

Ex. E-1 - Invalidity of U.S. Patent No. 8,327,426 against U.S. Patent Pub. No. 2006/0021019 to Hinton et al. ("Hinton 1")

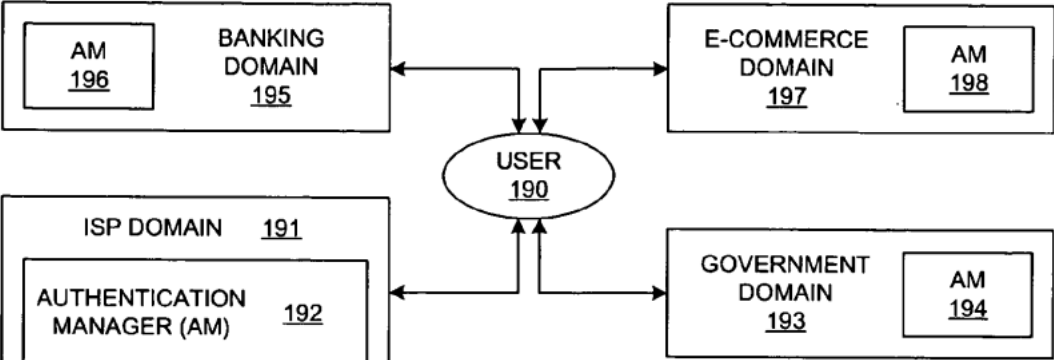
Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, Hinton 1 was filed on July 21, 2004, and published January 26, 2006, and is thus available as prior art under at least § 102(a) and (e).

As illustrated in the chart below, Hinton 1 anticipates the asserted claims of the '426 Patent. To the extent the Hinton 1 is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent the Hinton 1 is found not to anticipate any asserted claims or claim elements of the '426 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

Claim	Exemplary Citation from Hinton 1
<p>[1PRE] A machine-implemented method to execute on a machine, comprising:</p>	<p>Hinton 1 discloses and/or renders obvious a machine-implemented method to execute on a machine, the following steps.</p> <p>Hinton 1 at ¶63: "An assertion provides indirect evidence of some action. Assertions may provide indirect evidence of identity, authentication, attributes, authorization decisions, or other information and/or operations. An authentication assertion provides indirect evidence of authentication by an entity that is not the authentication service but that listened to the authentication service."</p> <p>Hinton 1 at ¶ 68: "An authentication credential is a set of challenge/response information that is used in various authentication protocols. For example, a username and password combination is the most familiar form of authentication credentials. Other forms of authentication credential may include various forms of challenge/response information, Public Key Infrastructure (PKI) certificates, smartcards, biometrics, etc. An authentication credential is differentiated from an authentication assertion: an authentication credential is presented by a user as part of an authentication protocol sequence with an authentication server or service, and an authentication assertion is a statement about the successful presentation and validation of a user's authentication credentials, subsequently transferred between entities when necessary."</p>

Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 237 856 264">Hinton 1 at Fig. 1E:</p>  <p data-bbox="1079 670 1262 756"><i>FIG. 1E</i> (PRIOR ART)</p> <p data-bbox="598 813 808 841">Hinton 1 at ¶74:</p> <p data-bbox="598 850 1892 1320">"In contrast to prior-art systems, the present invention provides a federation model for allowing enterprises to provide a single-sign-on experience to a user. In other words, the present invention supports a federated, heterogeneous environment. As an example of an object of the present invention, referring again to FIG. 1E, user 190 is able to authenticate to domain 191 and then have domain 191 provide the appropriate assertions to each downstream domain that might be involved in a transaction. These downstream domains need to be able to understand and trust authentication assertions and/or other types of assertions, even though there are no pre-established assertion formats between domain 191 and these other downstream domains. In addition to recognizing the assertions, the downstream domains need to be able to translate the identity contained within an assertion to an identity that represents user 190 within a particular domain, even though there is no pre-established identity mapping relationship. It should be noted, though, that the present invention is applicable to various types of domains and is not limited to ISP-type domains that are represented within FIG. 1E as exemplary domains."</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at ¶ 80: "As explained in more detail further below, the present invention provides significant user benefits. The present invention allows a user to authenticate at a first entity, hereinbelow also referred to as the user's home domain or authentication home domain. This first entity may act as an issuing party, which issues an authentication assertion about the user for use at a second entity. The user can then access protected resources at a second, distinct entity, termed the relying party, by presenting the authentication assertion that was issued by the first entity without having to explicitly re-authenticate at the second entity. Information that is passed from an issuing party to a relying party is in the form of an assertion, and this assertion may contain different types of information in the form of statements. For example, an assertion may be a statement about the authenticated identity of a user, or it may be a statement about user attribute information that is associated with a particular user."</p> <p>Hinton 1 at ¶ 101: "One role of a trust proxy/trust service may be to determine, or to be responsible for determining, the required token type for another domain and/or the trust proxy in that domain. A trust proxy has the ability or the responsibility to handle authentication token format translation from a format used by the issuing party to one understood by the receiving party. Trust proxy 254 is also responsible for any user identity translation or attribute translation that occurs for enterprise 250. In addition, a trust proxy can support the implementation of aliases as representatives of a user identity that uniquely identify a user without providing any addition information about the user's real world identity. Furthermore, a trust proxy can issue authorization and/or session credentials for use by the point-of-contact server. However, a trust proxy may invoke a trust broker for assistance, as described further below. Identity translation may be required to map a user's identity and attributes as known to an issuing party to one that is meaningful to a receiving party. This translation may be invoked by either a trust proxy at an issuing domain, a trust proxy at a receiving domain, or both."</p>
<p>[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;</p>	<p>Hinton 1 discloses and/or renders obvious 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.</p> <p>Hinton 1 at ¶ 106: "It should be noted that although FIG. 2C depicts point-of-contact server 252, trust proxy 254, security token service component 255, and authentication service runtime 256 as distinct entities, it is</p>

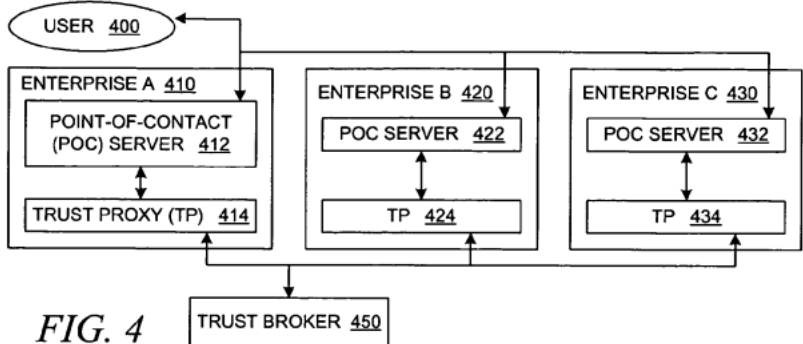
Claim	Exemplary Citation from Hinton 1
	<p>not necessary for these components to be implemented on separate devices. For example, it is possible for the functionality of these separate components to be implemented as applications on a single physical device or combined in a single application. In addition, FIG. 2C depicts a single point-of-contact server, a single trust proxy, and a single security token server for an enterprise, but an alternative configuration may include multiple point-of-contact servers, multiple trust proxies, and multiple security token servers for each enterprise. The point-of-contact server, the trust proxy, the security token service, and other federated entities may be implemented in various forms, such as software applications, objects, modules, software libraries, etc."</p> <p>Hinton 1 at ¶ 130: "With reference now to FIG. 3A, a flowchart depicts a generalized process at an issuing domain for creating an assertion within a federated environment. The process begins when the issuing domain's point-of-contact server is triggered for an assertion (step 302). The point-of-contact server may receive a request for a particular assertion for a given user from a relying domain, or it may intercept an outgoing request to a known relying domain that requires an assertion; these scenarios are described in more detail below with respect to FIG. 3C and FIG. 3D, respectively. In response to being triggered for an assertion, the issuing domain's point-of-contact server requests the assertion from the issuing domain's trust proxy (step 304), which generates the assertion (step 306), along with adding trust information, such as encryption/signature of the assertion/token; the issuing domain's trust proxy may request assistance from a trust broker to generate the required assertion if necessary. After generating the assertion, the issuing domain's trust proxy then returns the assertion to the issuing domain's point-of-contact server (step 308), which then injects the assertion into the output datastream in an appropriate manner (step 310), e.g., by inserting the assertion into an outgoing HTTP or SOAP message, thereby completing the process."</p> <p>Hinton at ¶ 139: "With reference now to FIG. 3D, a flowchart depicts a specific process for pushing an assertion from an issuing domain to a relying domain in response to the issuing domain actively intercepting an outgoing request to the relying domain. The process begins when a user requests a protected resource at the relying domain (step 352). The point-of-contact server intercepts the outgoing request (step 354), e.g., by filtering outgoing messages for predetermined Uniform Resource Identifiers (URI's), certain types of messages, certain types of message content, or in some other manner. The issuing</p>

Claim	Exemplary Citation from Hinton 1
	<p>domain's point-of-contact server then requests the generation of an appropriate assertion from the issuing domain's trust proxy (step 356), which generates the assertion with assistance from a trust broker if necessary (step 358). The issuing domain then transfers the user's request along with the generated assertion to the relying party (step 360), thereby completing the process. When the relying domain receives the request and its associated assertion, then the relying domain would validate the assertion in the manner shown in FIG. 3B."</p> <p>Hinton at ¶ 154: "With reference now to FIG. 4, a block diagram depicts a federated environment that supports federated single-sign-on operations. User 400, through a client device and an appropriate client application, such as a browser, desires to access a web service that is provided by enterprise/domain 410, which supports data processing systems that act as a federated domain within a federated environment. Domain 410 supports point-of-contact server 412 and trust proxy 414; similarly, domain 420 supports point-of-contact server 422 and trust proxy 424, while domain 430 supports point-of-contact server 432 and trust proxy 434. The trust proxies rely upon trust broker 450 for assistance, as described above. Additional domains and trust proxies may participate in the federated environment. FIG. 4 describes a federated single-sign-on operation between domain 410 and domain 420; a similar operation may occur between domain 410 and domain 430. The user completes an authentication operation with respect to domain 410; this authentication operation is handled by point-of-contact server 412. The authentication operation is triggered when the user requests access to some resource that requires an authenticated identity, e.g., for access control purposes or for personalization purposes. Point-of-contact server 412 may invoke a legacy authentication service, or it may invoke trust proxy 414 to validate the user's presented authentication credentials. Domain 410 becomes the user's home domain for the duration of the user's federated session."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 412, e.g., by selecting a special link on a web page that is hosted within domain 410 or by</p>

Claim	Exemplary Citation from Hinton 1
	<p>requesting a portal page that is hosted within domain 410 but that displays resources hosted in domain 420. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] B --> C[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] C --> D[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] D --> E[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] E --> F[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] F --> G([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] B --> C[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] C --> D[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] D --> E[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] E --> F[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] F --> G[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] G --> H[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] H --> I([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <pre> graph TD B1([BEGIN]) --> P1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] P1 --> P2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] P2 --> P3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] P3 --> P4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] P4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;"> <pre> graph TD B2([BEGIN]) --> P5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] P5 --> P6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] P6 --> P7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] P7 --> P8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] P8 --> P9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] P9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

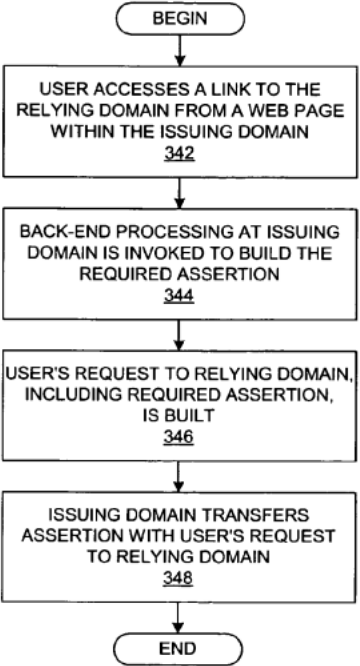
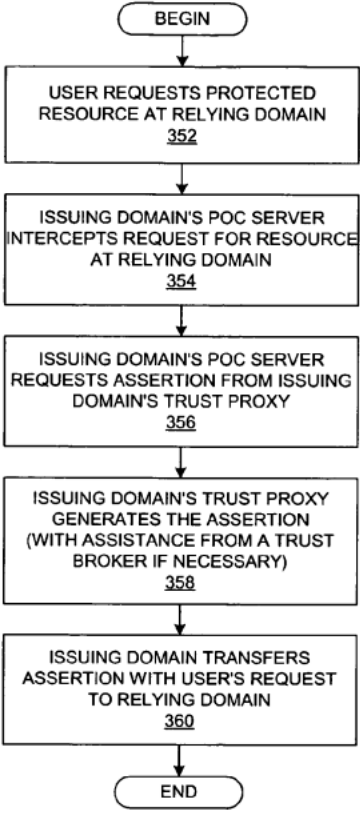
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 4 and corresponding text:</p>  <p><i>FIG. 4</i></p>
<p>[1B] authenticating, by the machine, the principal; and</p>	<p>Hinton 1 discloses and/or renders obvious authenticating, by the machine, the principal.</p> <p>Hinton 1 at ¶ 106: "It should be noted that although FIG. 2C depicts point-of-contact server 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. For example, it is possible for the functionality of these separate components to be implemented as applications on a single physical device or combined in a single application. In addition, FIG. 2C depicts a single point-of-contact server, a single trust proxy, and a single security token server for an enterprise, but an alternative configuration may include multiple point-of-contact servers, multiple trust proxies, and multiple security token servers for each enterprise. The point-of-contact server, the trust proxy, the security token service, and other federated entities may be implemented in various forms, such as software applications, objects, modules, software libraries, etc."</p> <p>Hinton 1 at ¶ 130: "With reference now to FIG. 3A, a flowchart depicts a generalized process at an issuing domain for creating an assertion within a federated environment. The process begins when the issuing domain's point-of-contact server is triggered for an assertion (step 302). The point-of-contact server may receive a request for a particular assertion for a given user from a relying domain, or it may intercept an outgoing request to a known relying domain that requires an assertion; these scenarios are</p>

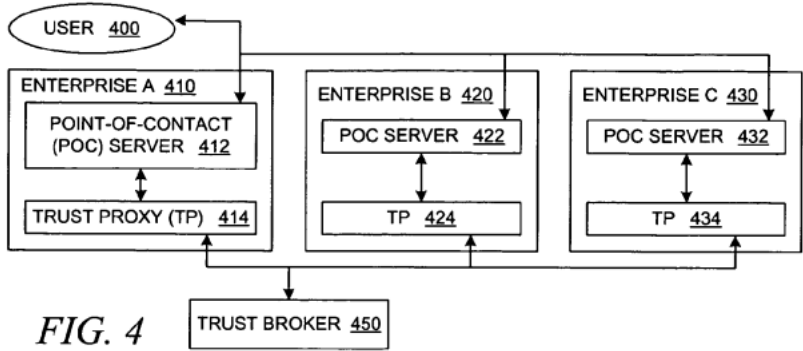
Claim	Exemplary Citation from Hinton 1
	<p>described in more detail below with respect to FIG. 3C and FIG. 3D, respectively. In response to being triggered for an assertion, the issuing domain's point-of-contact server requests the assertion from the issuing domain's trust proxy (step 304), which generates the assertion (step 306), along with adding trust information, such as encryption/signature of the assertion/token; the issuing domain's trust proxy may request assistance from a trust broker to generate the required assertion if necessary. After generating the assertion, the issuing domain's trust proxy then returns the assertion to the issuing domain's point-of-contact server (step 308), which then injects the assertion into the output datastream in an appropriate manner (step 310), e.g., by inserting the assertion into an outgoing HTTP or SOAP message, thereby completing the process."</p> <p>Hinton at ¶ 139: "\"With reference now to FIG. 3D, a flowchart depicts a specific process for pushing an assertion from an issuing domain to a relying domain in response to the issuing domain actively intercepting an outgoing request to the relying domain. The process begins when a user requests a protected resource at the relying domain (step 352). The point-of-contact server intercepts the outgoing request (step 354), e.g., by filtering outgoing messages for predetermined Uniform Resource Identifiers (URI's), certain types of messages, certain types of message content, or in some other manner. The issuing domain's point-of-contact server then requests the generation of an appropriate assertion from the issuing domain's trust proxy (step 356), which generates the assertion with assistance from a trust broker if necessary (step 358). The issuing domain then transfers the user's request along with the generated assertion to the relying party (step 360), thereby completing the process. When the relying domain receives the request and its associated assertion, then the relying domain would validate the assertion in the manner shown in FIG. 3B.\""</p> <p>Hinton at ¶ 154: "\"With reference now to FIG. 4, a block diagram depicts a federated environment that supports federated single-sign-on operations. User 400, through a client device and an appropriate client application, such as a browser, desires to access a web service that is provided by enterprise/domain 410, which supports data processing systems that act as a federated domain within a federated environment. Domain 410 supports point-of-contact server 412 and trust proxy 414; similarly, domain 420 supports point-of-contact server 422 and trust proxy 424, while domain 430 supports point-of-contact server 432 and trust proxy 434. The trust proxies rely upon trust broker 450 for</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance, as described above. Additional domains and trust proxies may participate in the federated environment. FIG. 4 describes a federated single-sign-on operation between domain 410 and domain 420; a similar operation may occur between domain 410 and domain 430. The user completes an authentication operation with respect to domain 410; this authentication operation is handled by point-of-contact server 412. The authentication operation is triggered when the user requests access to some resource that requires an authenticated identity, e.g., for access control purposes or for personalization purposes. Point-of-contact server 412 may invoke a legacy authentication service, or it may invoke trust proxy 414 to validate the user's presented authentication credentials. Domain 410 becomes the user's home domain for the duration of the user's federated session."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] B --> C[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] C --> D[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] D --> E[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] E --> F[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] F --> G([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] B --> C[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] C --> D[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] D --> E[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] E --> F[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] F --> G[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] G --> H[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] H --> I([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD BEGIN1([BEGIN]) --> 342[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] 342 --> 344[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] 344 --> 346[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] 346 --> 348[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] 348 --> END1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD BEGIN2([BEGIN]) --> 352[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] 352 --> 354[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] 354 --> 356[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] 356 --> 358[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] 358 --> 360[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] 360 --> END2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 4 and corresponding text:</p>  <p style="text-align: center;"><i>FIG. 4</i></p>
<p>[1C] supplying, by the machine, an authentication message for use by an identity service on behalf of the principal, 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,</p>	<p>Hinton 1 discloses and/or renders obvious supplying, by the machine, an authentication message for use by an identity service on behalf of the principal, 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.</p> <p>Hinton 1 at ¶ 94: "After joining a federated environment, the domain may continue to operate without the intervention of federated components. In other words, the domain may be configured so that users may continue to access particular application servers or other protected resources directly without going through a point-of-contact server or other component implementing this point-of-contact server functionality; a user that accesses a system in this manner would experience typical authentication flows and typical access. In doing so, however, a user that directly accesses the legacy system would not be able to establish a federated session that is known to the domain's point-of-contact server."</p> <p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token,</p>

Claim	Exemplary Citation from Hinton 1
	<p>including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158:</p> <p>"At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The</p>

Claim	Exemplary Citation from Hinton 1
	<p>federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p>

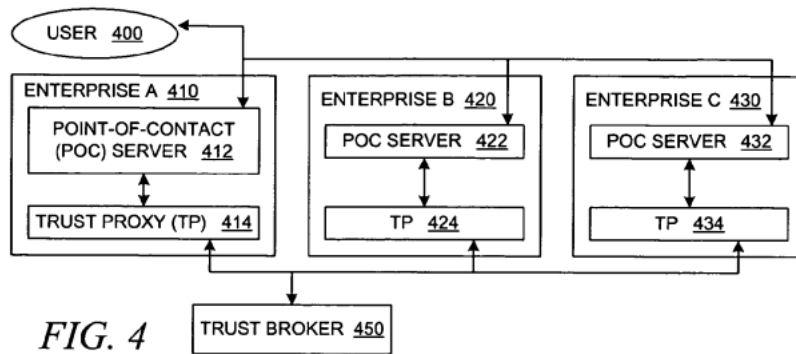
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] B --> C[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] C --> D[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] D --> E[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] E --> F[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] F --> G([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] B --> C[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] C --> D[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] D --> E[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] E --> F[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] F --> G[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] G --> H[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] H --> I([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <pre> graph TD BEGIN1([BEGIN]) --> 342[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] 342 --> 344[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] 344 --> 346[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] 346 --> 348[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] 348 --> END1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;"> <pre> graph TD BEGIN2([BEGIN]) --> 352[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] 352 --> 354[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] 354 --> 356[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] 356 --> 358[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] 358 --> 360[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] 360 --> END2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



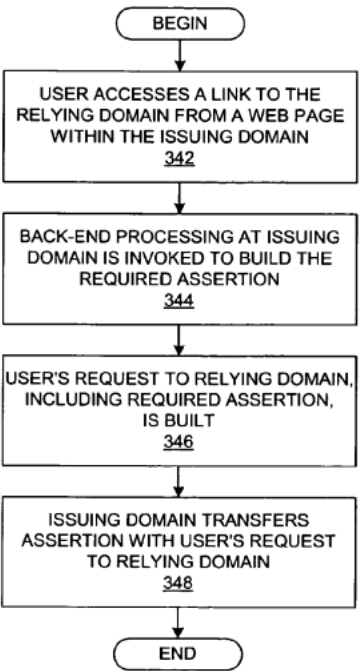
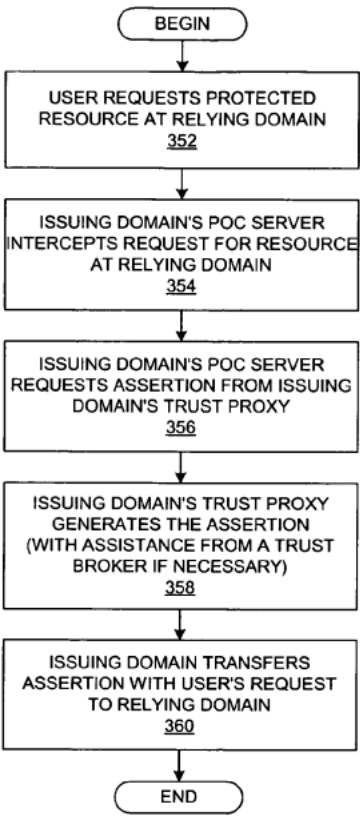
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[1D] the identity service acts as a proxy for access sessions to the other services on behalf of the principal,</p>	<p>Hinton 1 discloses and/or renders obvious that the identity service acts as a proxy for access sessions to the other services on behalf of the principal.</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at ¶ 94: "After joining a federated environment, the domain may continue to operate without the intervention of federated components. In other words, the domain may be configured so that users may continue to access particular application servers or other protected resources directly without going through a point-of-contact server or other component implementing this point-of-contact server functionality; a user that accesses a system in this manner would experience typical authentication flows and typical access. In doing so, however, a user that directly accesses the legacy system would not be able to establish a federated session that is known to the domain's point-of-contact server."</p> <p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420;</p>

Claim	Exemplary Citation from Hinton 1
	<p>this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will</p>

Claim	Exemplary Citation from Hinton 1
	<p>have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management server subsequently sends the federated provisioning message along with a security token to one or</p>

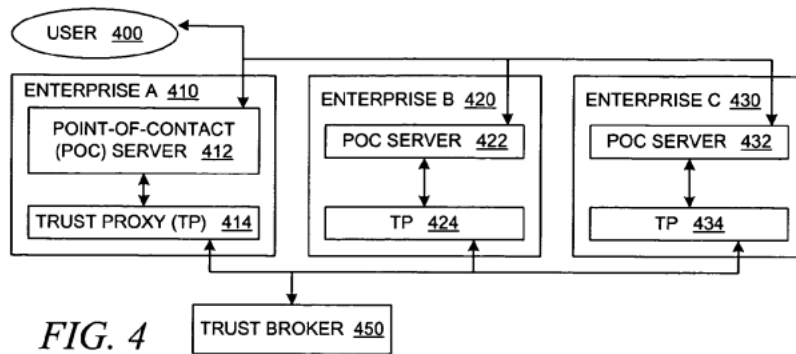
Claim	Exemplary Citation from Hinton 1
	<p>more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="611 386 898 1096" style="width: 45%;"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div data-bbox="957 386 1270 1274" style="width: 45%;"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

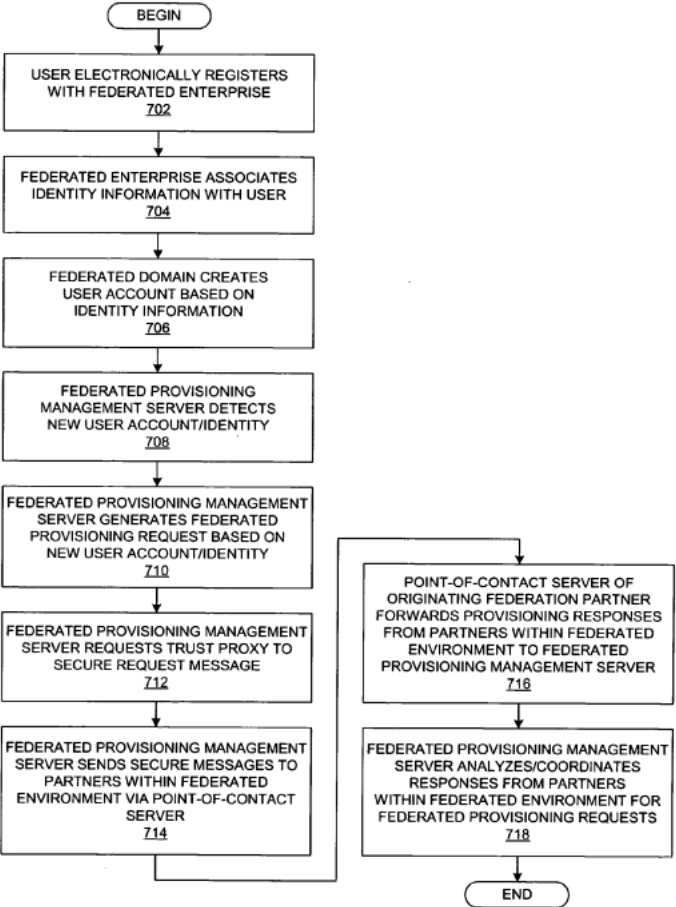
Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p>  <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[1E] the principal's access sessions occur indirectly through the identity service and transparently to the principal,</p>	<p>Hinton 1 discloses and/or renders obvious that the principal's access sessions occur indirectly through the identity service and transparently to the principal.</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at ¶ 94: "After joining a federated environment, the domain may continue to operate without the intervention of federated components. In other words, the domain may be configured so that users may continue to access particular application servers or other protected resources directly without going through a point-of-contact server or other component implementing this point-of-contact server functionality; a user that accesses a system in this manner would experience typical authentication flows and typical access. In doing so, however, a user that directly accesses the legacy system would not be able to establish a federated session that is known to the domain's point-of-contact server."</p> <p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420;</p>

Claim	Exemplary Citation from Hinton 1
	<p>this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will</p>

Claim	Exemplary Citation from Hinton 1
	<p>have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management server subsequently sends the federated provisioning message along with a security token to one or</p>

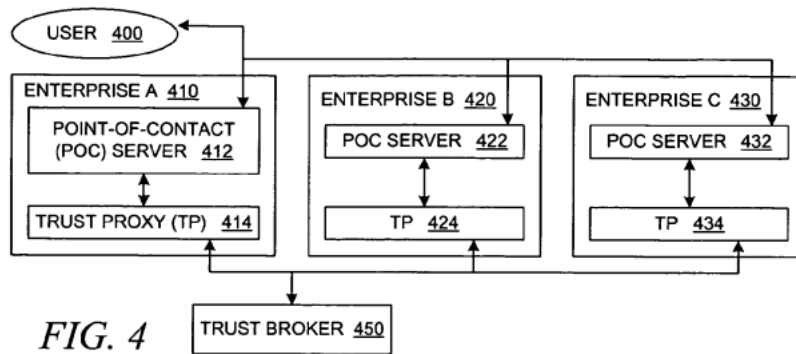
Claim	Exemplary Citation from Hinton 1
	<p>more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="611 386 898 1096" style="width: 45%;"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div data-bbox="957 386 1272 1274" style="width: 45%;"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;"> <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[1F] wherein the authentication message includes the new authentication request made on behalf of the principal</p>	<p>Hinton 1 discloses and/or renders obvious that 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>and the authentication message also includes a new authentication response that satisfies the new authentication request,</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account</p>

Claim	Exemplary Citation from Hinton 1
	<p>deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p>

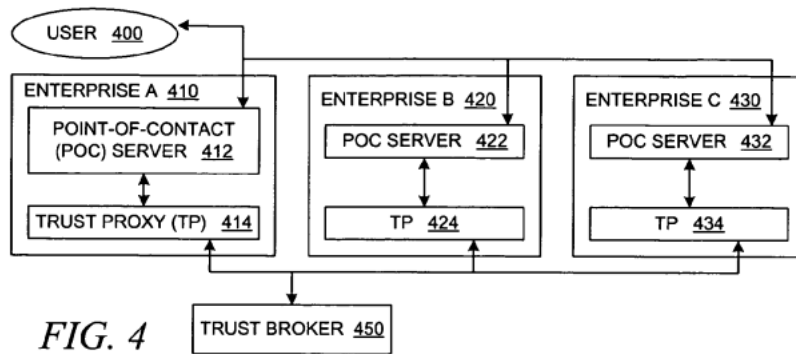
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] B --> C[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] C --> D[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] D --> E[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] E --> F[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] F --> G([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div style="width: 45%;"> <pre> graph TD A([BEGIN]) --> B[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] B --> C[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] C --> D[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] D --> E[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] E --> F[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] F --> G[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] G --> H[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] H --> I([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;"> <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



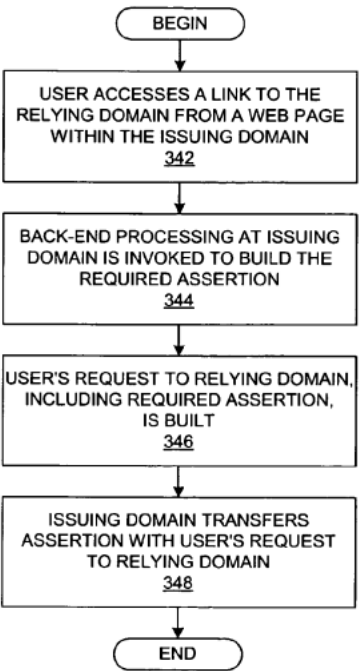
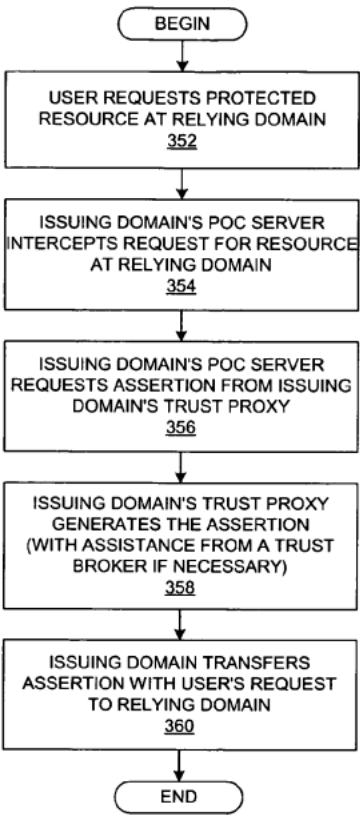
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[1G] that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal,</p>	<p>Hinton 1 discloses and/or renders obvious that that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal, the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to.</p>

Claim	Exemplary Citation from Hinton 1
<p>the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to,</p>	<p>Hinton 1 at ¶ 94: "After joining a federated environment, the domain may continue to operate without the intervention of federated components. In other words, the domain may be configured so that users may continue to access particular application servers or other protected resources directly without going through a point-of-contact server or other component implementing this point-of-contact server functionality; a user that accesses a system in this manner would experience typical authentication flows and typical access. In doing so, however, a user that directly accesses the legacy system would not be able to establish a federated session that is known to the domain's point-of-contact server."</p> <p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420;</p>

Claim	Exemplary Citation from Hinton 1
	<p>this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will</p>

Claim	Exemplary Citation from Hinton 1
	<p>have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management server subsequently sends the federated provisioning message along with a security token to one or</p>

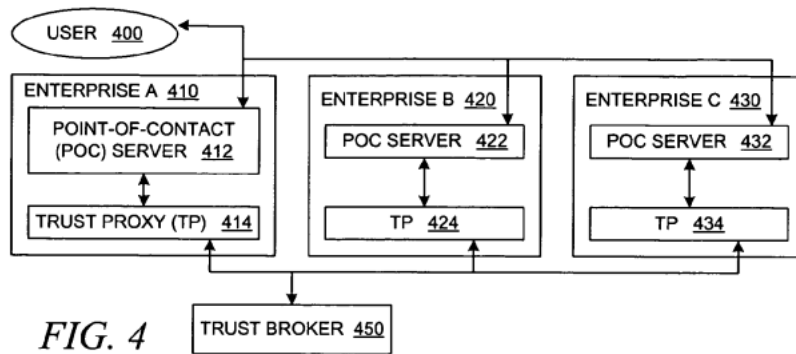
Claim	Exemplary Citation from Hinton 1
	<p>more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="611 386 898 1096" style="width: 45%;"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div data-bbox="957 386 1270 1274" style="width: 45%;"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



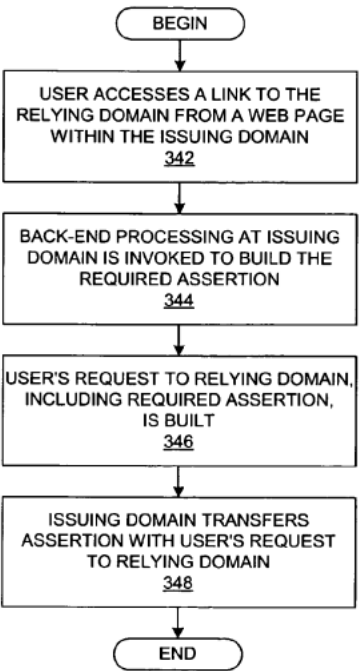
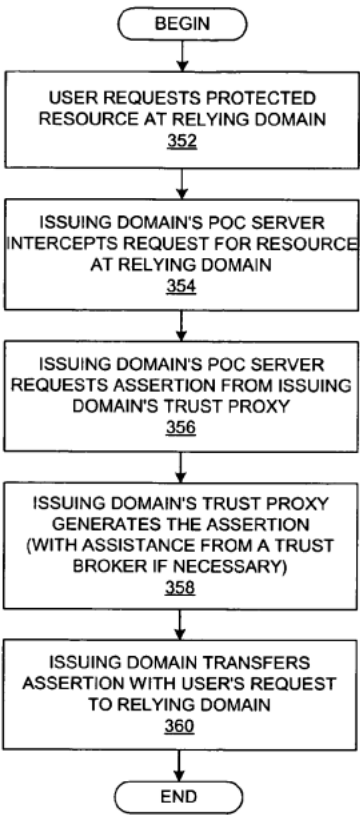
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[1H] and a determination as to whether to use a single interaction or multiple interactions for authentication of the</p>	<p>Hinton 1 discloses and/or renders obvious 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>principal to the other services is automatically communicated in the new authentication response.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

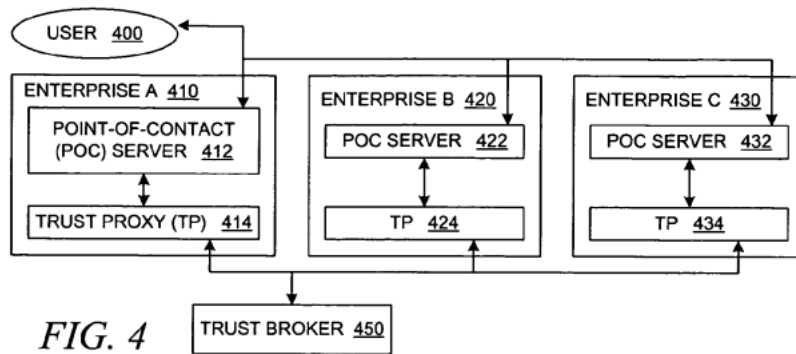
Claim	Exemplary Citation from Hinton 1
	<p>server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p>Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="611 423 898 1133"> <pre> graph TD B1(BEGIN) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1(END) </pre> <p style="text-align: center;"><i>FIG. 3A</i></p> </div> <div data-bbox="957 423 1272 1312"> <pre> graph TD B2(BEGIN) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2(END) </pre> <p style="text-align: center;"><i>FIG. 3B</i></p> </div> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[2] The method of claim 1 further comprising, making, by the machine, a target service available to interactions between the</p>	<p>Hinton 1 discloses and/or renders obvious 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>principal and an external service, the target service is directly accessible from an environment of the identity service.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

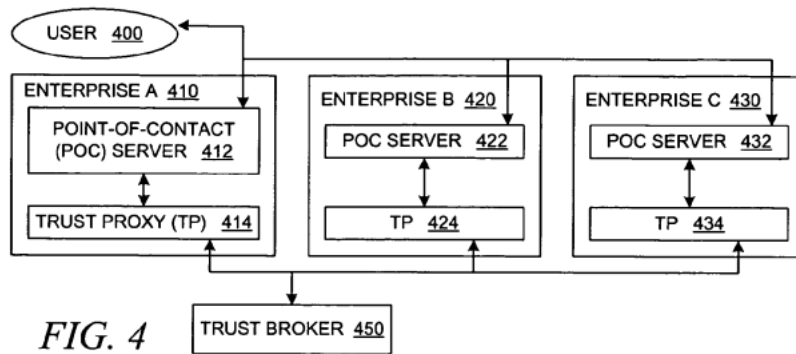
Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 240 1871 342">server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p data-bbox="598 383 1220 415">Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div data-bbox="606 423 898 1133"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p data-bbox="699 1149 806 1182"><i>FIG. 3A</i></p> </div> <div data-bbox="957 423 1270 1312"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p data-bbox="1058 1328 1165 1360"><i>FIG. 3B</i></p> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD BEGIN([BEGIN]) --> 342[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] 342 --> 344[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] 344 --> 346[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] 346 --> 348[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] 348 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 3C</i></p> </div> <div style="width: 45%;"> <pre> graph TD BEGIN([BEGIN]) --> 352[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] 352 --> 354[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] 354 --> 356[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] 356 --> 358[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] 358 --> 360[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] 360 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[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.</p>	<p>Hinton 1 discloses and/or renders obvious that 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>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.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

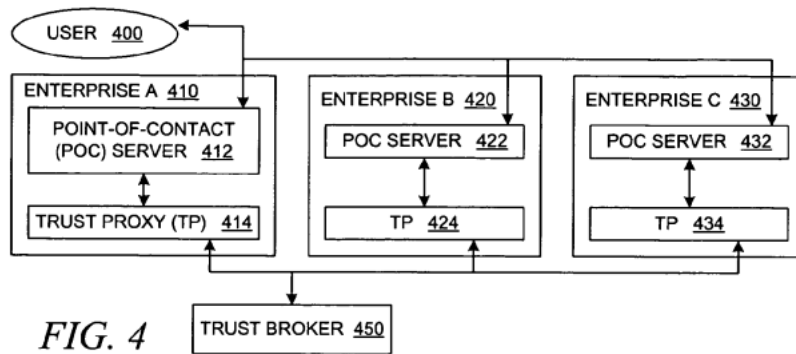
Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 240 1871 342">server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p data-bbox="598 383 1220 415">Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div data-bbox="611 423 898 1133"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p data-bbox="699 1149 806 1182"><i>FIG. 3A</i></p> </div> <div data-bbox="957 423 1272 1312"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p data-bbox="1058 1328 1165 1360"><i>FIG. 3B</i></p> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p style="text-align: center;"><i>FIG. 3C</i></p> </div> <div style="width: 45%;"> <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p style="text-align: center;"><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



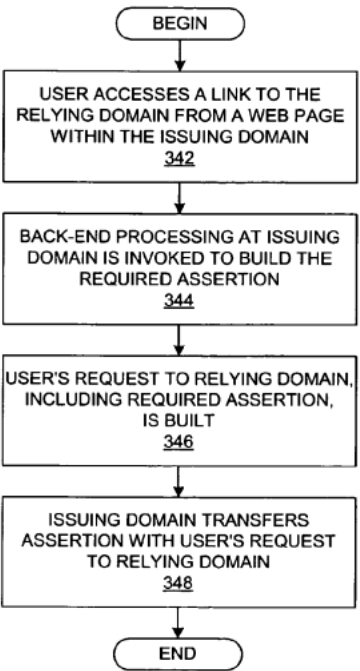
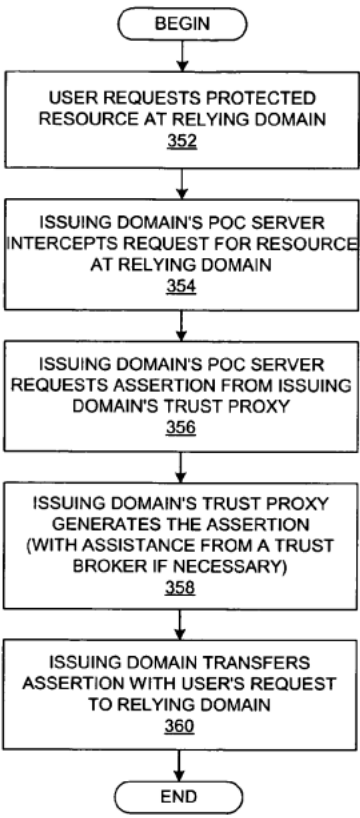
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[4] The method of claim 3, wherein supplying further includes representing the new authentication response as a first authentication</p>	<p>Hinton 1 discloses and/or renders obvious that 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>token that informs the identity service that the principal is currently already properly authenticated to the processing associated with the method.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

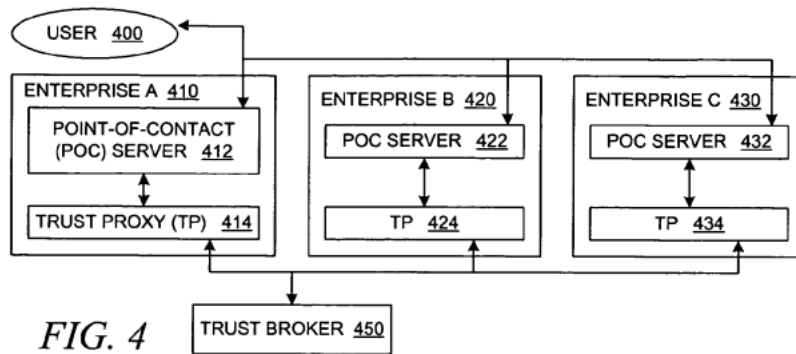
Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 240 1871 342">server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p data-bbox="598 383 1220 415">Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div data-bbox="611 423 898 1133"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p data-bbox="699 1149 806 1182"><i>FIG. 3A</i></p> </div> <div data-bbox="957 423 1268 1312"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p data-bbox="1058 1328 1165 1360"><i>FIG. 3B</i></p> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[5] The method of claim 4, wherein supplying further includes adding a second authentication to a second redirection of the principal,</p>	<p>Hinton 1 discloses and/or renders obvious that 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>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.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

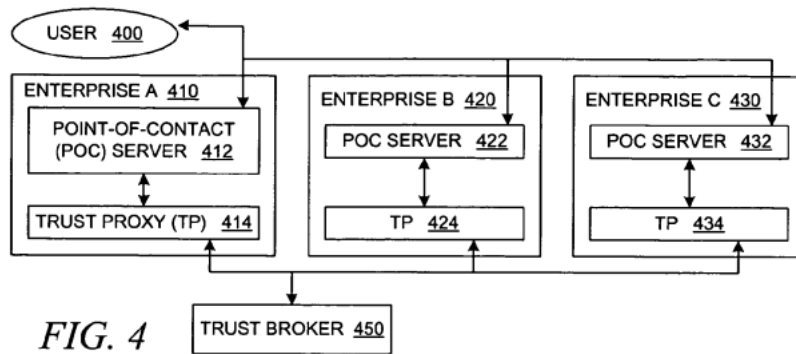
Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 240 1871 342">server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p data-bbox="598 383 1220 415">Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div data-bbox="611 423 898 1133"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p data-bbox="701 1149 806 1182"><i>FIG. 3A</i></p> </div> <div data-bbox="957 423 1268 1312"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p data-bbox="1058 1328 1163 1360"><i>FIG. 3B</i></p> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;"> <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



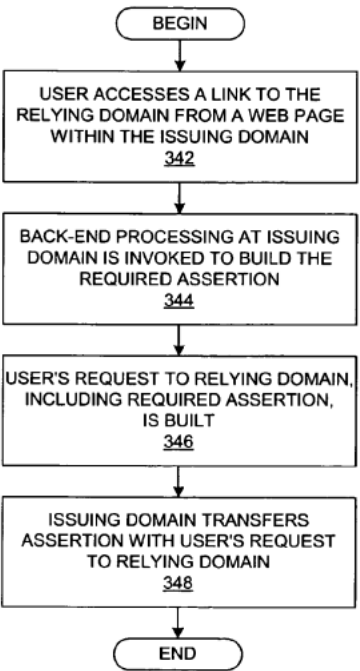
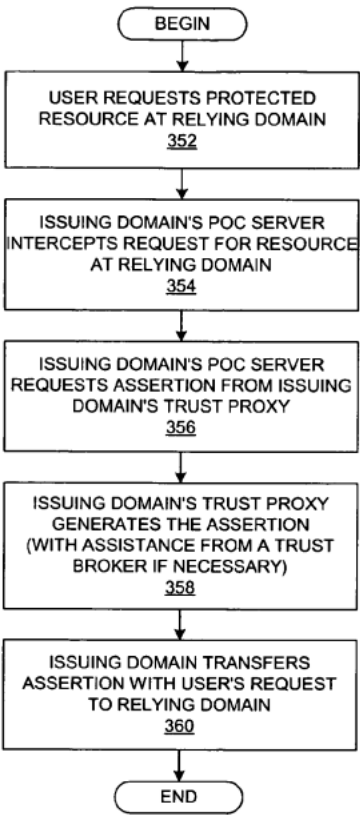
Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[6] The method of claim 1, wherein supplying further includes representing the new authentication response as an instruction to the</p>	<p>Hinton 1 discloses and/or renders obvious that 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service.</p>	<p>Hinton 1 at ¶ 132: "With reference now to FIG. 3B, a flowchart depicts a generalized process at a relying domain for tearing down an assertion. The process begins when a relying domain's point-of-contact server receives a message with an associated assertion (step 322), after which it extracts the assertion and forwards the assertion to the relying domain's trust proxy (step 324). The relying domain's trust proxy extracts information from the assertion, including the token received from the issuing domain (step 326); the relying domain's trust proxy will invoke the security token service to validate this token, including the information in the token and the trust information on the token such as encryption and signatures, thereafter returning a locally valid token for the user if appropriate (step 328)."</p> <p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with</p>

Claim	Exemplary Citation from Hinton 1
	<p>assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p> <p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a</p>

Claim	Exemplary Citation from Hinton 1
	<p>direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶ 181: "Continuing with the process in FIG. 7, the federated provisioning management server generates a federated provisioning request that is based on the new user identity and/or other user-specific information (step 710); the federated provisioning request is a message body or other data item that contains the user-registration information to be transmitted to other federated partners. It should be noted, though, that provisioning entails many types of operations, such as account creation, account deletion, attribute update (write, update, delete), and other types of operations, so a federated provisioning request message may be directed to any other these operations. The federated provisioning management server requests that the local trust proxy within the federated enterprise build a security token that accompanies the federated provisioning request (step 712). It should be noted that any of the described processing steps may include many steps; for example, the federated provisioning management server may perform a series of operations, including functionality over web-application services (WAS), thereby causing the invocation of WAS security handlers that subsequently invoke the trust proxy to validate the tokens associated with the incoming request. The federated provisioning management server includes the functionality of packing/unpacking the provisioning request/response itself, which is independent of packing/unpacking the security on the request/response. The trust proxy may encrypt information, generate security tokens, perform authorization decisions, or perform other security-related operations that are necessary to ensure that federated partners that receive the federated provisioning message can trust the contents of the received message based on the trust relationships that have been established between the federated partners and that are managed by the local trust proxy in conjunction with trust proxies at the federated partners. The manner in which the federated provisioning message is built may depend on the identity of the targeted/destination federated domain and the requirements of the secure messages that are expected by the trust proxy at the destination federated domain. The identities of the federation partners to which the newly registered user should be provisioned may be determined by reference to a local database or other source of information that is used to manage the relationships between the federated enterprise and its federated partners. The federated provisioning management</p>

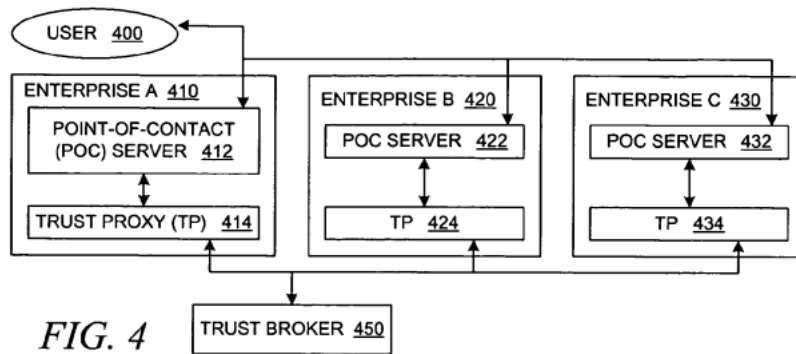
Claim	Exemplary Citation from Hinton 1
	<p data-bbox="598 240 1871 342">server subsequently sends the federated provisioning message along with a security token to one or more federated domains using the local point-of-contact server within the federated enterprise (step 714)."</p> <p data-bbox="598 383 1220 415">Hinton 1 at Figs. 3A-3D and corresponding text:</p> <div data-bbox="598 423 903 1136"> <pre> graph TD B1([BEGIN]) --> S1[ISSUING DOMAIN'S POINT-OF-CONTACT (POC) SERVER IS TRIGGERED FOR AN ASSERTION 302] S1 --> S2[ISSUING DOMAIN'S POC SERVER REQUESTS THE ASSERTION FROM THE ISSUING DOMAIN'S TRUST PROXY 304] S2 --> S3[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 306] S3 --> S4[ISSUING DOMAIN'S TRUST PROXY RETURNS THE ASSERTION TO ISSUING DOMAIN'S POC SERVER 308] S4 --> S5[ISSUING DOMAIN'S POC SERVER INSERTS ASSERTION INTO OUTPUT DATASTREAM IN AN APPROPRIATE MANNER, E.G., OUTGOING MESSAGE 310] S5 --> E1([END]) </pre> <p data-bbox="699 1149 808 1182"><i>FIG. 3A</i></p> </div> <div data-bbox="955 423 1270 1307"> <pre> graph TD B2([BEGIN]) --> S6[RELYING DOMAIN'S POC SERVER GETS MESSAGE WITH ASSOCIATED ASSERTION 322] S6 --> S7[RELYING DOMAIN'S POC SERVER EXTRACTS ASSERTION AND FORWARDS IT TO RELYING DOMAIN'S TRUST PROXY 324] S7 --> S8[RELYING DOMAIN'S TRUST PROXY EXTRACTS INFORMATION FROM ASSERTION 326] S8 --> S9[RELYING DOMAIN'S TRUST PROXY ATTEMPTS TO VALIDATE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 328] S9 --> S10[RELYING DOMAIN'S TRUST PROXY GENERATES LOCAL INFORMATION 330] S10 --> S11[RELYING DOMAIN'S TRUST PROXY RETURNS REQUIRED INFORMATION TO RELYING DOMAIN'S POC SERVER 332] S11 --> S12[RELYING DOMAIN'S POC SERVER FORWARDS USER REQUEST AND RELEVANT INFORMATION TO BACKEND APPLICATION OR SERVICE 334] S12 --> E2([END]) </pre> <p data-bbox="1056 1328 1165 1360"><i>FIG. 3B</i></p> </div>

Claim	Exemplary Citation from Hinton 1
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <pre> graph TD B1([BEGIN]) --> S1[USER ACCESSES A LINK TO THE RELYING DOMAIN FROM A WEB PAGE WITHIN THE ISSUING DOMAIN 342] S1 --> S2[BACK-END PROCESSING AT ISSUING DOMAIN IS INVOKED TO BUILD THE REQUIRED ASSERTION 344] S2 --> S3[USER'S REQUEST TO RELYING DOMAIN, INCLUDING REQUIRED ASSERTION, IS BUILT 346] S3 --> S4[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 348] S4 --> E1([END]) </pre> <p><i>FIG. 3C</i></p> </div> <div style="text-align: center;">  <pre> graph TD B2([BEGIN]) --> S5[USER REQUESTS PROTECTED RESOURCE AT RELYING DOMAIN 352] S5 --> S6[ISSUING DOMAIN'S POC SERVER INTERCEPTS REQUEST FOR RESOURCE AT RELYING DOMAIN 354] S6 --> S7[ISSUING DOMAIN'S POC SERVER REQUESTS ASSERTION FROM ISSUING DOMAIN'S TRUST PROXY 356] S7 --> S8[ISSUING DOMAIN'S TRUST PROXY GENERATES THE ASSERTION (WITH ASSISTANCE FROM A TRUST BROKER IF NECESSARY) 358] S8 --> S9[ISSUING DOMAIN TRANSFERS ASSERTION WITH USER'S REQUEST TO RELYING DOMAIN 360] S9 --> E2([END]) </pre> <p><i>FIG. 3D</i></p> </div> </div>

Claim

Exemplary Citation from Hinton 1

Hinton 1 at Fig. 4 and corresponding text:



Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at Fig. 7 and corresponding text:</p> <pre> graph TD BEGIN([BEGIN]) --> 702[USER ELECTRONICALLY REGISTERS WITH FEDERATED ENTERPRISE 702] 702 --> 704[FEDERATED ENTERPRISE ASSOCIATES IDENTITY INFORMATION WITH USER 704] 704 --> 706[FEDERATED DOMAIN CREATES USER ACCOUNT BASED ON IDENTITY INFORMATION 706] 706 --> 708[FEDERATED PROVISIONING MANAGEMENT SERVER DETECTS NEW USER ACCOUNT/IDENTITY 708] 708 --> 710[FEDERATED PROVISIONING MANAGEMENT SERVER GENERATES FEDERATED PROVISIONING REQUEST BASED ON NEW USER ACCOUNT/IDENTITY 710] 710 --> 712[FEDERATED PROVISIONING MANAGEMENT SERVER REQUESTS TRUST PROXY TO SECURE REQUEST MESSAGE 712] 712 --> 714[FEDERATED PROVISIONING MANAGEMENT SERVER SENDS SECURE MESSAGES TO PARTNERS WITHIN FEDERATED ENVIRONMENT VIA POINT-OF-CONTACT SERVER 714] 714 --> 716[POINT-OF-CONTACT SERVER OF ORIGINATING FEDERATION PARTNER FORWARDS PROVISIONING RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT TO FEDERATED PROVISIONING MANAGEMENT SERVER 716] 716 --> 718[FEDERATED PROVISIONING MANAGEMENT SERVER ANALYZES/COORDINATES RESPONSES FROM PARTNERS WITHIN FEDERATED ENVIRONMENT FOR FEDERATED PROVISIONING REQUESTS 718] 718 --> END([END]) </pre> <p style="text-align: center;"><i>FIG. 7</i></p>
<p>[7] The method of claim 1 further comprising, interacting, by the machine, with the principal via a World-Wide Web (WWW)</p>	<p>Hinton 1 discloses and/or renders obvious 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.</p>

Claim	Exemplary Citation from Hinton 1
<p>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.</p>	<p>Hinton 1 at ¶ 156-158: "At some later point in time, the user initiates a transaction at a federation partner, such as enterprise 420 that also supports a federated domain, thereby triggering a federated single-sign-on operation. For example, a user may initiate a new transaction at domain 420, or the user's original transaction may cascade into one or more additional transactions at other domains. As another example, the user may invoke a federated single-sign-on operation to a resource in domain 420 via point-of-contact server 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. Point-of-contact server 412 sends a request to trust proxy 414 to generate a federation single-sign-on token for the user that is formatted to be understood or trusted by domain 420. Trust proxy 414 returns this token to point-of-contact server 412, which sends this token to point-of-contact server 422 in domain. Domain 410 acts as an issuing party for the user at domain 420, which acts as a relying party. The user's token would be transferred with the user's request to domain 420; this token may be sent using HTTP redirection via the user's browser, or it may be sent by invoking the request directly of point-of-contact server 422 (over HTTP or SOAP-over-HTTP) on behalf of the user identified in the token supplied by trust proxy 414. Point-of-contact server 422 receives the request together with the federation single-sign-on token and invokes trust proxy 424. Trust proxy 424 receives the federation single-sign-on token, validates the token, and assuming that the token is valid and trusted, generates a locally valid token for the user. Trust proxy 424 returns the locally valid token to point-of-contact server 422, which establishes a session for the user within domain 420. If necessary, point-of-contact server 422 can initiate a federated single-sign-on at another federated partner. Validation of the token at domain 420 is handled by the trust proxy 424, possibly with assistance from a security token service. Depending on the type of token presented by domain 410, the security token service may need to access a user registry at domain 420. For example, domain 420 may provide a binary security token containing the user's name and password to be validated against the user registry at domain 420. Hence, in this example, an enterprise simply validates the security token from a federated partner. The trust relationship between domains 410 and 420 ensures that domain 420 can understand and trust the security token presented by domain 410 on behalf of the user."</p>

Claim	Exemplary Citation from Hinton 1
	<p>Hinton 1 at ¶ 159: "Federated single-sign-on requires not only the validation of the security token that is presented to a relying domain on behalf of the user but the determination of a locally valid user identifier at the relying domain based on information contained in the security token. One result of a direct trust relationship and the business agreements required to establish such a relationship is that at least one party, either the issuing domain or the relying domain or both, will know how to translate the information provided by the issuing domain into an identifier valid at the relying domain. In the brief example above, it was assumed that the issuing domain, i.e. domain 410, is able to provide the relying domain, i.e. domain 420, with a user identifier that is valid in domain 420. In that scenario, the relying domain did not need to invoke any identity mapping functionality. Trust proxy 424 at domain 420 will generate a security token for the user that will "vouch-for" this user. The types of tokens that are accepted, the signatures that are required on tokens, and other requirements are all pre-established as part of the federation's business agreements. The rules and algorithms that govern identifier translation are also pre-established as part of the federation's business agreements. In the case of a direct trust relationship between two participants, the identifier translation algorithms will have been established for those two parties and may not be relevant for any other parties in the federation."</p> <p>Hinton 1 at § 160: "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. In some cases, it may be the relying domain that knows how to do this mapping, while in yet other cases, neither party will know how to do this translation, in which case a third party trust broker may need to be invoked. In other words, in the case of a brokered trust relationship, the issuing and relying domains do not have a direct trust relationship with each other. They will, however, have a direct trust relationship with a trust broker, such as trust broker 450. Identifier mapping rules and algorithms will have been established as part of this relationship, and the trust broker will use this information to assist in the identifier translation that is required for a brokered trust relationship."</p> <p>Hinton 1 at ¶66: "A Security Assertion Markup Language (SAML) assertion is an example of a possible assertion format that may be used within the present invention. SAML has been promulgated by the</p>

Claim	Exemplary Citation from Hinton 1
	<p>Organization for the Advancement of Structured Information Standards (OASIS), which is a non-profit, global consortium. SAML is described in "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)", Committee Specification 01, May 31, 2002, as follows: The Security Assertion Markup Language (SAML) is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. A typical example of a subject is a person, identified by his or her email address in a particular Internet DNS domain. Assertions can convey information about authentication acts performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. Assertions are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different internal statements about authentication, authorization, and attributes. Note that assertions containing authentication statements merely describe acts of authentication that happened previously. Assertions are issued by SAML authorities, namely, authentication authorities, attribute authorities, and policy decision points. SAML defines a protocol by which clients can request assertions from SAML authorities and get a response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols; SAML currently defines one binding, to SOAP over HTTP. SAML authorities can use various sources of information, such as external policy stores and assertions that were received as input in requests, in creating their responses. Thus, while clients always consume assertions, SAML authorities can be both producers and consumers of assertions. The SAML specification states that an assertion is a package of information that supplies one or more statements made by an issuer. SAML allows issuers to make three different kinds of assertion statements: authentication, in which the specified subject was authenticated by a particular means at a particular time; authorization, in which a request to allow the specified subject to access the specified resource has been granted or denied; and attribute, in which the specified subject is associated with the supplied attributes. As discussed further below, various assertion formats can be translated to other assertion formats when necessary."</p>