonable expectation of success for any such modification.

Petitioner's grounds are based on Starner (EX1004) as a primary reference, alleging obviousness of claims 1–10 of the '982 Patent in four grounds (1A–D). However, Starner does not teach the claim limitations alleged in the Petition. *Infra* §§ IV.A.1–3. Despite Petitioner's allegations (Paper 2, Pet., at 19–22, 32), Starner does not teach at least feature 1.6.2, “wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet,” which was relied upon by the Examiner in the Reasons for Allowance in the Notice of Allowability issued April 19, 2022. *See infra* § IV.A.1; EX2001 at 13–23. Petitioner relies on a reference to its discussion related to feature 1.1 (“collecting, based on a predetermined authentication policy, at least one context data element”) where Petitioner's declarant makes a series of logical leaps to

conclude that a digital template representing patterns in the eye-scan data in Starner corresponds to the “captured image represented as a string of bits with a fixed length constituting a data packet.” Paper 2, Pet., at 19–22, 32. This is impermissible. “[E]xpert testimony ... may not be used to supply a missing claim limitation.” Memorandum from Coke Morgan Stewart, Under Sec’y of Com. for Intellectual Prop. & Acting Dir. of the U.S. Patent & Trademark Office, to Members of the Patent Trial and Appeal Board, at 1 (July 31, 2025) (“Rule 42.104(b)(4) Enforcement Memo”) (“Per 35 U.S.C. § 312(a)(4), the Board shall deny an IPR petition that fails to comply with Rule 104(b)(4).”).

Petitioner further fails to show that Starner in combination with Leskovec (EX1007) teaches to “generate a hash distance” (limitation 1.5), where in fact, Starner teaches away from any such generation. *Contra* Paper 2, Pet., at 26–30. Indeed, Starner praises the security of exact hash matching that eliminates any need to store actual images, unlike use of the Hamming Distance, which Petitioner relies on as corresponding to a hash distance as recited in the claims of the ’982 Patent. *See infra* § IV.A.2.

Moreover, Petitioner’s attempt to create disclosure in the Starner and Leskovec combination related to limitation 1.6.3, namely, the hash being a byte stream, also fails. *Contra* Paper 2, Pet., at 32–34. Indeed, the concept of a byte

stream appears nowhere in the disclosures of Starner and Leskovec, forcing Petitioner to formulate its grounds on extrinsic, unasserted references, which still fail to remedy the deficiencies of Starner and Leskovec. *See infra* § IV.A.3.

Institution should thus be denied under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.104(b)(4).

II. TECHNOLOGY BACKGROUND

A. Authentication Using Mutable Context Data

Context data authentication, as described by the '982 Patent, relates to variable, contextual environment data collected at a first device during an authentication request, and using that data to authenticate a user. *See generally* EX1001.

In prior systems, context-based authentication was performed by sending “entire” context data element(s) to an authentication server, because unlike fixed data, such as usernames and passwords, context data elements can vary within acceptable limits. EX2001 at 72. In such systems, the complete context data was compared to determine a score associated with each environmental characteristic, and that score was compared to a predetermined reference score to determine whether or not to authorize. EX1001 at 1:26–37.

B. Asserted References

1. Starner (EX1004)

Petitioner's primary reference, Starner (EX1004), is directed to biometric authentication using a wearable computing device (e.g., head-mounted display ("HMD")) as a substitute for traditional passwords. EX1004 at ¶¶ [0020]–[0023]. The disclosed system enables a first computing device (e.g., HMD) to authenticate a user in response to detecting a machine-readable code displayed by a second computing device, and to grant access to protected information on the second computing device upon successful verification. *Id.* at ¶¶ [0020]. Starner emphasizes replacing or supplementing password-based authentication with automatically acquired biometric data, particularly in wearable computing environments. *Id.* at ¶¶ [0022], [0024].

Starner discloses processing biometric data to generate an authentication payload, which involves transforming the raw biometric input into a digital template by identifying patterns in the raw biometric input. *Id.* at ¶ [0077]. Starner describes transforming exemplary patterns such as light and dark image data that correspond to the dark pupil and the sclera to create the digital template, and that the digital templates may include 1024-byte records as 32x32x1 byte grayscale or color. EX1004 at ¶ [0077].

In Starner, a server compares received biometric data and the corresponding digital template with stored data to determine a match. *Id.* at ¶ [0090]. Two “match” determination techniques are described in Starner, the first being comparison of full biometric data (i.e., received eye-scan data and digital template) with the stored data using a Hamming Distance. *Id.* at ¶¶ [0090]–[0091]. The second determination technique is described by Starner as a matching of digital signatures generated using hash functions. *Id.* at ¶¶ [0092].

Starner is directed towards authentication based on immutable biometric data and lacks any disclosure related to the claimed context data element authentication and handling of variability in context data elements associated therewith. It therefore fails as a primary reference.

2. Leskovec (EX1007)

Leskovec is a textbook related to “[m]ining of [m]assive [d]atasets.” EX1007 at 1; *see generally* EX1007. Leskovec includes disclosure related to determining “similar” documents among millions, indeed billions, of documents, and implementation of hashing algorithms to make such determinations. *See, e.g.*, EX1007 at § 3.4.

In the context of finding similar documents, Leskovec describes implementations of various distance measures, such as Hamming Distance and Jaccard Distance. *See, e.g., id.* at §§ 3.5.6, 3.5.3.

Leskovec is entirely unrelated to authentication and security.

III. THE '982 PATENT

A. Overview of the '982 Patent and Independent Claim 1

The '982 Patent relates to novel and inventive systems and methods for efficient, secure user authentication using context data while reducing bandwidth usage tied to context-based authentication processes. EX1001 at 1:38–51, 3:4–5. In prior systems, context-based authentication was performed by sending “entire” context data element(s) to an authentication server, because unlike fixed data, such as usernames and passwords, context data elements can vary within acceptable limits. EX2001 at 72.

The '982 Patent explains that each context data element is “preferably a string of bits (or units of information) with an individual fixed length” and that by using a hash generated from each of these context data elements, rather than sending each context data element in its entirety for an authentication, “the invention solution does not need a large bandwidth to transmit data, including the hash, relating to the concerned environment or context, since the data relating to the concerned context

includes only a few data (up to a few kbytes) to be transmitted.” EX1001 at 1:66–2:4, 2:65–3:3, 6:51–52. Bandwidth, as one of skill readily understands in the context of mobile computing, is a key resource for which usage should be limited, particularly for administrative tasks like authentication, and Patent Owner succeeded in doing so by way of the claimed methods and systems. Independent claim 1 is representative for purposes of this Preliminary Response:

1. An authentication method comprising:
collecting, based on a predetermined authentication policy, at least one context data element;
constituting a data packet, based on the at least one collected context data element;
generating a hash, by using a predetermined hash type algorithm and the data packet, as input to the predetermined hash type algorithm
sending the generated hash;
generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash;
and
authenticating successfully or not based on the generated hash distance, as an authentication; wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet, and wherein said hash is a byte stream generated from said string of bits

representing said captured image for said data packet.

B. Prosecution History Summary

International Application PCT/EP2018/081759 included 15 claims, with claims 1, 11, 13, and 15 being independent. EX2005 at 23–26. Upon entry to the U.S. National Stage as the '252 application, Patent Owner filed a preliminary amendment cancelling claims 1–15 and replacing them with claims 16–25. EX2001 at 323, 325–29. In advance of the first non-final office action, Patent Owner filed two IDSs disclosing all references identified during searches carried out by the corresponding international and European authorities in the counterpart applications. EX2001 at 138–45, 220–22.

The Examiner initially rejected the original claims as obvious over the combination of Lawrence (EX1028), Cheng (EX1029), Aura (EX1030), and Sakamoto (EX1031), alleging that they collectively taught all elements of the claims. EX2001 at 91–96. In doing so, the Examiner acknowledged that Lawrence did not disclose, among other things, (1) “collecting, based on a predetermined authentication policy, at least one context data element,” (2) “generating, as a hash distance step, a hash distance between the generated hash and a predetermined reference hash,” and (3) “authenticating successfully or not based on the generated hash distance, as an authentication step.” EX2001 at 92–94.

In response, Patent Owner did not amend the claims, but instead argued the impropriety of the rejections, namely that (1) Lawrence does not teach the features acknowledged as lacking by the Examiner and (2) Cheng does not remedy the deficiencies of Lawrence because everything in Cheng happens internally to the computing system so neither a hash, nor a hash distance, is needed for authentication. EX2001 at 73–75. Patent Owner further argued that any hash assessment in Aura was not for authentication but for selecting the most secure hash value, and that Sakamoto has nothing to do with the claims and does not remedy any of the noted deficiencies. EX2001 at 75–79. Thus, Patent Owner concluded that the combination of references did not teach at least the claimed steps of (1) “generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash” and (2) “authenticating successfully or not based on the generated hash distance as an authentication step.” EX2001 at 79.

The Examiner contacted Patent Owner's representative by telephone on April 5, 2022, to propose amendments, namely:

- i) wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet,
- ii) and wherein said hash is a byte stream generated from said string of

bits representing said captured image for said data packet.

EX2001 at 18–21, 24.

Patent Owner accepted these amendments, and they were added to the claims by Examiner's Amendment in the Notice of Allowance. EX2001 at 13–23. The Examiner explicitly relied upon the above limitations in allowing the claims. EX2001 at 21–22.

IV. THE PETITION FAILS TO ESTABLISH A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE OBVIOUS

A. Petitioner Fails to Establish All Claim Limitations

Petitioner alleges that Starner discloses generating, as a hash distance generation step, a hash distance between the generated hash and a predetermined reference hash (limitation 1.5); wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet (limitation 1.6.2); and wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet (limitation 1.6.3). *See generally* Paper 2, Pet., at 19–22, 26–30, 32–34. Petitioner's grounds, however, fail to demonstrate that the combination of Starner and Leskovec discloses these limitations, instead relying on statements from its declarant to fill gaps in the disclosure. *See generally* Paper 2, Pet., at § V.

Moreover, Petitioner further relies on misinterpretations of Starner and Leskovec to support its allegations that the combination discloses the noted limitations.

1. Petitioner Improperly Relies on Declarant Assumptions for Missing Limitation “wherein said at least one context data element is a captured image represented as a string of bits with a fixed length for constituting said data packet.” [1.6.2]

Petitioner's mapping of Starner to feature 1.6.2 fails at least because Starner does not disclose the claimed “*captured image* represented as a string of bits with a fixed length....” Unable to identify that disclosure specifically, Petitioner resorts to sleight of hand referring back to limitation 1.1 (Paper 2, Pet., at 19–22), discussing Starner's “digital template” as a fixed length (e.g., “a 1024-byte data record”), and relying on its declarant's interpretation of this disclosure. Paper 2, Pet., at 32 (citing EX1003 at ¶ 153). However, Starner does not disclose this limitation, which was relied upon for allowance by the Examiner (EX2001 at 21–22), and the conclusory statements of Petitioner's declarant cannot cure the deficiencies of the reference.

Starner expressly distinguishes the underlying eye-scan image and the processed information, i.e., the *digital template*, derived from it. EX1004 at ¶ [0077]. Starner explains that eye-scan data is analyzed “to identify patterns in an iris, and convert the patterns into a *digital template*.” *Id.* (emphasis added). Starner further discloses that “the HMD may identify patterns of light and dark image data

that correspond the dark pupil and the sclera (e.g., the white of the eye) to create the *digital template*,” or “[i]n still another embodiment, the *digital template* may include a 1024-byte *record* (32x32xl byte grayscale or color).” *Id.* Thus, the digital template is a *derivative construct* created after processing of the captured biometric image; it is not the captured image itself. *Id.* Petitioner’s theory depends on erasing that distinction because, without doing so, Petitioner has no disclosure for the limitation it attempts to show.

Petitioner’s reliance on Starner’s reference to a “1024-byte record” only underscores the problem, namely a misreading of the reference. *See* Paper 2, Pet., at 20–21. In context, Starner states that the stored digital template may take the form of a 1024-byte record and that the “stored digital template may be used as stored eye-scan data,” which may take the form of a 1024-byte record. EX1004 at ¶¶ [0077], [0089]. But this discloses only that Starner stores the *digital template* in a fixed-size format, not the *captured image* of biometric data. As recited in claim 1 at limitation 1.6.2, the claimed “context data element” itself is “a captured image represented as a string of bits with a fixed length.” EX1001, Claim 1. Petitioner’s argument thus conflates three distinct concepts—captured image, extracted patterns for a digital template, and fixed-length stored record—because that conflation is the

only way to manufacture the limitation from Starner. The Board should reject the attempt.

This defect is fatal to Petitioner's grounds. The Board cannot find a missing disclosure based on attorney argument, labels, or expert testimony where the reference itself does not teach the claimed subject matter. Rule 42.104(b)(4) Enforcement Memo at 1. Here, Petitioner has not shown—because it cannot show—where Starner discloses a captured image represented as a string of bits with a fixed length for constituting said data packet. That failure alone defeats Petitioner's showing as to feature 1.6.2 and warrants denial of institution.

2. Starner and Leskovec Fail to Teach Generating a *Hash Distance* [1.5]

Petitioner's separate contention that Starner teaches "generat[ing] a hash distance" is equally untenable. *See generally* Paper 2, Pet., at 26–30. Petitioner asserts that because Starner authenticates when a later eye image "substantially matches" an earlier image, Starner must implicitly generate a hash distance. *Id.* at 27–28 (citing EX1004 at ¶ [0092]). This again misunderstands Starner.

Indeed, Starner explains that a locality specific hash (LSH) function allows *the same digital signature* to be generated from *different* eye scan images despite ordinary variations such as lighting or eye position. EX1004 at ¶ [0092]. It is important to understand that in Starner, the "digital signature" *is not* the same as the

“digital template.” The digital signature corresponds to a security artifact derived from the biometric data (i.e., hashed and encrypted) to provide additional security, while the digital template is created by identifying patterns in the raw biometric input, and storing the identified patterns in the template. *See, e.g., id.* at ¶¶ [0077]–[0078].

Petitioner appears to conflate these two concepts to create disclosure not actually present in Starner. *See* Paper 2, Pet., 27–28. In fact, Starner’s own discussion of Hamming Distance confirms just how far Petitioner’s theory departs from the actual disclosure: Starner discusses Hamming Distance only in connection with un-hashed biometric image information, i.e., either the eye scan data itself, or the *digital template* of the eye scan data. EX1004 at ¶¶ [0090]–[0091]. Starner then expressly contrasts that approach with its technique of generating encrypted digital signatures and determining whether the received digital signature *matches* (i.e., exactly) a stored digital signature associated with the user. *Id.* at ¶ [0092]. Starner even states that, under its digital signature-based process, “actual images of the wearer’s eye may never need to be stored...unlike processes that utilize calculation of a Hamming Distance.” *Id.* Petitioner’s theory ignores that express distinction because it must. *See* Paper 2, Pet., 27–28.

Starner's approach to the digital signatures effectively normalizes variation, via the LSH algorithm, before or during *digital signature* generation so that the resulting digital signatures match notwithstanding variation in the input images. *See* EX1004 at ¶ [0092]. Thus, the "substantial match" language pertains to the underlying eye images, while the operative authentication comparison in Starner is whether the resulting *digital signatures* match. *Id.* Petitioner's attempt to transform this match framework into "generation of a hash distance" has no support in Starner.

In view of the above, a person of ordinary skill reading Starner would understand it to disclose two different paradigms: (1) Hamming Distance analysis of full biometric image data/digital templates, or (2) the preferred comparison of digital signatures to find an exact match. EX1004 at ¶¶ [0090]–[0092]. Starner does not, however, disclose or even imply generation of a hash distance between digital signatures, let alone a hash distance between a generated hash and a predetermined reference hash. Petitioner's argument is therefore not a reasonable reading of Starner; it is an effort to rewrite Starner into something it never was.

Petitioner also fails to explain why a person of ordinary skill would have modified Starner to incorporate the type of hash-distance concept Petitioner attributes to Leskovec, particularly when Starner itself uses no hash distances whatsoever. *See* Paper 2, Pet., at 28–29. Starner affirmatively touts the security and

operational advantages of its digital signature matching approach, including the ability to avoid storing underlying biometric images. EX1004 at ¶ [0092]. Yet Petitioner asks the Board to graft onto that framework a fundamentally different similarity analysis drawn from a reference directed to large-scale data mining. *See* Paper 2, Pet. at 28–30. Petitioner offers no persuasive reason for doing so—only hindsight by its declarant in view of the '982 Patent. *Id.* (citing EX1003 at ¶¶ 147–48). That is not enough: the opinions of the declarant do not change or add to the disclosure of the references. Obviousness cannot be established by plucking an abstract concept from a textbook and forcing it onto another that teaches away from the modification. Because Petitioner has not shown that Starner discloses, suggests, or would have been modified to perform the claimed generation of a hash distance—let alone authentication based on that generated hash distance—this ground fails as a matter of law and fact.

3. Starner and Leskovec Fail to Teach, “wherein said hash is a byte stream generated from said string of bits representing said captured image for said data packet” [1.6.3]

Citing paragraphs [0062], [0077], [0078], [0089], and [0092] of Starner, Petitioner alleges that, based on the *digital template*, the biometric images captured by Starner form the recited data packet. Paper 2, Pet., at 32. Petitioner then alleges that, based on the *digital signature*, and in view of its declarant's testimony, Starner

teaches the recited “byte stream.” *Id.* (citing EX1003 at ¶ 156; EX1004 at ¶¶ [0078], [0092]). This again demonstrates a clear misinterpretation of Starnier for purposes of generating disclosure not existing therein, and upon which the Examiner relied for allowance. *See* EX2001 at 21–22. As described above, the digital template and the digital signature of Starnier are two separate and distinct concepts, neither of which are combined with the other for any purpose in Starnier. *See supra* §§ IV.A.1–2.

Apparently recognizing this deficiency, Petitioner turns to Leskovec. Paper 2, Pet., at 33. However, this reliance is misplaced. While Leskovec describes techniques for mining “data streams” (*See, e.g.*, EX1007 at § 4), one of skill would understand that a “data stream” is a broad term referring to a sequence of structured or formatted data elements (such as text, integers, objects, or packets) being continuously *transmitted or processed*. In contrast, one of skill would understand that a “byte stream” is a sequential flow of *8-bit binary chunks* (bytes) over time. In other words, disclosure of a data stream and its processing by Leskovec does not disclose a byte stream, let alone a byte stream generated from said string of bits representing said captured image.

Petitioner cites specifically to Leskovec’s disclosure of use of the minhash algorithm to create a minhash signature, and more particularly, that the minhash

signature for a “set” is vector $[h_1(S), h_2(S), \dots, h_n(S)]$ ”, where $h_1, h_2, \dots, h_n(S)$ are permutations that determine the minhash function and are represented as a column. Paper 2, Pet., at 33 (citing EX1007 at original page 78). Relying on testimony of its declarant, Petitioner then cites to an unasserted reference, ISO/IEC 14882 (EX1060) disclosing “[t]he elements of a vector are *stored* contiguously” (emphasis added), and alleges that the vector of values corresponds to the recited byte stream. Paper 2, Pet., at 33 (citing EX1003 at ¶ 157). Petitioner has again tortured its interpretation of the reference to obtain disclosure otherwise lacking therein.

Notably, in addition to the disclosure reproduced by Petitioner at page 33 of the Petition, ISO/IEC 14882 also states that a vector “is a kind of sequence that supports *random access iterators*.” EX1060 at 4 (emphasis added). As one of ordinary skill in the art would understand, random-access iterators can be used to access elements *at an arbitrary offset position* relative to the element they point to, offering similar functionality to pointers. Thus, contiguous *storage* of vector values (such as in EX1060 at 4) says nothing of how elements of that vector are accessed, transmitted, or processed. Indeed, the elements of the vector may be processed in an exponentially large number of combinations, depending on the size of the vector (*Id.*), and disclosure of a “byte stream” does not even appear as one of those combinations in the portions of ISO/IEC 14882 provided.

Thus, neither Starner nor Leskovec, in combination with non-asserted references, discloses or even suggests a “byte stream” representation of a hash, let alone that byte stream being generated from a string of bits representing the captured image. *See supra* § IV.A.1. Petitioner must rely entirely on extrinsic materials, conclusory statements of its declarant, and tortured interpretations for allegations related to this limitation. *See* Paper 2, Pet., at 32–34. The disclosure cannot be found in the asserted references.

B. Deficiencies of the Starner Leskovec Combination Cannot be Overcome

The features discussed above underscore the gap between the claimed invention and the primary combination, namely, Starner and Leskovec, relied on in all four grounds. *See supra* §§ IV.A.1–3. Whereas the '982 Patent is directed to hash-based authentication using variable context data while preserving efficiency and limiting exposure of underlying data (*see e.g.*, EX1001 at 1:66–2:4, 2:65–3:5), Starner focuses on digital template creation or digital signature matching, both based on a user's biometric data. *See, e.g.*, EX1004 at ¶¶ [0077]–[0078]

That distinction is important because the variance in context data addressed by the '982 Patent is not variance in immutable biometric identity characteristics, but variance in ordinary contextual inputs surrounding an authentication event—such as environmental, situational, or device-related data—which may naturally

change from one login attempt to the next even for the same authorized user. EX1001 at 2:36–55, 13:50–53. In contrast, Starner's biometric data is used as authentication information tied to the user's physiological identity, and Starner's stated objective is to normalize incidental capture differences at the time of digital signature creation using an LSH algorithm so that the same digital signature is generated from substantially matching biometric data (e.g., eye images). *See, e.g.*, EX1004 at ¶ [0092]. Starner is not concerned with assessing whether variable contextual conditions are sufficiently similar under a risk-based policy. *Compare* EX1004 at ¶ [0092] *with* EX1001 at 13:50–53.

Leskovec is directed to large-scale data mining and, specifically, to identifying documents that are similar to one another across massive datasets for purposes of comparison and retrieval. *E.g.*, EX1007 at 27. That objective is fundamentally different from the '982 Patent, which is not concerned with document similarity, search, or retrieval, but with security—namely, comparing a reference hash of context data elements for a known user with a hash generated from context data elements for a user attempting authentication. *E.g.*, EX1001 at 2:36–55. Thus, the relevant inquiry in the '982 Patent is not whether items are sufficiently alike to be treated as related documents, but whether the variable user context presented during authentication is sufficiently similar to the context captured at enrollment to

support an authentication decision. *See, e.g., id.* Although general similarity concepts such as Jaccard distance or hash-based distance measures were known, there is no reason a person of ordinary skill would have looked to Leskovec's large-scale document-similarity techniques to solve the distinct, security-focused authentication problem addressed by the '982 Patent.

Petitioner, apparently recognizing these deficiencies, turns to extrinsic unasserted references, such as EX1063 and EX1064, to bolster its argument. Paper 2, Pet., at 32–33. However, like ISO/IEC 14882 (EX1060) discussed above, they do not and cannot remedy the deficiencies of the Starner and Leskovec combination. *See supra* § IV.A.3.

On this record, any attempt to combine Leskovec with Starner, and to remedy the deficiencies thereof with additional references, whether or not named in the grounds, rests not on a reasoned technical rationale but on impermissible hindsight.

V. CONCLUSION

The Petition falls well short of establishing a reasonable likelihood that Petitioner would prevail with respect to any challenged claim. *See* 35 U.S.C. § 314(a). Petitioner's analysis of claim 1, which also applies to the other independent claims, is not merely weak—it is built on a complete misinterpretation of Starner, Leskovec, and unasserted references. Petitioner repeatedly substitutes what the

claims require with what it wishes the references disclosed. These are not minor disputes over phrasing; they are fundamental defects in Petitioner's theory, and they independently preclude institution.

Dated: June 5, 2026

By: /Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP

Counsel for Patent Owner
Thales DIS France SAS

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, Patent Owner certifies that the word count of
PATENT OWNER'S PRELIMINARY RESPONSE as measured by Microsoft
Word is 4,584.

Dated: June 5, 2026

By: /Joshua L. Goldberg/
Joshua L. Goldberg, Reg. No. 59,369
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP

Counsel for Patent Owner
Thales DIS France SAS

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served electronically via email on June 5, 2026, in its entirety on the following:

Kenneth W. Darby, Jr.
Nicholas Stephens
Ryan Chowdhury
FISH & RICHARDSON P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
IPR56407-0019IP1@fr.com
PTABInbound@fr.com

Petitioner has consented to service by electronic mail.

Dated: June 5, 2026

/ William Esper /
William Esper
Senior Litigation Paralegal
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP