

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Fortinet, Inc.,

Petitioner,

v.

Netskope, Inc.,

Patent Owner.

Case No. 2026-00026

U.S. Patent 8,327,426

PETITION FOR *INTER PARTES* REVIEW

Mail Stop "PATENT BOARD"

Patent Trial and Appeal Board

U.S. Patent Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF ABBREVIATIONS	ix
EXHIBIT LIST	x
I. INTRODUCTION	1
II. GROUNDS FOR STANDING (37 C.F.R. §42.104(a)).....	1
III. THE PATENT AND STATE OF THE ART	2
A. User Accounts	2
B. Single Sign-On (SSO)	2
C. Federated Architectures	3
D. The '426 Patent	3
E. Challenged Claims	7
F. POSITA.....	11
IV. Claim Construction.....	11
V. SUMMARY OF CHALLENGE AND RELIEF REQUESTED.....	11
A. 37 C.F.R. §42.104(b)(1): The Challenged Claims	11
B. 37 C.F.R. §42.104(b)(1): Prior Art Overview and Specific Grounds of Rejection	11
1. Hinton	12
2. Overview of Burch.....	12
3. Grounds of Rejection	12

VI. GROUND 1 AND 2 – CLAIMS 1-4, 6-11, 13 ARE ANTICIPATED BY HINTON AND CLAIMS 1-13 ARE RENDERED OBVIOUS BY HINTON ALONE 12

A. Overview of Hinton..... 12

B. Claim 1 14

1. 1[pre]: "A machine-implemented method to execute on a machine, comprising:" 14

2. 1[a]: "receiving, by the machine, an authentication request from a principal, the request directed by the principal to an external service and intercepted by the method for receipt;" 15

3. 1[b]: "authenticating, by the machine, the principal; and" 17

4. 1[c]: "supplying, by the machine, an authentication message for use by an identity service on behalf of the principal," 17

5. 1[d]: "the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service," 18

6. 1[e]: "the identity service acts as a proxy for access sessions to the other services on behalf of the principal," 20

7. 1[f]: "the principal's access sessions occur indirectly through the identity service and transparently to the principal," 22

8. 1[g]: "wherein the authentication message includes the new authentication request made on behalf of the principal and the authentication message also includes a new authentication response that satisfies the new authentication request, that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal," 22

9.	1[h]: "the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to,"	23
10.	1[i]: "and a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response."	25
C.	Claim 2: "The method of claim 1 further comprising, making, by the machine, a target service available to interactions between the principal and an external service, the target service is directly accessible from an environment of the identity service."	27
D.	Claim 3: "The method of claim 1, wherein supplying further includes redirecting the principal to the identity service and including with the redirection the new authentication request and the new authentication response represented by the authentication message, and the identity service authenticates the principal automatically in response to the new authentication response included with the authentication message."	27
E.	Claim 4: "The method of claim 3, wherein supplying further includes representing the new authentication response as a first authentication token that informs the identity service that the principal is currently already properly authenticated to the processing associated with the method."	28
F.	Claim 5: "The method of claim 4, wherein supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service."	28

G.	Claim 6: "The method of claim 1, wherein supplying further includes representing the new authentication response as an instruction to the identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service.".....	29
H.	Claim 7: "The method of claim 1 further comprising, interacting, by the machine, with the principal via a World-Wide Web (WWW) browser over the Internet using at least one of a Security Assertion Markup Language (SAML), a Liberty Alliance markup language, and Web Services (WS) Foundation markup language."	30
I.	Claim 8	30
	1. 8[pre]: "A machine-implemented method to execute on a machine, comprising:"	30
	2. 8[a]: "receiving, by the machine, an authentication request and an authentication response as a single sign-on transaction from a principal,"	31
	3. 8[b]: "the authentication request and the authentication response are received indirectly from the principal via an original identity service acting as a proxy on behalf of the principal and"	31
	4. 8[c]: "actions of that original identity service are transparent to the principal and"	32
	5. 8[d]: "the authentication response produced by that original identity service to authenticate the principal for the single sign-on transaction,"	32
	6. 8[e]: "the authentication request and the authentication response produced by the original identity service are different from that which was originally provided by the principal to the original identity service and"	32

7.	8[f]: "the authentication request and the authentication response are made on behalf of the principal once the principal is authenticated by the original identity service;"	33
8.	8[g]: "detecting, by a machine and from an identity service, an instruction, which is represented in the authentication response,"	33
9.	8[h]: "the identity service is different from the original identity service, and the identity service and the original identity service are in a secure relationship with one another; and"	34
10.	8[i]: "taking, by the machine, an action in response to the instruction to authenticate the principal for access to targeted services,"	35
11.	8[j]: "access to the target services occur via proxied sessions through the identity service and transparent to the principal,"	35
12.	8[k]: "wherein the action taken is dynamic and a real-time evaluation of policies processed by the identity service.".....	35
J.	Claim 9: "The method of claim 8, wherein detecting further includes identifying the instruction as an assertion from the identity service that the principal is currently already authenticated to the identity service."	35
K.	Claim 10: "The method of claim 9, wherein taking further includes authenticating the principal, in response to the assertion, and supplying an authentication token to the principal indicating that the principal is authenticated for access to the targeted services."	36
L.	Claim 11: "The method of claim 8, wherein detecting further includes identifying the instruction as an identity service request from the identity service to independently authenticate the principal."	36

M.	Claim 12: "The method of claim 11, wherein taking further includes interactively authenticating the principal via a challenge and response dialogue in response to the identity service request and supplying an authentication token to the principal that indicates the principal is authenticated for access to the targeted services, if authentication is successful."	37
N.	Claim 13	38
1.	13[pre]: "The method of claim 8 further comprising:"	38
2.	13[a]: "receiving, by the machine, an authentication service token from the identity service or an external service associated with the principal, the authentication service token indicates the principal has been authenticated for access to the targeted services, and the targeted services are external to the identity service; and"	38
3.	13[b]: "using, by the machine, the authentication service token to proxy the targeted services to the identity service or the external service associated with the principal transparent to the principal, access sessions between the principal and the target services are proxied via the identity service or the external service."	39
VII.	GROUND 3 – CLAIMS 1-13 ARE RENDERED OBVIOUS BY HINTON OVER BURCH	39
A.	Overview of Burch.....	39
B.	Motivation to Combine Hinton and Burch.....	41
C.	Claim 1	43
1.	1[i]: "and a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response."	43

D.	Claim 5: "The method of claim 4, wherein supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service."	44
E.	Claim 12: "The method of claim 11, wherein taking further includes interactively authenticating the principal via a challenge and response dialogue in response to the identity service request and supplying an authentication token to the principal that indicates the principal is authenticated for access to the targeted services, if authentication is successful."	45
F.	Claims 2-4, 6-11, 13.....	46
VIII.	MANDATORY Notices Under 37 C.F.R. §42.8(a)(1)	46
A.	37 C.F.R. §42.8(b)(1): Real Parties-In-Interest.....	46
B.	37 C.F.R. §42.8(b)(2): Related Matters	46
C.	37 C.F.R. §42.8(b)(3)-(4): Lead And Back-Up Counsel And Service Information.....	46
IX.	FEES UNDER 37 C.F.R. §42.103	47
X.	CONCLUSION	47

TABLE OF AUTHORITIES

Cases

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 11

Statutes

35 U.S.C. §§102(a) 12
35 U.S.C. §§102 (e) 12
35 U.S.C. §311..... 1

Rules

37 C.F.R. § 42.100(b) 11
37 C.F.R. §42.103..... 47
37 C.F.R. §42.104(a) 1
37 C.F.R. §42.104(b)(1) 11
37 C.F.R. §42.21 1
37 C.F.R. §42.8(a)(1)..... 46
37 C.F.R. §42.8(b)(1) 46
37 C.F.R. §42.8(b)(2) 46
37 C.F.R. §42.8(b)(3) 46
37 C.F.R. §42.8(b)(4) 46

TABLE OF ABBREVIATIONS

Abbreviation	Full Name
'426 Patent	U.S. Patent No. 8,327,426
Challenged Claims	Claims 1-13 of the '426 Patent
Patent Owner	Patent Owner Netskope, Inc.
Petitioner	Petitioner Fortinet, Inc.
POSITA	Person of Ordinary Skill In The Art

EXHIBIT LIST

Exhibit No.	Document
1001	U.S. Patent No. 8,327,426 ("the '426 patent")
1002	File History of the '426 patent
1003	Declaration of Dr. Kevin Almeroth.
1004	U.S. Patent Pub. No. 2006/0021019 to Hinton et al. ("Hinton")
1005	U.S. Patent Pub. No. 2007/0234408 to Burch et al. ("Burch")

I. INTRODUCTION

Petitioner Fortinet, Inc. ("Petitioner") respectfully petitions, under 35 U.S.C. §311 and 37 C.F.R. §42.21, for *inter partes* review ("IPR") of claims 1-13 ("the Challenged Claims") of U.S. Patent No. 8,327,426 ("the '426 patent") (EX1001) on the grounds below.¹

The '426 patent relates to using a proxy to help the user sign on to one identity service and to also be authenticated with another identity service. The patent, however, does not purport to invent identity services. Nor could it. The patent itself acknowledges identity services in the prior art. Nor does the patent purport to invent the idea of single-sign on (SSO), which predates the patent by decades. The '426 patent therefore describes specific methods for authenticating a user with multiple identity services that have a trusted relationship. Even those specific methods, however, are clearly disclosed in the prior art described herein, none of which were before the examiner during prosecution, rendering the Challenged Claims invalid.

Accordingly, Petitioner respectfully requests that the Board cancel the Challenged Claims.

II. GROUNDS FOR STANDING (37 C.F.R. §42.104(a))

Petitioner certifies that the '426 patent is available for IPR and that Petitioner

¹ Unless otherwise noted, all emphases and annotations have been added.

is not barred or estopped from requesting IPR of the Challenged Claims on the grounds in this petition. The '426 patent issued more than 9 months ago, and Petitioner was served with the complaint alleging infringement of the '426 patent less than one year ago.

III. THE PATENT AND STATE OF THE ART

The '426 patent was filed on June 1, 2006, and does not claim priority to any earlier applications. EX1001. For the purposes of this petition, Petitioner therefore assumes a priority date of June 1, 2006. Because it was filed before March 2013, the '426 patent is subject to pre-AIA patent laws and cites herein to Title 35 of the U.S.C. will be to that version unless otherwise specified.

A. User Accounts

As the patent itself recognizes, users typically have multiple accounts for different services on the internet. As of the priority date of the patent, the typical way for users to log in to their internet accounts would be to type in a username and password. EX1003, ¶48. It was already well known that unique passwords should be used for each account, which created a problem for users that needed to remember multiple different passwords. *Id.*

B. Single Sign-On (SSO)

Single Sign-on (SSO) technology began to emerge in the 1980s. The idea was to help companies and government agencies consolidate their employees' login credentials into a single infrastructure using an identity and access management

system (IAM). EX1003, ¶49. For example, the Lightweight Directory Access Protocol (LDAP), which was available by at least 1997. *Id.* LDAP was an industry-standard application protocol for accessing and maintaining distributed login information. And companies like Microsoft introduced commercial tools like Active Directory and its predecessor (NT Directory Services) in the 1990s. *Id.*

C. Federated Architectures

Federated architectures that decentralize systems and organizations were also well-known years before the '426 patent. For example, the Security Assertion Markup Language (SAML) was ratified in 2002 as a secure method for sharing identity information between distributed networks or systems. *See id.*, ¶50.

D. The '426 Patent

According to the '426 patent, with businesses and users increasingly conducting business and other transactions over the internet, people have an ever-growing number of online accounts to manage, each of which may require a different username and password. EX1001, 1:11-53. The '426 patent uses the example of a user who wants to purchase something through a vendor using their bank account, but the "user may maintain separate accounts with the vendor and with the bank and neither the vendor or the bank are designed to interact with one another." *Id.*, 1:29-32. The patent contends that the user may be forced to abort the process or sign up for a separate service compatible with both the vendor and

the bank. *Id.*, 1:33-37. The patent insists that "there is a need for techniques that permit a user to achieve single sign on for any given network transaction, where that transaction includes the proxing [sic] of services." *Id.*, 1:53-55.

To solve that alleged problem, the patent describes the use of an "identity service," which it defines as "a special type of service that is designed to manage and supply authentication services and authentication information for principals and for other services." *Id.*, 2:33-36. There may be more than one of these "identity services" that help manage the authentication of the user. According to the patent, the identity service may "act as a proxy for a session" or it may "facilitate a session directly." *Id.*, 5:67-6:3.

Figure 5 depicts one example of this:²

² Colors are added here for convenience.

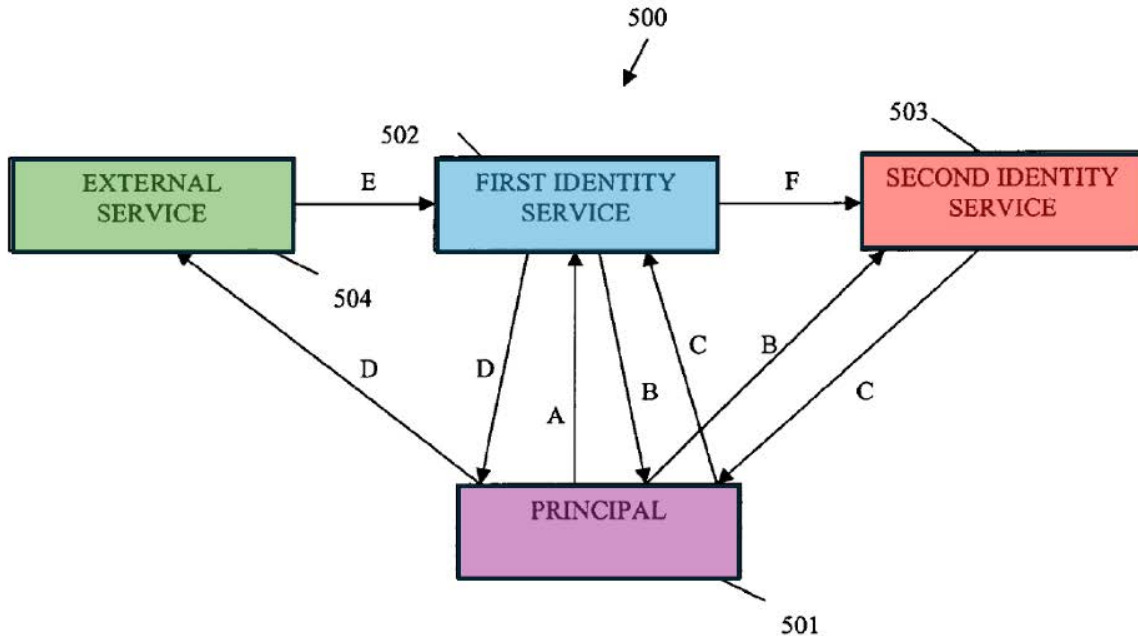


FIG. 5

The patent explains that the principal 501 (e.g., a user) wants to interact with an external service 504, such as by submitting a request through a browser. The patent explains that, instead of communicating directly with the external service, the user may be redirected to authenticate via the first identity service 502. EX1001, 10:17-24. The principal will then make an authentication request to the first identity service via message A. *Id.*, 10:17-18. The first identity service will then authenticate the principal via an appropriate authentication method, e.g., challenge/response dialogue. *Id.*, 10:28-32. The first identity service will then automatically redirect the browser of the principal to the second identity service 503 via message B. *Id.*, 10:25-32.

The redirection message B to the second identity service will indicate to the

second identity service that the **principal** is already authenticated by the **first identity service** because the **first identity service** will formulate message **B** to include both an authentication request and response. *Id.*, 10:33-40. Upon receipt of the authentication request and response, the **second identity service** will consider the **principal** to also be authenticated with that **second identity service**. *Id.*, 10:40-42. The **second identity service** will send an authentication token to the **principal** via message **C**, which will also be passed to the **first identity service**. *Id.*, 10:45-49.

The **first identity service** will then pass along its authentication statement or token with the token from the **second identity service** in message **D**, which the **principal** can redirect to the **external service**. *Id.*, 10:58-61. The **external service** will therefore know that the **principal** is authenticated with both the **first** and **second** identity services. *Id.*, 10:62-64.

After the **principal** is authenticated with the **external service**, the **principal** may want to access a targeted service that is provided by the **second identity service**. A "targeted service" is a service that is "accessible to and perhaps controlled by an identity service." *Id.*, 2:41-43. In such a situation, the **external service** will send a request to the **first identity service** via message **E**. *Id.*, 10:64-11:2. The **first identity service** will add the proper authentication tokens for the **principal** and send them to the **second identity service** via message **F**. *Id.*, 11:2-4.

In response, the **second identity service** will provide a service token to allow the **principal** to gain proxied access to the targeted service. *Id.*, 11:4-8. According to the patent, that proxied access "can occur via the **first identity service** 502 or it can occur directly via the **external service** 504 interacting with the **second identity service** 503." *Id.*, 11:8-10. The Challenged Claims require that the identity service "acts as a proxy for access sessions to the other services on behalf of the principal." *Id.*, cl. 1.

E. Challenged Claims

The '426 patent has 17 claims, three of which are independent. For the purposes of this petition, however, Petitioner challenges only independent claims 1 and 8. The challenged independent claims are a bit different and are reproduced below.

Claim 1 is from the perspective of the machine with the **first identity service** from Figure 5.

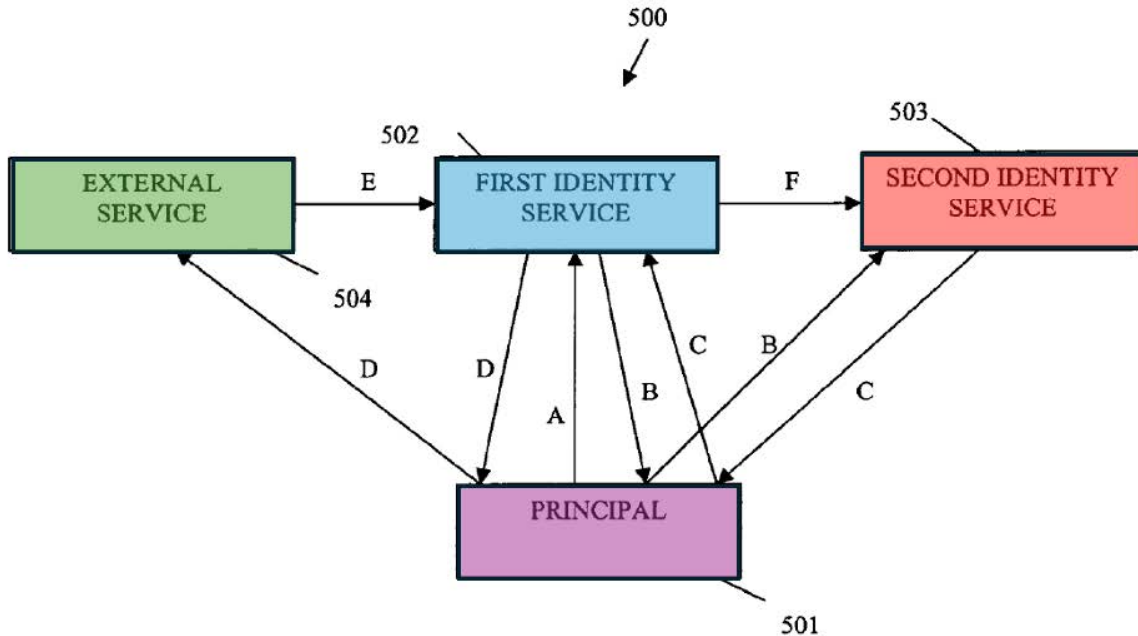


FIG. 5

[1PRE] A machine-implemented method to execute on a machine, comprising:

[1A] receiving, by the machine, an authentication request from a principal, the request directed by the principal to an external service and intercepted by the method for receipt;

[1B] authenticating, by the machine, the principal; and

[1C] supplying, by the machine, an authentication message for use by an identity service on behalf of the principal,

[1D] the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service,

[1E] the identity service acts as a proxy for access sessions to the other services on behalf of the principal,

[1F] the principal's access sessions occur indirectly through the identity service and transparently to the principal,

[1G] wherein the authentication message includes the

new authentication request made on behalf of the principal and the authentication message also includes a new authentication response that satisfies the new authentication request,

[1H] that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal,

[1I] the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to, and

[1J] a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response.

Claim 8 is from the perspective of the machine with the **second identity service** from Figure 5.

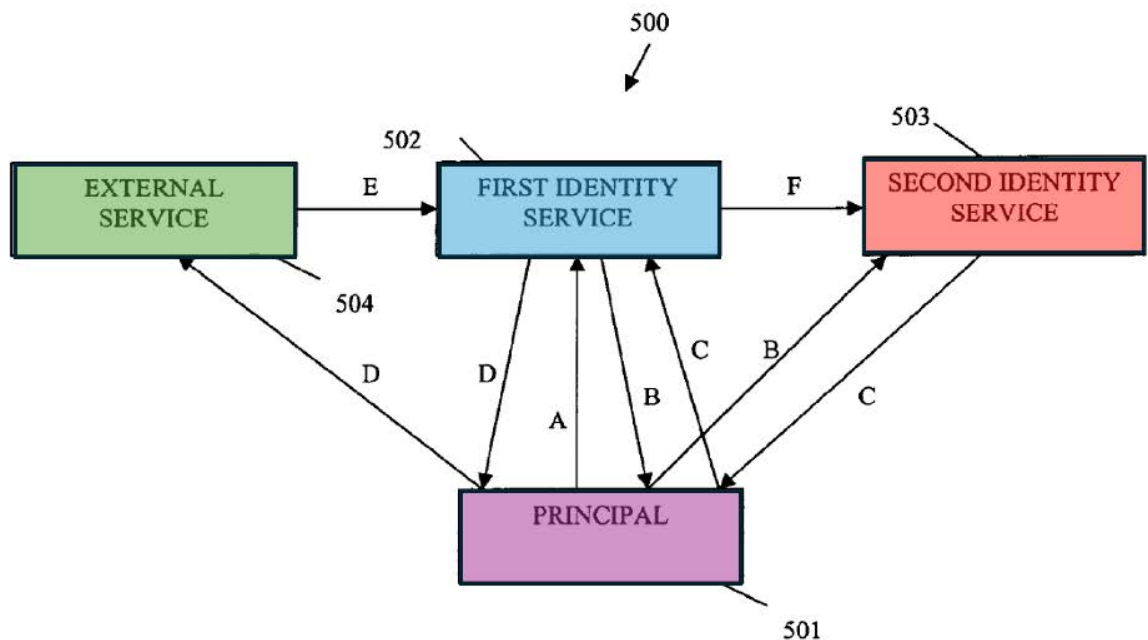


FIG. 5

[8PRE] A machine-implemented method to execute on a machine,

comprising:

- [8A] receiving, by the machine, an authentication request and an authentication response as a single sign-on transaction from a principal,
- [8B] the authentication request and the authentication response are received indirectly from the principal via an original identity service acting as a proxy on behalf of the principal and
- [8C] actions of that original identity service are transparent to the principal and the authentication response produced by that original identity service to authenticate the principal for the single sign-on transaction,
- [8D] the authentication request and the authentication response produced by the original identity service are different from that which was originally provided by the principal to the original identity service and
- [8E] the authentication request and the authentication response are made on behalf of the principal once the principal is authenticated by the original identity service;
- [8F] detecting, by a machine and from an identity service, an instruction, which is represented in the authentication response,
- [8G] the identity service is different from the original identity service, and
- [8H] the identity service and the original identity service are in a secure relationship with one another; and
- [8I] taking, by the machine, an action in response to the instruction to authenticate the principal for access to targeted services,
- [8J] access to the target services occur via proxied sessions through the identity service and transparent to the principal,
- [8K] wherein the action taken is dynamic and a real-time evaluation of policies processed by the identity service.

F. POSITA

The relevant art for the '426 patent is the field of computer science generally, and specifically, computer security. A POSITA, as of June 2006, would have been an individual with either (1) at least a bachelor's degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer security, or (2) at least three years of experience working in the field of computer security, even without a formal degree. EX1003, ¶¶62-63.

IV. CLAIM CONSTRUCTION

A claim is construed "using the same claim construction standard that would be used to construe the claim in a civil action," 37 C.F.R. § 42.100(b), which is governed by *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). Under the standard set out in *Phillips*, this petition applies the plain and ordinary meaning to each term in the '426 Patent, which is "the meaning that the term would have to a [POSITA] in question at the time of the invention." *Id.* at 1313.

Petitioner respectfully submits that there are no specific constructions required to resolve the issues raised in this Petition.

V. SUMMARY OF CHALLENGE AND RELIEF REQUESTED

A. 37 C.F.R. §42.104(b)(1): The Challenged Claims

Petitioner requests IPR and cancellation of the Challenged Claims (*i.e.*, claims 1-13) in view of the references discussed below.

B. 37 C.F.R. §42.104(b)(1): Prior Art Overview and Specific

Grounds of Rejection

1. Hinton

Hinton is a U.S. patent application that was filed on July 21, 2004, and published on January 26, 2006. EX1004. It is prior art to the '426 patent under at least 35 U.S.C. §§102(a), (e).

2. Overview of Burch

Burch is a U.S. patent application that was filed on March 31, 2006, and published on October 4, 2007. EX1005. It is prior art to the '426 patent under at least 35 U.S.C. §102(e).

3. Grounds of Rejection

Petitioner asserts the following specific grounds:

Ground	Claims	Basis	Prior Art
1	1-4, 6-11, 13	§102	Hinton
2	1-13	§103	Hinton
3	1-13	§103	Hinton over Burch

VI. GROUNDS 1 AND 2 – CLAIMS 1-4, 6-11, 13 ARE ANTICIPATED BY HINTON AND CLAIMS 1-13 ARE RENDERED OBVIOUS BY HINTON ALONE

A. Overview of Hinton

Hinton discloses a system of federated (distributed) provisioning in which a user can be authenticated to multiple domains after authenticating to a single point-of-contact server ("POC"). Figure 4 depicts the architecture of one such method of authentication:

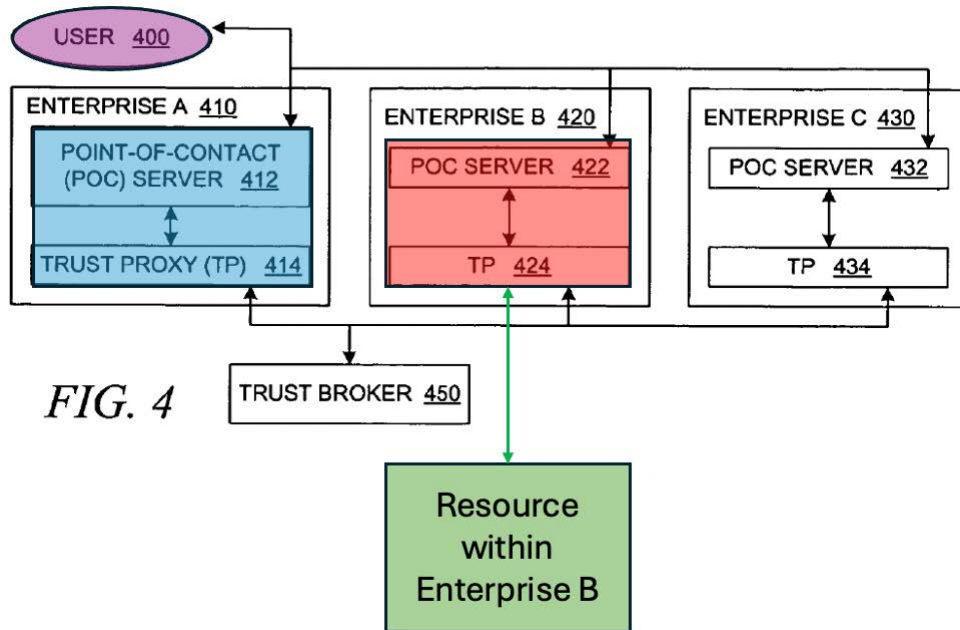


FIG. 4

The user 400 may first authenticate with Enterprise A 410 (domain 410) via the POC 412. EX1004, ¶155. The POC may use a trust proxy ("TP") 414 to help with the authentication process, but the POC and TP may be implemented on the same device. *Id.*, ¶106 ("It should be noted that although FIG. 2C depicts [POC] 252, trust proxy 254, security token service component 255, and authentication service runtime 256 as distinct entities, it is not necessary for these components to be implemented on separate devices."). Once the user is authenticated with Enterprise A, further logins may "trigger[] a federated single-sign-on operation." *Id.*, ¶156.

For example, if the user wants to access some resource within Enterprise B 420 (domain 420), Enterprise A will be the "issuing party" and Enterprise B will be the "relying party." *Id.*, ¶156. The POC/TP of Enterprise A will "generate[] a

federation single-sign-on token for the user that is formatted to be understood or trusted by" Enterprise B. *Id.* The POC 422 and TP 424 of Enterprise B will validate that token and establish a session for the user within the Enterprise B domain, thereby allowing access to the requested resource within Enterprise B. *Id.*, ¶157. After authentication via the POC/TP of Enterprise B, the user may continue to access the resource through Enterprise B's POC, so it is able to "establish a federated session that is known to the domain's [POC]." *Id.*, ¶94.

B. Claim 1

- 1. 1[pre]: "A machine-implemented method to execute on a machine, comprising:"**

Hinton discloses a machine-implemented method that executes each of the claimed steps. For example, Hinton discloses that the POC 412 and TP 414 are implemented on a server, and need not be on separate devices. EX1004, ¶106. The POC/TP of Enterprise A is the machine on which the method of claim 1 is executed (just like the first identity service from Fig. 5 in the '426 patent). *Id.*; EX1003, ¶69.

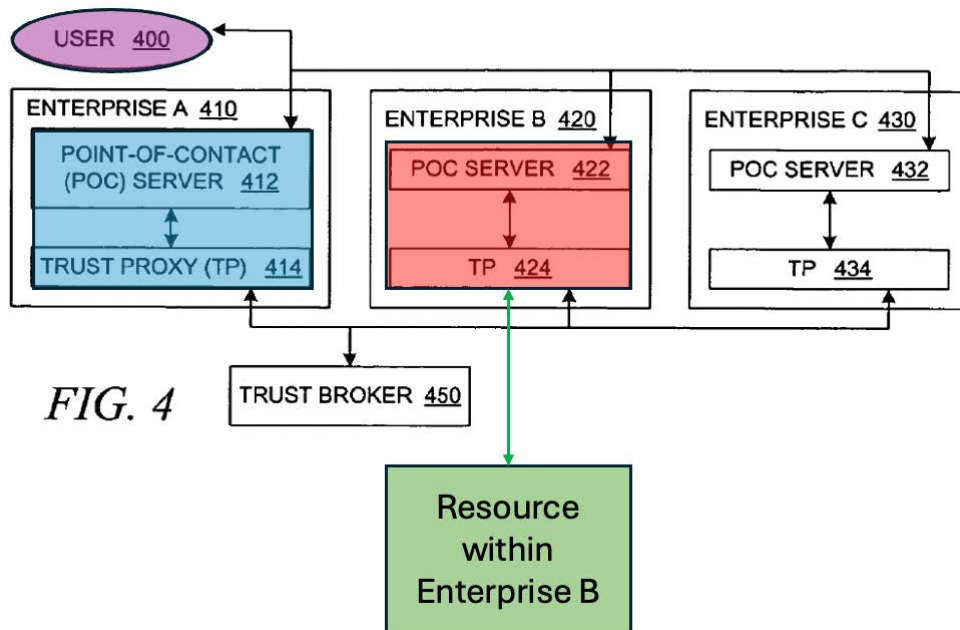


FIG. 4

2. 1[a]: "receiving, by the machine, an authentication request from a principal, the request directed by the principal to an external service and intercepted by the method for receipt;"

Hinton discloses that the Enterprise A POC/TP (*i.e.*, the machine on which the method is performed) receives an authentication request from the user (*i.e.*, the principal) to access some resource hosted in the Enterprise B domain. For example, "the user may invoke a federated single-sign-on operation to a resource in domain 420 via [POC] 412, *e.g.*, by selecting a special link on a web page that is hosted within domain 410 or by requesting a portal page that is hosted within domain 410 but that displays resources hosted in domain 420." EX1004, ¶156.

Hinton further explains this process in the flowchart of Figure 3D.

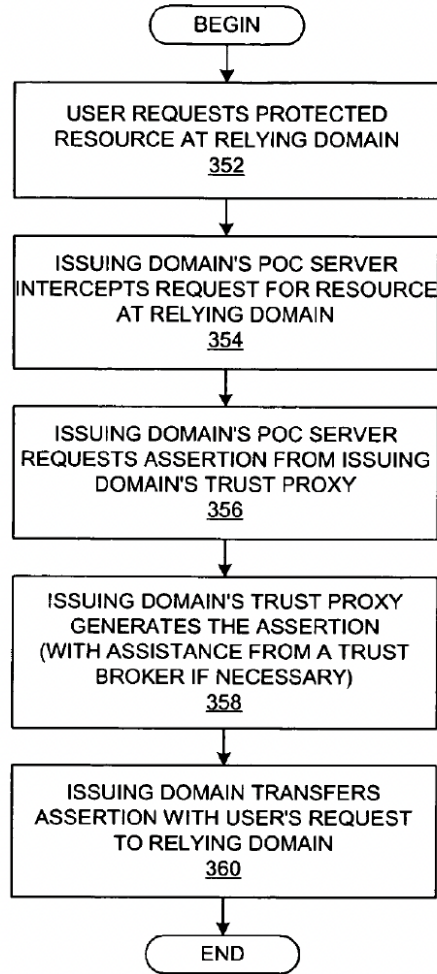


FIG. 3D

As described in the Figure, Enterprise A is the "issuing domain" and Enterprise B is the "relying domain." As shown above, when the user (*i.e.*, principal) requests a protected resource in the relying domain (Enterprise B), the issuing domain's (Enterprise A's) POC "actively intercept[s]" the request (step 354). *Id.*, ¶139. Hinton, therefore, discloses receiving a request from the user by intercepting the request ("intercepted by the method for receipt"). *Id.*; EX1003, ¶¶70-72.

3. 1[b]: "authenticating, by the machine, the principal; and"

Hinton discloses that the POC/TP of Enterprise A (*i.e.*, the machine) authenticates the user (*i.e.*, the principal) to access the Enterprise A domain by "validat[ing] the user's presented authentication credentials." EX1004, ¶155.

Hinton further discloses that, after receiving the request to access a resource in Enterprise B, the POC/TP "generate[s] a federation single-sign-on token" for the user. *Id.*, ¶156. A POSITA would have understood that the system authenticates the user before generating a federation token for that user at least because the POC/TP of Enterprise A needs to know for which user to generate the token. EX1004, ¶156; EX1003, ¶¶73-75. Further, it would have been obvious to a POSITA to authenticate the user before generating the federation token. For example, a POSITA would have known that the system would need to check whether the user is still authorized to access its system and that permissions have not been revoked after the user first authenticated with the POC/TP of Enterprise A and before the request to access a resource in Enterprise B. EX1003, ¶¶73-75.

4. 1[c]: "supplying, by the machine, an authentication message for use by an identity service on behalf of the principal,"

Hinton discloses that the POC/TP of Enterprise A supplies the "federation single-sign-on token for the user that is formatted to be understood or trusted by" the Enterprise B domain **420** (*i.e.*, an authentication message). EX1004, ¶156. As such, that token is supplied by the POC/TP of Enterprise A on behalf of the user

(*i.e.*, principal). Further, a POSITA would have understood that this token would be sent as part of an authentication message for the POC/TP of Enterprise B (*i.e.*, machine that runs the identity service). EX1003, ¶¶76-77. A POSITA would have understood that servers, like the POCs, communicate by sending messages. *Id.* As such, supplying authentication information from the POC/TP of Enterprise A to the POC/TP of Enterprise B requires sending an authentication message from the POC/TP of Enterprise A to the POC/TP of Enterprise B. *Id.*

5. **1[d]: "the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service,"**

As in Claim 1[c], Hinton discloses that the POC/TP of Enterprise A supplies an authentication message to the POC/TP of Enterprise B (identity service) on behalf of a user (principal). Hinton explains that this includes sending the "federation single-sign-on token" with "the user's request" from the POC/TP of Enterprise A to the POC/TP of Enterprise B as part of an authentication message. EX1004, ¶156.

A POSITA would have understood that the user's request to the POC/TP of Enterprise A is a first request and the subsequent request from the POC/TP of Enterprise A sent to the POC/TP of Enterprise B would be a new, different message at least because the new request comes from the POC/TP of Enterprise A

(machine on which the method is executed) instead of the user (principal).

EX1003, ¶¶78-79.

A POSITA would have further understood that the token itself serves as the new authentication response. EX1003, ¶80.

Further, to the extent a POSITA wanted to better understand the format of the new authentication message, she would use her knowledge as to how authentication messages are formatted. In using that general knowledge of authentication messages, it would have been obvious to a POSITA that the token could serve as both a new authentication request and a new authentication response. It would have been obvious to a POSITA that the token would have to be formatted in a way to request access on behalf of the user (new authentication request) from the POC/TP of Enterprise B (*i.e.*, the identity service). A POSITA also would have understood that the token would also need to include the proper credentials to authenticate the user with Enterprise B (new authentication response). It would have been obvious to a POSITA that if the token was not formatted as such, the POC/TP of Enterprise B would need to request that information from the user, which would mean that it would not be a "single-sign-on token" as disclosed by Hinton. EX1003, ¶81. And, it would have been obvious to a POSITA that, because the authentication token was generated by the POC/TP

of Enterprise A, it would have a new, different authentication request and response.

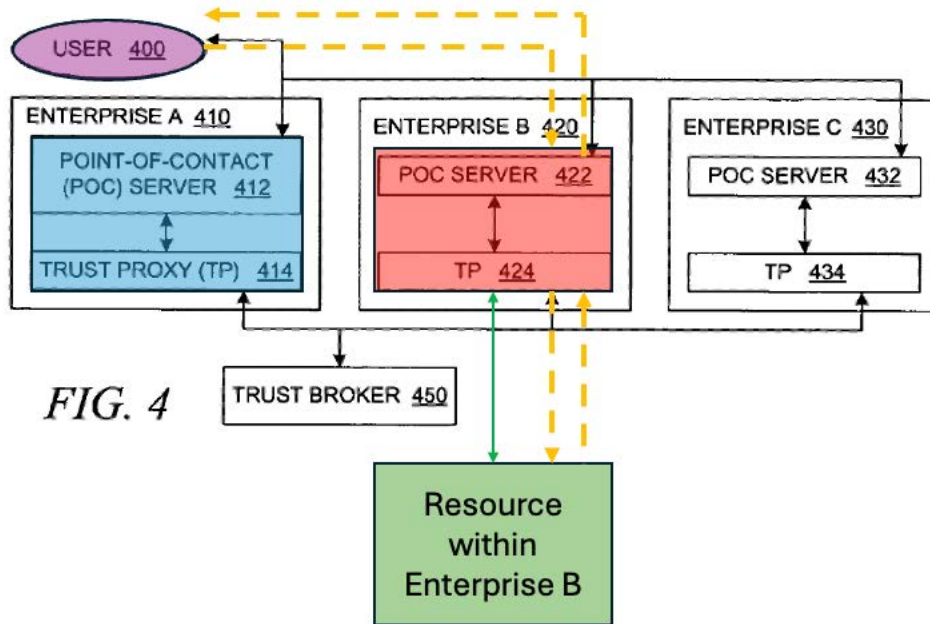
Id.

6. 1[e]: "the identity service acts as a proxy for access sessions to the other services on behalf of the principal,"

The POC/TP of Enterprise B (machine running the identity service) then acts as a proxy for access sessions by the principal. After authentication via the POC/TP of Enterprise B, Hinton discloses two scenarios: (1) the user accesses the requested service directly, and (2) the user accesses the requested resource through the POC/TP of Enterprise B, which acts as a proxy. For example, according to Hinton, "the domain may be configured so that users may continue to access particular application servers or other protected resources directly without going through a [POC] or other component implementing this [POC] functionality." EX1004, ¶94. Hinton explains that, in scenario 1, "a user that directly accesses the legacy system would not be able to establish a federated session that is known to the domain's [POC]." *Id.* A POSITA, therefore, would have understood, in scenario 2, when the user continues to access resources in Enterprise B via its POC/TP, that the POC/TP of Enterprise B will know the federated sessions of the user. EX1003, ¶82.

Further, it would have been obvious to a POSITA that the POC of Enterprise B could continue to serve as a proxy for access to the resources of Enterprise B. For example, in Figure 4 reproduced below, after the user is authenticated, the user

would continue to access the resource within Enterprise B through the POC of Enterprise B.



This means the POC of Enterprise B will act as a proxy for access sessions of the user to the resource. Because the POC is in the middle for these sessions, it will know and be able to control these sessions as needed, such as by limiting bandwidth to the resource or denying access if authentication is revoked during a session. See EX1004, ¶94; EX1003, ¶¶82-83.

7. **1[f]: "the principal's access sessions occur indirectly through the identity service and transparently to the principal,"**

As in Claim 1[e], Hinton discloses and/or renders obvious that the POC/TP of Enterprise B (identity service) acts as a proxy for access sessions to its resources. As such, Hinton teaches that the flow of communication (*i.e.*, access session) would be from the user (*i.e.*, principal) to the service through the POC/TP of Enterprise B, *i.e.*, indirectly. EX1003, ¶84.

A POSITA would have further understood that, in the context of Hinton, Enterprise B POC/TP would be transparent to users, and a user would not know that such access was indirect. *Id.*, ¶85.

8. **1[g]: "wherein the authentication message includes the new authentication request made on behalf of the principal and the authentication message also includes a new authentication response that satisfies the new authentication request, that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal,"**

As in Claims 1[c] and 1[d], Hinton discloses or it would have been obvious that the authentication message includes a new authentication request (on behalf of the user) and a new authentication response that satisfies the request (*i.e.*, single-sign-on token) and has already been addressed in Claims 1[d] and 1[c].

A POSITA would have further understood that, through the new authentication request and new authentication response already discussed, the new

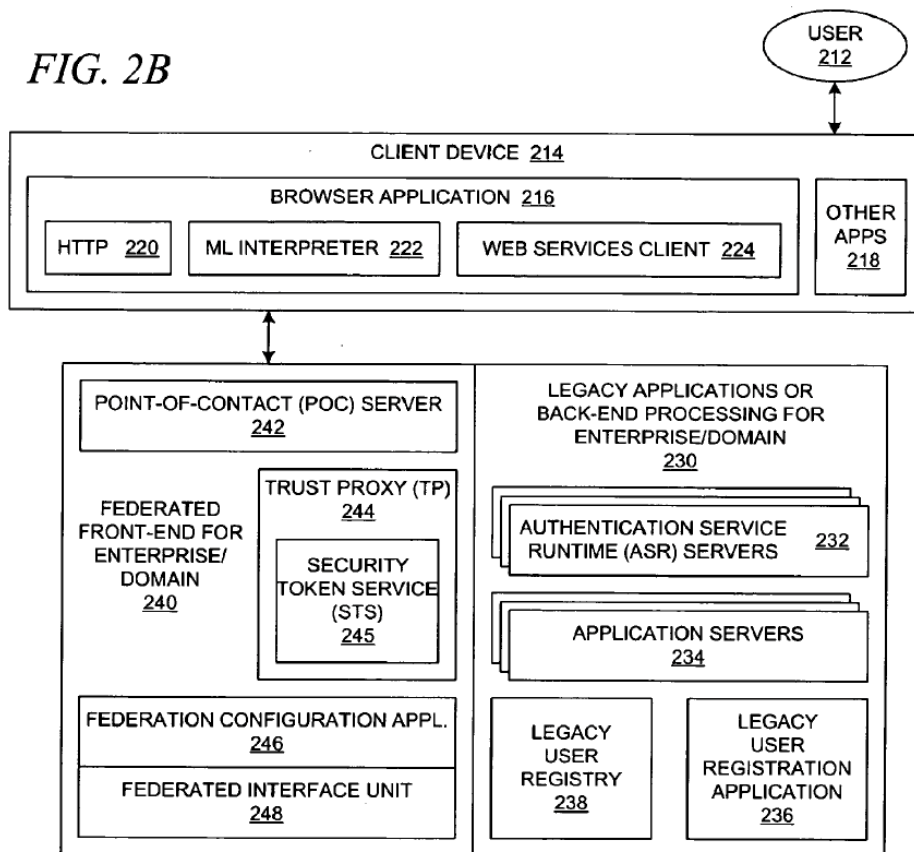
authentication response answers the new authentication request, thereby vouching for the user at the Enterprise B POC/TP for the single sign-on access of the user (principal). EX1003, ¶¶86-87.

9. 1[h]: "the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to,"

Although the scope of "the principal believing interactions are with the external service" is unclear, the '426 patent discloses: "The presence of the single sign-on service may be transparent or unknown to the principal. That is, the principal may believe that it is interacting or attempting to interact with an external service and the single sign-on service intercepts the communication and attempts to authenticate the principal in the manners described herein and below." EX1001, 4:9-16. As explained in 1[f], the user's access session occurs transparently through the POC/TP of Enterprise B. Therefore, the user in Hinton "may believe that it is interacting" that resource in Enterprise B (the external service). EX1003, ¶88.

Next, Hinton further discloses that the POC/TP of Enterprise B controls access to the applications and other resources of Enterprise B. For example, Figure 2B (reproduced below) shows that the POC/TP control access to "protected resources" of the enterprises (other services, including the external service), which may be hosted by application servers 234. EX1004, ¶93. Hinton explains that a "protected resource is a resource (an application, an object, a document, a page, a

file, executable code, or other computational resource, communication-type resource, etc.) for which *access is controlled or restricted.*" *Id.*, ¶61; see EX1003, ¶89.



Further, it would have been obvious to a POSITA that the POC/TP of Enterprise B controls access to the protected resources of Enterprise B. Indeed, that is the purpose of the POC/TP set forth in Hinton. EX1004, ¶155 (explaining that the POC/TP are used "for access *control* purposes"); EX1003, ¶¶89-90. And it would have been obvious to a POSITA that the POC may control access to

resources that are internal or external to the Enterprise B domain. EX1003, ¶¶89-90.

10. 1[i]: "and a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response."

Hinton teaches that the number of interactions for Enterprise B to authenticate the user "[d]epend[] on the type of token presented by domain 410." EX1004, ¶158. "For example, domain [410]³ may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420." *Id.* In this example, only one interaction is required because the user's credentials would be validated against the user registry at the Enterprise B domain. EX1003, ¶91.

Hinton further explains, however, "it is not always the case that the issuing domain will know how to map the user from a local identifier for domain 410 to a local identifier for domain 420." EX1004, ¶160. In these cases, Enterprise B POC/TP will need multiple interactions with other entities, such as with the trust broker 450. *Id.*; EX1003, ¶92.

³ A POSITA would have understood this to be a typo given that the security token is provided by domain 410. EX1003, ¶99.

Therefore, a POSITA would have understood that the need for single or multiple interactions for authentication is automatically communicated in the single-sign-on token. The POC/TP of Enterprise B determines whether one interaction or two interactions is required based upon the received single sign-on token, based upon whether it receives (a) a binary security token or (b) a user name that must be mapped to the local identifier for the domain as set forth above.

EX1003, ¶93.

As above, the number of interactions needed for Enterprise B to authenticate the user depends upon the type of token received by the Enterprise B POC/TP. If the single sign-on token is a binary security token and only requires one interaction, this information is communicated in the new authentication response. Alternatively, if the issuing domain is not able to map the user to a local identifier, that would also be communicated in the new authentication response. EX1003, ¶94.

Further, it would have been obvious that the POC/TP of Enterprise B determines which of the above two authentication methods to use based upon the type of token it received and what information the POC/TP of Enterprise B has access to. *Id.*, ¶95.

- C. Claim 2: "The method of claim 1 further comprising, making, by the machine, a target service available to interactions between the principal and an external service, the target service is directly accessible from an environment of the identity service."**

As in Claim 1[c] and 1[d], Hinton discloses (and it would have been obvious to a POSITA), that the POC/TP of Enterprise A (the machine) helps authenticate the user with the POC/TP of Enterprise B (machine running the identity service), which controls access to different services, including external services, any one of which could be the target service. Hinton thus discloses that the POC/TP of Enterprise A makes a target service available to the user, allowing the user to interact with an external service, where the target service is directly accessible from the domain of Enterprise B. EX1003, ¶96.

- D. Claim 3: "The method of claim 1, wherein supplying further includes redirecting the principal to the identity service and including with the redirection the new authentication request and the new authentication response represented by the authentication message, and the identity service authenticates the principal automatically in response to the new authentication response included with the authentication message."**

As in Claim 1[c] and 1[g], Hinton discloses that Enterprise A POC/TP supplies an authentication message in the form of a single-sign-on token with a new authentication request and new authentication response that automatically authenticates the user with Enterprise B POC/TP. Hinton further discloses that the token "may be sent using HTTP redirection via the user's browser." EX1004, ¶156. A POSITA would have understood that HTTP redirection involves

redirecting the user (principal) to Enterprise B POC/TP (identity service) and that the redirection would have included the new authentication request and new authentication response so the user could be authenticated. EX1003, ¶97.

- E. Claim 4: "The method of claim 3, wherein supplying further includes representing the new authentication response as a first authentication token that informs the identity service that the principal is currently already properly authenticated to the processing associated with the method."**

As in Claim 1[c] and 1[g], Hinton discloses that Enterprise A POC/TP supplies an authentication message including a new authentication request and a "single-sign-on token," which informs Enterprise B POC/TP that the user is already authenticated to access the requested resource. EX1003, ¶98.

- F. Claim 5: "The method of claim 4, wherein supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service."**

As in Claim 3, Hinton discloses first redirection via an HTTP request from the user. After that redirection, Hinton teaches that the number of interactions for Enterprise B to authenticate the user "[d]epend[]" on the type of token presented by domain **410**." EX1004, ¶158. "For example, domain **[410]**⁴ may provide a binary

⁴ A POSITA would have understood this to be a typo given that the security token is provided by domain **410**. EX1003, ¶99.

security token containing the user's name and password to be validated against the user registry at domain 420." *Id.*

It further would have been obvious to a POSITA that certain domains require second authentication challenge/response layer (*e.g.*, two-factor authorization), particularly those with sensitive information. EX1003, ¶¶99-100. Indeed, Hinton recognizes that additional steps may be required to authenticate the user with the Enterprise B domain. EX1004, ¶¶158-160. It would have been obvious that this second authentication challenge/response layer directs the user to a service proxied through Enterprise B POC/TP, which would then perform the second authentication. EX1003, ¶¶99-100.

G. Claim 6: "The method of claim 1, wherein supplying further includes representing the new authentication response as an instruction to the identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service."

As in Claim 1[g], Hinton discloses, and it would have been obvious to a POSITA that the single-sign-on token supplied from Enterprise A POC/TP to Enterprise B POC/TP informs Enterprise B POC/TP that the user is authenticated with Enterprise A.

Similar to Claims 1[i] and 5, Hinton discloses, and it would have been obvious to a POSITA that Enterprise B may have its own additional, independent authentication policies that would need to be enforced, such as its own user

registry. EX1004, ¶158. A POSITA would have therefore understood that the single-sign-on token acts as an instruction to Enterprise B POC/TP to enforce its own authentication policies. EX1003, ¶¶101-102.

H. Claim 7: "The method of claim 1 further comprising, interacting, by the machine, with the principal via a World-Wide Web (WWW) browser over the Internet using at least one of a Security Assertion Markup Language (SAML), a Liberty Alliance markup language, and Web Services (WS) Foundation markup language."

Hinton discloses that a SAML "assertion is an example of a possible assertion format that may be used within the present invention." EX1004, ¶64. A POSITA therefore would have understood that Hinton discloses interactions between the user's web browser and Enterprise A POC/TP occurring via SAML. EX1003, ¶103.

I. Claim 8

1. 8[pre]: "A machine-implemented method to execute on a machine, comprising:"

Whereas Claim 1 was from the perspective of the Enterprise A POC/TP, for Claim 8, the machine implementing and executing the claimed method is the Enterprise B POC/TP (which is the second identity service from the '426 patent). As Hinton describes, the method could at least be implemented and run on a single device. EX1004, ¶106; EX1003, ¶105.

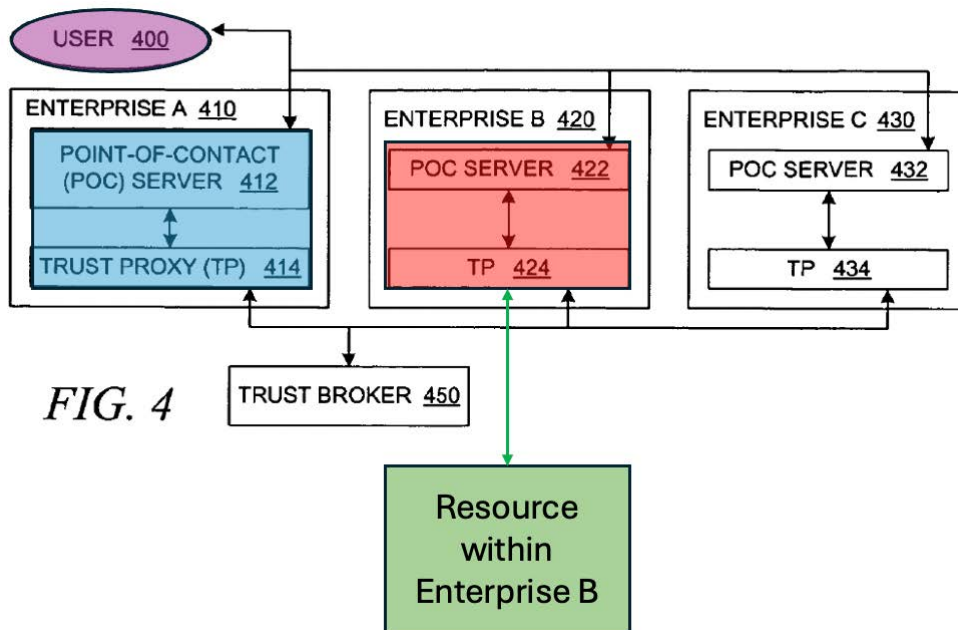


FIG. 4

2. **8[a]: "receiving, by the machine, an authentication request and an authentication response as a single sign-on transaction from a principal,"**

As in Claim 1[c], Hinton discloses that Enterprise B POC/TP receives a "federation single-sign-on token for the user." EX1004, ¶156. As in Claim 1[d], a POSITA would have understood or it would have been obvious that this token would include a new authentication request and authentication response as a single-sign-on transaction from a user. EX1003, ¶106.

3. **8[b]: "the authentication request and the authentication response are received indirectly from the principal via an original identity service acting as a proxy on behalf of the principal and"**

Hinton discloses that the single-sign-on token "may be sent [from Enterprise A POC/TP] by invoking the request directly of" Enterprise B POC/TP. EX1004, ¶156. A POSITA would have understood that this means the authentication

request and authentication response are received by the Enterprise B POC/TP (the machine) indirectly from the user via Enterprise A POC/TP (original identity service), which is acting as a proxy on behalf of the principal. EX1003, ¶107.

4. 8[c]: "actions of that original identity service are transparent to the principal and"

Hinton discloses that, when the user requests a protected resource in the relying domain (Enterprise B), the issuing domain's (Enterprise A's) POC (original identity service) "actively intercept[s]" the request. EX1004, ¶139. A POSITA would have understood that this interception means that the actions of Enterprise A POC/TP are transparent to the user. EX1003, ¶108.

5. 8[d]: "the authentication response produced by that original identity service to authenticate the principal for the single sign-on transaction,"

As in Claim 1[d], the Enterprise A POC/TP (original identity service) produces a single-sign-on token that authenticates the user with Enterprise B as part of a single-sign-on transaction. EX1003, ¶109.

6. 8[e]: "the authentication request and the authentication response produced by the original identity service are different from that which was originally provided by the principal to the original identity service and"

As in Claim 1[d], the "federation single-sign-on token" sent by Enterprise A POC/TP (original identity service) to Enterprise B POC/TP (the machine) includes a new authentication request and new authentication response. A POSITA would have understood that the user's request would necessarily have to be different from

the user's initial authentication request because the request would need to identify the user that was making the request, since it could come from Enterprise A POC instead of directly from the user. EX1003, ¶110. A POSITA would have understood that the "federation single-sign-on token" (authentication response) is generated by Enterprise A POC/TP and is therefore different than what was originally provided by the user to Enterprise A. *Id.*

7. **8[f]: "the authentication request and the authentication response are made on behalf of the principal once the principal is authenticated by the original identity service;"**

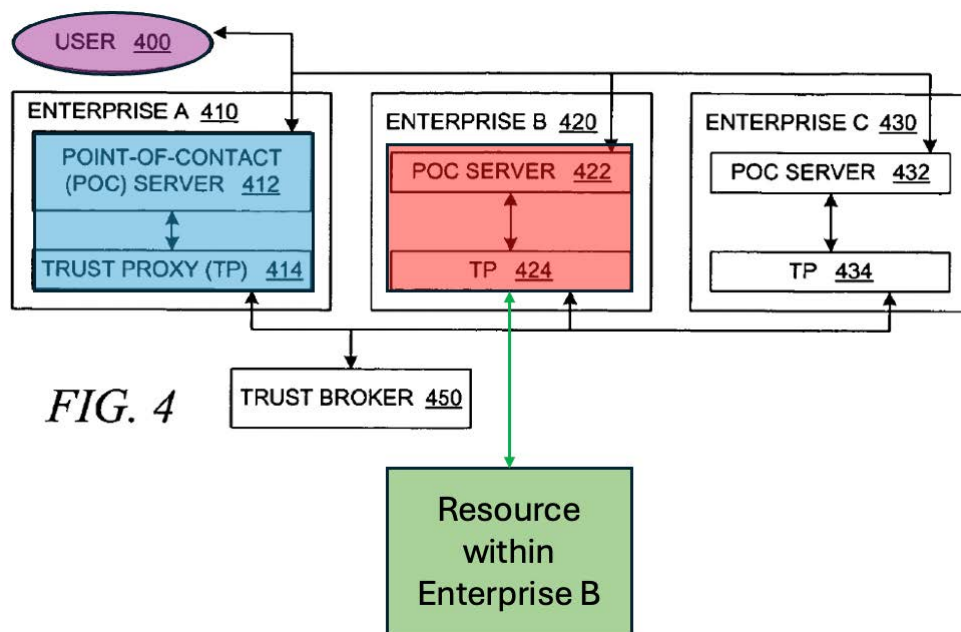
As in Claim 1[b], Hinton discloses and/or renders obvious that the user is first authenticated with Enterprise A POC/TP (original identity service) before the single-sign-on token is sent to the Enterprise B POC/TP (the machine). EX1003, ¶111.

8. **8[g]: "detecting, by a machine and from an identity service, an instruction, which is represented in the authentication response,"**

As in Claim 6, Hinton discloses, and it would have been obvious to a POSITA that Enterprise B POC/TP (identity service) detects receipt of the single-sign-on token, which acts as an instruction to Enterprise B POC/TP. EX1003, ¶112.

9. **8[h]: "the identity service is different from the original identity service, and the identity service and the original identity service are in a secure relationship with one another; and"**

Hinton discloses multiple identity services, including Enterprise A POC/TP (original identity service) and Enterprise B POC/TP (machine running the different identity service, claimed as "the identity service [] different from the original identity service"), which are different from each other, as shown below.



Hinton further discloses that Enterprise A POC/TP and Enterprise B POC/TP are in a secure relationship with one another that can be verified via the trust broker 450, which "is used to establish, on behalf of a federation participant, a trust relationship based on transitive trust with other federation partners." EX1004, ¶125; EX1003, ¶¶113-114.

- 10. 8[i]: "taking, by the machine, an action in response to the instruction to authenticate the principal for access to targeted services,"**

As in Claim 8[g], Hinton discloses that, upon detecting receipt of the single-sign-on token, Enterprise B POC/TP "validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user." EX1004, ¶157. A POSITA would have understood that these are actions in response to the instruction to authenticate the user for access to targeted services. EX1003, ¶115.

- 11. 8[j]: "access to the target services occur via proxied sessions through the identity service and transparent to the principal,"**

As in Claim 1[f], the access to the user's requested services occurs through Enterprise B POC/TP (identity service) transparently to the user. EX1003, ¶116.

- 12. 8[k]: "wherein the action taken is dynamic and a real-time evaluation of policies processed by the identity service."**

As in Claim 8[i], the actions taken are to validate the user to check if the token is valid and trusted, and the user is authorized, which happens dynamically and in real-time, at least because it would not be acceptable for the user to wait for a process that was not evaluated in real-time. EX1003, ¶117.

- J. Claim 9: "The method of claim 8, wherein detecting further includes identifying the instruction as an assertion from the identity service that the principal is currently already authenticated to the identity service."**

As in Claim 8[g], Hinton discloses, and it would have been obvious to a POSITA that the Enterprise B POC/TP detects the receipt of the single-sign-on

token, which acts as an instruction to Enterprise B POC/TP. EX1003, ¶118. And, a POSITA would have understood that the single-sign-on token is an assertion by Enterprise A POC/TP that the user is already authenticated with the Enterprise A POC/TP. *Id.*

- K. Claim 10: "The method of claim 9, wherein taking further includes authenticating the principal, in response to the assertion, and supplying an authentication token to the principal indicating that the principal is authenticated for access to the targeted services."**

As in Claim 8[j], Enterprise B POC/TP takes action in the form of "validat[ing] the token, and assuming that the token is valid and trusted, generat[ing] a locally valid token for the user." EX1004, ¶157. A POSITA would have understood that this locally valid token for the Enterprise B domain indicates that the user is authenticated to access requested services (targeted services) within that domain and would then need to be supplied to the principal. EX1003, ¶119. Further, it would have been obvious to supply that locally valid token to the user so the user could use that token. *Id.*

- L. Claim 11: "The method of claim 8, wherein detecting further includes identifying the instruction as an identity service request from the identity service to independently authenticate the principal."**

As in Claim 8[g], Hinton discloses, and it would have been obvious to a POSITA that the Enterprise B POC/TP detects the receipt of the single-sign-on token, which acts as an instruction to Enterprise B POC/TP. EX1003, ¶120.

Hinton explains that "domain [410]⁵ may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420." EX1004, ¶158. Domain 420 will thus independently authenticate the user using its own user registry. *See* Section VI.G, *supra*; EX1003, ¶120.

M. Claim 12: "The method of claim 11, wherein taking further includes interactively authenticating the principal via a challenge and response dialogue in response to the identity service request and supplying an authentication token to the principal that indicates the principal is authenticated for access to the targeted services, if authentication is successful."

Hinton teaches that the number of interactions for Enterprise B to authenticate the user "[d]epend[] on the type of token presented by domain 410." EX1004, ¶158. "For example, domain [410]⁶ may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420." *Id.*

It would have been further obvious to a POSITA that certain domains require an additional challenge/response layer (*e.g.*, two-factor authorization), particularly those with sensitive information. EX1003, ¶¶121-122. Indeed, Hinton recognizes that additional steps may be required to authenticate the user with the

⁵ A POSITA would have understood this to be a typo given that the security token is provided by domain 410. EX1003, ¶99.

⁶ A POSITA would have understood this to be a typo given that the security token is provided by domain 410. EX1003, ¶99.

Enterprise B domain. EX1004, ¶¶158-160. It would have been obvious that Enterprise B POC/TP can send the challenge response directly to the user and will only authenticate the user by sending the authentication token if that additional authentication is successful. EX1003, ¶¶121-122.

N. Claim 13

1. 13[pre]: "The method of claim 8 further comprising:"

See Claim 8.

2. 13[a]: "receiving, by the machine, an authentication service token from the identity service or an external service associated with the principal, the authentication service token indicates the principal has been authenticated for access to the targeted services, and the targeted services are external to the identity service; and"

As in Claim 8[g], Hinton discloses that Enterprise B POC/TP (*i.e.*, the machine in this claim limitation) "validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user." EX1004, ¶157.

A POSITA would have understood that the Enterprise B POC/TP thus receives the locally valid token from the Enterprise A POC/TP (identity service), which indicates the user is authenticated to access the services accessible via Enterprise B POC/TP. EX1003, ¶124.

As in Claim 1[h], Enterprise B POC/TP may authenticate users to access targeted services external to the Enterprise B domain. EX1003, ¶125.

3. **13[b]: "using, by the machine, the authentication service token to proxy the targeted services to the identity service or the external service associated with the principal transparent to the principal, access sessions between the principal and the target services are proxied via the identity service or the external service."**

As in Claim 8[j], the access to the user's requested services is proxied through Enterprise B POC/TP (identity service) transparently to the user. A POSITA would have understood that this proxied access utilizes the locally valid token discussed in Claim 13[a]. EX1003, ¶126. It further would have been obvious to a POSITA that the proxied access utilizes the locally valid token discussed in Claim 13[a] because the proxied access must be authenticated, and it would have been obvious that the token is needed for that authentication. *Id.*

VII. GROUND 3 – CLAIMS 1-13 ARE RENDERED OBVIOUS BY HINTON OVER BURCH

As in Grounds 1-2, Hinton alone discloses and/or renders obvious Claims 1-13. These claims are further rendered obvious by Hinton over Burch.

A. Overview of Burch

Burch discloses a multi-factor authentication system that can be used for legacy services. EX1005, Abstract. Burch recognizes the importance of "enhanced and improved security techniques" for certain applications with sensitive information like "on-line banking." *Id.*, ¶4. Burch proposes a way to add enhanced security to legacy systems. Figure 4 depicts one proposed solution.

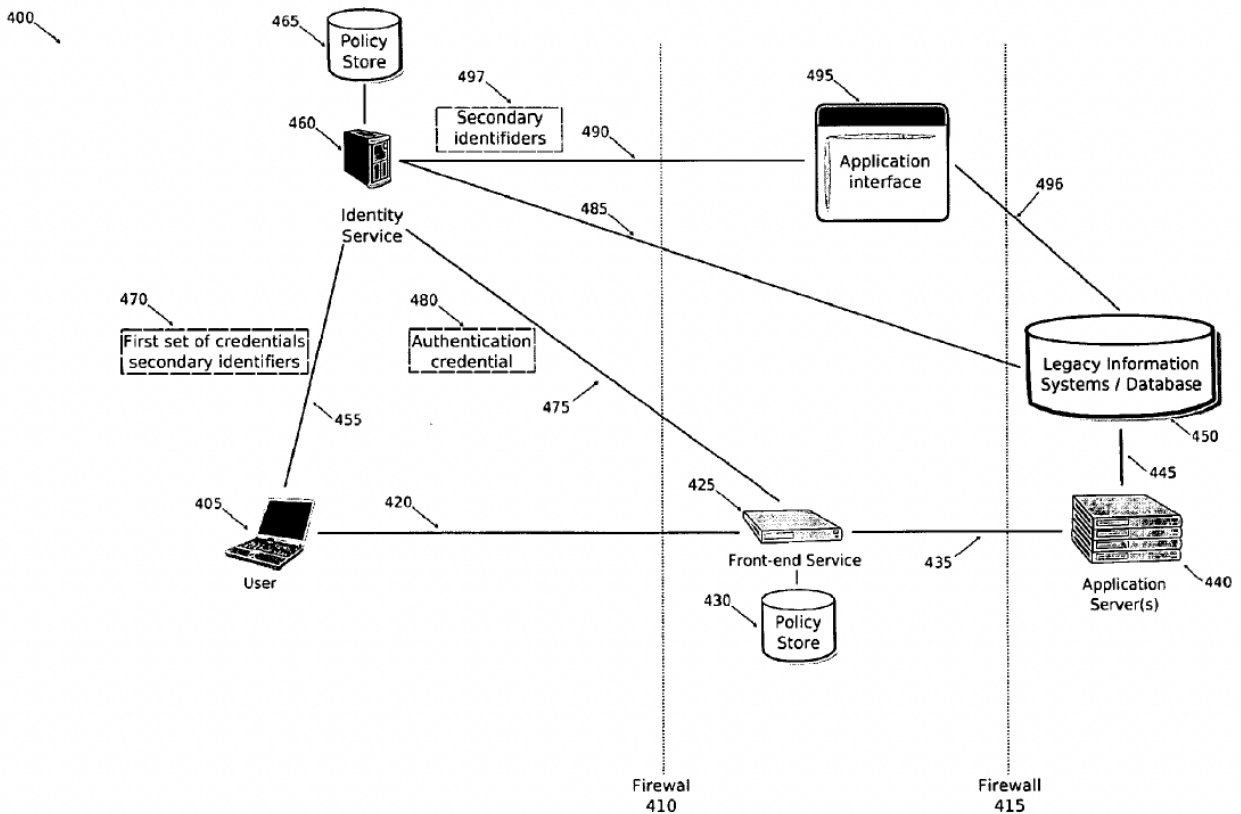


Figure 4

According to Burch, when a user **405** tries to access an application hosted on server **440**, the user may be first redirected to an identity service **460** for authentication. *Id.*, ¶¶91-93. Burch explains that the user will be authenticated based upon the policy set forth at the authentication service **460**. "In particular, the policy information **465** may specify a first set of credentials **470** and one or more secondary identifiers **497** that are to be produced by user **405** in order to authenticate its identity. In addition to specifying the one or more secondary identifiers **497**, the policy information **465** may also indicate how these identifiers

497 may be obtained." *Id.*, ¶94. In other words, the user may need to produce multiple identifiers to be authenticated (multifactor authentication).

B. Motivation to Combine Hinton and Burch

Hinton discloses a federated single-sign-on system in which a user may authenticate with one domain, and the system will leverage that authentication to also authenticate with another trusted domain. EX1004, ¶¶155-157.

From this disclosure, a POSITA would have recognized that different domains would sometimes have different authentication policies. This understanding would be supported by a POSITA's knowledge and confirmed by other art in the field. For example, Burch explains that "enhanced and improved security techniques" are needed for certain applications with sensitive information like "on-line banking." EX1005, ¶4. Hinton itself recognizes that the way in which Enterprise B authenticates the user "[d]epend[s] on the type of token presented by domain 410." EX1004, ¶158. "For example, domain [410] may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420." *Id.*

Given this understanding, a POSITA would have first recognized the need for enhanced security in at least some scenarios. A POSITA would have then understood that other forms of authentication could also be supported in Hinton's system. Burch provides an example of another form of authentication that could

be supported in Hinton. A POSITA would have been motivated to use the multifactor authentication disclosed in Burch to supplement the authentication process in Hinton. EX1003, ¶131.

In doing so, it would have been obvious to a POSITA that, by using multifactor authentication in the Hinton federated system, Enterprise B POC/TP could receive the username and password in the security token from Enterprise A, but would still need a secondary identifier from the user, as disclosed in Burch. EX1005, ¶94; EX1003, ¶132.

A POSITA would have recognized the benefits of supplementing the authentication process in Hinton with the multi-factor authentication from Burch because, as Burch discloses, it would provide enhanced security for certain applications. EX1005, ¶4. And, the benefits of single sign-on as disclosed in Hinton would still be present because the user would not have to re-type her username and password, and instead would only need to provide the secondary identifier specific to Enterprise B. EX1004, ¶11; EX1003, ¶133.

It further would have been obvious to a POSITA to combine Hinton and Burch because they are in the same general field of user authentication. EX1004 ¶74; EX1005, ¶11; EX1003, ¶134.

A POSITA would have had a reasonable expectation of success at least because Burch discloses adding multifactor authentication to legacy (existing)

systems and it would have been obvious to a POSITA that this means it could have been added to the federated system in Hinton using well-known programming capabilities of a POSITA. EX1005, ¶5; EX1003, ¶135. Furthermore, Hinton itself recognizes that the POC/TP of Enterprise B may have its own authentication database and protocols. EX1004, ¶¶158-160. A POSITA, therefore, would have had a reasonable expectation of success in adding the multifactor authentication system in Burch to the POC/TP of Enterprise B. EX1003, ¶135.

C. Claim 1

The analysis for the Claim 1 limitations other than 1[i] is the same as Grounds 1-2 and is incorporated by reference herein. EX1003, ¶136.

1. **1[i]: "and a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response."**

The same analysis from Grounds 1-2 also applies here, but to the extent Patent Owner argues that this limitation requires determining whether or not to use multifactor authentication by the identity service (Enterprise B POC/TP in Hinton), this limitation is rendered obvious by Hinton over Burch. As described above, Burch discloses using multifactor authentication based upon the required policy of a particular domain. EX1005, ¶94. And a POSITA would have been motivated to use this multifactor authentication technique for Enterprise B POC/TP for the reasons explained above.

As such, the new authentication response to Enterprise B POC/TP will automatically communicate whether to use a single interaction or multiple interactions because, if the message contains only one authentication response and Enterprise B POC/TP requires multi-factor authentication, Enterprise B POC/TP will determine that it needs multiple interactions with the principal. EX1003, ¶¶137-138. This determination by the POC/TP of Enterprise B is made based upon the information sent in the new authentication response. *Id.*

D. Claim 5: "The method of claim 4, wherein supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service."

As in Claim 3 from Grounds 1-2, Hinton discloses a first redirection via the user's browser. EX1004, ¶156 (disclosing that the token "may be sent using HTTP redirection via the user's browser" to Enterprise B the POC/TP). The combination of Hinton over Burch renders obvious a second authentication via a second redirection. Burch discloses that adding multifactor authentication may involve redirecting the authentication request to a separate identity service **460**. EX1005, ¶92. A POSITA would have been motivated to add this second redirection for multifactor authentication for the reasons described in the motivation to combine Hinton and Burch. Furthermore, Burch explains that this redirection process

allows multifactor authentication to be used for legacy systems, meaning the Enterprise B POC/TP would not need to be changed to accommodate multifactor authentication. EX1003, ¶139.

It would have been obvious to a POSITA that this second redirection to a separate identity service, as described in Burch, would be directing the user to request a target service (the service the user wants to access) and that the multifactor authentication from Burch is required to access that service, making the redirection a request to access the service. EX1003, ¶140. And, as in Claim 1[e], Enterprise B POC/TP acts as a proxy on behalf of the user for the target service.

Id.

- E. Claim 12: "The method of claim 11, wherein taking further includes interactively authenticating the principal via a challenge and response dialogue in response to the identity service request and supplying an authentication token to the principal that indicates the principal is authenticated for access to the targeted services, if authentication is successful."**

Burch discloses multifactor authentication which would be added to the Enterprise B POC/TP when combined with Hinton. It would have been obvious to a POSITA that this requires an additional challenge and response dialogue to authenticate the user because that is the method by which authentication is performed. EX1005, ¶94; EX1003, ¶141. Indeed, Hinton discloses that "typical user authentication" involves an "authentication challenge" and "authentication response." EX1004, Fig. 1C; *id.*, ¶¶46-47.

As in Claim 10 from Grounds 1-2, Hinton discloses or it would have been obvious that an authentication token is supplied to the user. EX1003, ¶142. It would have been obvious to a POSITA that the authentication token would only be supplied to the user if the additional challenge/response dialogue is successful because that is the entire purpose of that challenge/response dialogue. *Id.*

F. Claims 2-4, 6-11, 13

Claims 2-4, 6-11, and 13 are rendered obvious by Hinton over Burch for the reasons set forth in Grounds 1 and 2. EX1003, ¶143.

VIII. MANDATORY NOTICES UNDER 37 C.F.R. §42.8(a)(1)

A. 37 C.F.R. §42.8(b)(1): Real Parties-In-Interest

Petitioner is the real party-in-interest.

B. 37 C.F.R. §42.8(b)(2): Related Matters

The '426 patent is asserted against Petitioner in *Netskope, Inc. v. Fortinet, Inc.*, No. 4:25-cv-02360-HSG (N.D. Cal. filed Mar. 7, 2025).

C. 37 C.F.R. §42.8(b)(3)-(4): Lead And Back-Up Counsel And Service Information

Designated Counsel for Petitioner and service information is below:

Lead Counsel	Back-Up Counsel
Andrew D. Gish (Reg. # 67,562) GISH PLLC 41 Madison Avenue New York, New York 10010 Telephone: (212) 518-7380 andrew@gishpllc.com	Ryan Iwahashi (Reg. # 63,378) GISH PLLC 50 California Street, Suite 1500 San Francisco, CA 94111 Telephone: (415) 630-8960 ryan@gishpllc.com

Petitioner consents to service by email at the addresses above.

IX. FEES UNDER 37 C.F.R. §42.103

Petition and Post-Institution fees totaling \$51,875 have been paid by electronic funds transfer.

X. CONCLUSION

Petitioner requests the Board institute IPR of the Challenged Claims and cancel them.

Respectfully Submitted,

Dated: October 7, 2025

/s/Andrew Gish

Andrew Gish (Reg. #67,562)

ATTORNEY FOR PETITIONER

CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. §42.24(a)

I, the undersigned, do hereby certify that the attached petition contains 8,942 words, as measured by the Word Count function of Microsoft Word. This is less than the limit of 14,000 words as specified by 37 C.F.R. §42.24(a)(i).

Dated: October 7, 2025

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER

CERTIFICATION OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§42.6(e) and 42.105 on the Patent Owner of a copy of this Petition for *Inter Partes* Review and supporting materials via FedEx at the following correspondence address of record:

Davison IP
2244 Faraday Avenue, Suite 157
Carlsbad, CA
UNITED STATES

Dated: October 7, 2025

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER