Trust Framework

Identity Federation Rules
For the Insurance and Financial Services Industry

Version 1.5, December 14, 2023

Revision History

Date	Author	Version	Change Reference
April 30, 2014		1.0	Initial Version
December 20, 2017	I. Kantar	1.1	General Cleanup – removed reference to WS Federation and SSL
March 20, 2020	I. Kantar	1.2	Added MFA Attribute to Section 3.02©(iii)
November 15, 2020	I. Kantar	1.3	Added de-provisioning to Section 3.02(d)(i)
June 1, 2021	I. Kantar	1.4	Added OIDC to Section 3.02(a)(ii) Standards and to all instances of SAML, and GUID in Section 3.02(c)(ii) Optional Attributes,
December 1, 2023	A. Vaz	1.5	Added 3-year recertification Deleted MFA Attribute requirements Section 3.02(c)(iii) Added MFA Attributes 3.02(c)(iv) Added MFA Code Lists Appendix H Updated version date to 12/14/2023

Mission Statement

Our mission is promoting information security and identity management for trusted transactions across the financial services and insurance industries for purposes including but not limited to reducing transaction friction, lowering cost and bolstering independent agent access.

Article 1: Business

1.01(a) Scope

This Trust Framework defines the business, legal and technology Rules governing Participation in the ID Federation. The ID Federation is intended to provide federation of identities as described in this Trust Framework by and between Participants who have Existing Commercial Relationships by which they are involved in the provision of, sale, distribution, licensing, or use of a financial or insurance-related product or service. This Trust Framework is not intended to create commercial relationships between Parties with no other relationship, but rather is intended to improve security, enhance ease of use, and replace passwords with federated identities by and between Parties with existing trusted relationships within the financial services and insurance industry. This Trust Framework applies to Parties that have executed the Participation Agreement and thereby have agreed to the terms and conditions of this Trust Framework. The authoritative and current version of this Trust Framework is the document available at the ID Federation website (currently signononce.Org.). This Trust Framework incorporates by reference Formal Policies and Official Documents which are available from the ID Federation website.

Parties may also have a capacity within the ID Federation. One simple example is that an insurance carrier may be a Member of the ID Federation and, in that capacity, the insurance carrier could vote on Rule changes. At the same time, that Party may also be a Relying Party, and in that capacity they are subject to the Rules in this Trust Framework.

1.01(b) Roles

The Roles described in Sections 1.01(b)(i)-(vi) are Participants in the ID Federation operational system. A Party may undertake more than one Role under this Trust Framework.

1.01(b)(i) Identity Provider

An Identity Provider (IdP) is a Participant that issues Tokens to Individual Users and effectuates the passing of those Tokens to Relying Parties for purposes of asserting and Authenticating Individual User identities. An IdP is responsible for issuing a Token only to Individual Users that have been provisioned by the duly authorized and responsible User Authority for each such Individual User and for revoking the Token of each such Individual User upon their de-provisioning by their respective User Authority. An IdP is responsible for the Existing Commercial Relationship as well as each User Authority to which it issues Individual User Credentials and Tokens and each Relying Party that accepts any such Credential and Token.
An Identity Provider may delegate services to one or more Identity Provider Proxies as long as the Authenticating Identity Provider and all Identity Provider Proxies have a Certified Service and the Relying Party is made aware of the specific details of the Delegation in the Underlying Commercial Contract or as otherwise specified by the Participants.

Certified Services: An IdP may have one or more active Certified Services that have been certified by an ID Federation-identified Assessor under the Trust Framework Certification Policy that is hereby incorporated by reference into this Trust Framework and is attached hereto at Appendix A.

1.01(b)(ii) Relying Party

A Relying Party (RP) is a Participant that accepts and relies upon a Token of an Individual User that has been issued by an IdP, and received for the purpose of asserting and Authenticating the identity of the Individual User. The RP is responsible for determining for itself whether to accept any given Token and determining the extent to which reliance upon any Token is reasonable, and to determine whether, how or the extent to which a given Individual User may be authorized to conduct a transaction or other interaction with the RP. An RP is responsible for the Existing Commercial Relationship with each IdP issuing Tokens accepted by that RP. An RP is also responsible for the Existing Commercial Relationship with each User Authority for any Individual User whose Tokens that RP accepts.

Certified Services: ID Federation members will not require a Certified Service to perform the role of Relying Party but an RP may have one or more active Certified Services if the RP acts as an Identity Provider.

1.01(b)(iii) User Authority

A User Authority (UA) is a Participant with authority and responsibility to identify, enumerate and manage the Individual Users within its business. Individual Users within a User Authority's business may include employees, contractors and others. The User Authority is responsible for requesting provisioning, managing access to, and de-provisioning the ID Credentials and Tokens of Individual Users within its business. A User Authority is responsible for the Existing Commercial Relationship with an IdP that issues a Token to any Individual User within its business. A User Authority is responsible for determining the Existing Commercial Relationship with each RP that accepts and relies upon a Token issued to any Individual User within its business.

1.01(b)(iv) Policy Authority

The Board of Directors, sometimes referred to herein as the Policy Authority (PA), promulgates this Trust Framework and is responsible for amending the Trust Framework, as well as for the strategic, organic and other material decision-making activities operating under the Trust Framework, including approval of the requirements for Certified Services.

1.01(b)(v) Federation Operator

The Federation Operator is responsible for day-to-day-operations of the ID Federation, including the provision of business services such as "first-point-of-contact" telephone and email communications for the ID Federation, the Onboarding of new Participants, and maintaining current records in the Participant Directory.

1.01(b)(vi) Assessor

An Assessor is a third party who is responsible for certifying the service of an applicant based on a neutral and independent assessment and testing as determined by the Policy Authority from time to time.

1.02 Communications and Policies

1.02(a) Official Communication

Official communications by the ID Federation may only be made or approved by the Policy Authority, or a Party that has been expressly authorized by the Policy Authority to make such communications. The ID Federation is not responsible for any unauthorized communications including unauthorized use of the Trust Mark.

Published materials may be accessible through the ID Federation website or other means designated or approved by the Policy Authority from time to time. Any materials that are not freely available to the public (including those behind website logon, password-protected or explicitly labeled) may not be shared or distributed publicly.

1.02(b) Formal Policies and Official Document

The Policy Authority, or its designees, shall promulgate and amend Formal Policies and Official Documents from time to time and ensure the current version of each such document is available at the ID Federation website. When the text of this Trust Framework explicitly refers to a Formal Policy and/or Official Document as "incorporated by reference," then the content of that policy or other document shall have the same force and effect as if directly published within this Trust Framework.

1.03 Participation in the ID Federation

The following Rules apply to Participation in the ID Federation.

1.03(a) Eligibility

In order to be a Participant in the ID Federation, a Party must:

- Be involved in the provision of, sale, distribution, licensing, or use of a financial or insurance-related product or service;
- Meet or exceed the applicable requirements of the Trust Framework, including for Certified Services (when applicable);
- Execute the Participation Agreement, indicating the Role(s) it will conduct as defined in this Trust Framework;
- Have or intend to have an Existing Commercial Relationship with one or more other Participants; and
- Remain in compliance with all applicable Rules of the Trust Framework, including payment of applicable fees.

1.03(b) Continued Compliance

Every Party shall remain in compliance with the current Rules of this Trust Framework for so long as the Party is a Participant in the ID Federation. Every Party must review the ID Federation website or other means designated or approved by the Policy Authority from time to time for updates to the Trust Framework, including without limitation the Formal Policies, Official Documents, or Rules.

1.04 Termination and Suspension

All rights and obligations of a Participant under the Trust Framework cease upon termination or suspension, subject to provisions of Section 2.11. The ID Federation may terminate this Trust Framework, with respect to all Members, for any reason and at any time with advance notice to each Member. Upon termination or suspension, fees paid relative to Participation, including any related to

Assessment for a Certified Service, will not be reimbursed. Notwithstanding the foregoing, the ID Federation shall return any available funds on a pro rata basis to Members (based on the fees paid by each Member) in the event that the ID Federation terminates the Trust Framework as to all Members.

1.04(a) Voluntary Termination

Any Party may voluntarily terminate its Participation in the ID Federation for any reason by written notice to the Federation Operator. Information about a terminated Participant shall be removed from the Participant Directory, including information about any Certified Service of the Participant. Members of the ID Federation shall be given notice of the termination of the Party's Participation in the ID Federation, which may be by mail, email, or general notice to all Participants.

1.04(b) Involuntary Suspension and Termination

If, for any reason, the Federation Operator and/or the Policy Authority become aware or reasonably suspect that a Participant is violating the Rules of this Trust Framework, it may request that an executive level employee of the Participant be available for resolution of the matter. A Participant shall reasonably participate in such discussions. If, upon discussion of the matter, there is good cause to believe that a Participant is in violation of the Rules of this Trust Framework, the following consequences may be pursued.

1.04(b)(i) Warning

The Policy Authority or the Federation Operator may provide a warning to a Participant for violation of the Rules of this Trust Framework. Warnings shall include a description of the violation, a description of the corrective action or actions sought, and a time frame within which to cure the violations.

1.04(b)(ii) Audit

In the event the Policy Authority believes the discussions described in Section 1.04(b) have not resulted in resolution of the violation of the Rules of this Trust Framework by a Participant within the time frame to cure noted in the warning, and the Participant that has been warned asserts it is in fact in compliance, then the Policy Authority may request that the Participant's President, CEO, COO, or senior employee of the Participant who is directly involved with the ID Federation be reasonably available for purposes of resolving the matter. The Participant may present evidence in its discretion in support of its compliance with the Trust Framework.

1.04(b)(iii) Suspension

The Policy Authority may suspend a Participant for violation of the Rules of this Trust Framework. As determined by the Policy Authority, a notice of suspension may be effective immediately–in the case of a serious violation threatening the security of the ID Federation or the rights or property of any Participant in the ID Federation (in the sole discretion of the Policy Authority)-or the suspension may be effective after a notice period and an opportunity to cure. A notice of suspension shall be delivered in writing by the Federation Operator to the business and technical contacts identified by the Participant. The notice of suspension shall include a description of the violation, a description of the corrective action or actions sought, and a time frame within which to cure the violations. During the suspension term, the Participant shall be removed from the Participant Directory, including information about any Certified Service of the Participant. Members of the ID Federation shall be given notice of the suspension of the Party's Participation in the ID Federation. Any suspension longer than one (1) year shall be considered an involuntary termination. A suspension may also become an involuntary termination if corrective action does not take place within the time frame required in the notice of suspension. In

either instance, the Policy Authority may involuntarily terminate the Participant with thirty (30) days written notice.

1.04(b)(iv) Involuntary Termination

The Policy Authority may cause a Participant to be involuntarily terminated for serious violation of the Rules of this Trust Framework (in the sole discretion of the Policy Authority). A notice of involuntary termination may be effective immediately, in the case of a serious violation threatening the security of the ID Federation or the rights or property of any Participant in the ID Federation (in the sole discretion of the Policy Authority), or the involuntary termination may be effective after a notice period and an opportunity to cure. A notice of termination shall be delivered in writing by the Policy Authority to the Business and Technical Contacts for the Participant. The notice of termination shall include a description of the violation and, if applicable, a description of the corrective action or actions sought and a time frame within which to cure the violations. Information about an involuntarily terminated Participant shall be removed from the Participant Directory, including information about any Certified Service of the Participant. Members of the ID Federation shall be given notice of the termination of the Party's Participation in the ID Federation.

1.04(c) Reinstatement

Any suspended or terminated Participant may be reinstated as an active Participant of the ID Federation. Reinstatement of an involuntarily terminated Participant shall require approval by the Policy Authority upon determination that the circumstances giving rise to the suspension or termination have been resolved. A Party undergoing reinstatement from suspension or termination must successfully complete any actions reasonably requested by the Policy Authority.

1.04(d) No Liability for Suspension or Termination

Each Member acknowledges and agrees that the Policy Authority has the right to make suspension and termination determinations, and any related determination, as described herein in its discretion and in no event will a Participant hold the Policy Authority, or any individual member, employee, contractor or agent of the Policy Authority or any other Participant liable for any such determination.

1.05 Business Practices and Operations

1.05(a) Personnel Practices

1.05(a)(i) Provisioning, Maintenance and Modification of Individual User Accounts

A User Authority requesting provision of a new Individual User account must ensure that the identity data used for that user is accurate and is appropriately updated as needed.

1.05(a)(ii) Termination and De-Provisioning User Accounts

It is the duty of a User Authority to promptly de-provision any Individual User for which the User Authority is responsible within twenty-four (24) hours of the cause of de-provision. Cause for de-provision includes, without limitation, termination of employment with the User Authority, change of job function or any other change in status so that the Individual User is no longer authorized to use the Token.

1.05(b) Training

Each Participant shall educate and train its internal staff regarding each applicable Rule of this Trust Framework, including relevant business practices, legal procedures and technology processes. This Trust Framework and all relevant Formal Policies are accessible from the ID Federation website.

1.06 Use and Management of Trust Mark

The Policy Authority shall designate an ID Federation Membership Trust Mark and an ID Federation Certification Trust Mark. The rights, obligations and licensing terms applicable to said marks shall be detailed in the ID Federation Trust Mark Policy that is hereby incorporated by reference into this Trust Framework and is attached hereto at Appendix B. No Participant may use or display an ID Federation Trust Mark in association with an assessment or otherwise use or display the Trust Mark associated with any service, product, literature, or other information unless such use has been approved by the Federation Operator subject to the ID Federation Trust Mark Policy.

Article 2: Legal

2.01 Participation Legal Criteria

Each Participant in the ID Federation must execute the Participation Agreement, indicating the respective Role or Roles applicable to that Participant. Each Participant shall pay the applicable fees. In no event will the ID Federation be responsible for refunding any fees paid.

2.02 Liability

2.02(a) Liability Between Participants

The relevant provisions of any Existing Commercial Contract between Participants, that governs the activities and subject matter contemplated herein, shall first and foremost govern the relationship of and liability between those Participants in the ID Federation. In the event of a conflict between the terms of the aforementioned Existing Commercial Contract and the relevant provisions of this Trust Framework, including the Participation Agreement, the Existing Commercial Contract shall govern. In the event that there is no Existing Commercial Contract between relevant Participants, or if such an Existing Commercial Contract does exist but does not address the activities and subject matter contemplated under this Trust Framework, then the provisions of the Trust Framework shall govern.

2.02(a)(i) Disclaimers

ANY SPECIFICATION PROVIDED BY THE ID FEDERATION UNDER THIS TRUST FRAMEWORK AND ANY SERVICES PROVIDED BY THE ID FEDERATION ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION IN WHOLE OR IN ANY PART SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER ID FEDERATION, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION. THE ID FEDERATION EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, AND ALL OBLIGATIONS OR LIABILITIES FOR DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIRD PARTY SERVICES, WHETHER OR NOT RECOMMENDED BY, REFERRED BY, OR PROVIDED THROUGH THE ID FEDERATION, INCLUDING BUT NOT LIMITED TO THE SERVICES OF THE ASSESSOR.

2.02(a)(ii) Limitation of Liability

As between Participants, each Participant shall be responsible for harm caused by its own acts and omissions and not for the acts or omissions of any other Participant, and each Participant shall be responsible for such harm to the extent that it was caused by the Participant's breach of the provisions of the Trust Framework arising out of its negligent conduct or willful misconduct.

2.02(a)(iii) Limitation of Damages

In no event will the ID Federation or a Participant be liable for any consequential, indirect, incidental, punitive, special, or exemplary damages, including, without limitation, damages for lost profits, business interruption or loss of data incurred by another Participant as result of any activity undertaken pursuant to this Trust Framework, even if the ID Federation or the Participant has been advised of the possibility of such damages.

In no event will the ID Federation or a Participant be liable for any direct damages hereunder, except, in the case of a Participant, for damages to the extent caused by the Participant's breach of the provisions of the Trust Framework arising out of its negligent conduct or willful misconduct.

In no event will a Participant with a Certified Service have an entire cumulative liability for any direct liabilities, losses, claims, judgments, damages, expenses, or costs arising out of this Trust Framework — whether sounding in contract, tort or otherwise — that exceeds the greater of: (i) an amount equal to three (3) times the amount of the annual fee paid by such Participant pursuant to the Trust Framework during any consecutive twelve (12) month period; or (ii) $500,000.00, whichever is greater.

2.02(b) Liability Between Participants and Non-Participants

These Rules are made solely and specifically among and for the benefit of Participants. No person who is not a Participant shall have any rights, interest or claims under these Rules or be entitled to any benefits under or on account of these Rules, whether as a third party beneficiary or otherwise. There shall be no liability by a Participant to a person who is a not a Participant.

2.03 Antitrust Policy

The Antitrust Policy is hereby incorporated by reference into this Trust Framework and is attached hereto at Appendix C.

2.04 Intellectual Property

2.04(a) Intellectual Property Rights Policy

The Intellectual Property Rights Policy is hereby incorporated by reference into this Trust Framework and is attached hereto at Appendix D.

2.04(b) Copyright and Restricted Access

The copyright for the Trust Framework, including without limitation the Formal Policies, Official Documents, or Rules shall belong to the ID Federation.

Any materials published without access restrictions and publicly available on the ID Federation website shall be made available pursuant to the Terms of Use on the ID Federation website.

Any materials published with access restrictions on the ID Federation website shall be subject to the additional restrictions in Section 2.07.

2.05 Dispute Resolution

2.05(a) Disputes Between Participants

2.05(a)(i) Negotiation

In the event of any dispute, claim, question, or disagreement arising from or relating to these Rules or the breach thereof, the relevant Participants shall use their best efforts to settle the dispute, claim, question, or disagreement. To this effect, they shall consult and negotiate with each other in good faith and, recognizing their mutual interests, attempt to reach a just and equitable solution satisfactory to both parties.

2.05(a)(ii) Mediation

If a dispute arises out of or relates to these Rules, or the breach thereof, and if the dispute cannot be settled through negotiation, the parties agree first to try in good faith to settle the dispute by mediation administered by the American Arbitration Association under its Commercial Mediation Procedures before resorting to arbitration, litigation, or some other dispute resolution procedure (as permitted by this Trust Framework).

2.05(a)(iii) Arbitration

If Participants do not reach a resolution of the dispute by mediation within a period of sixty (60) days, then, upon notice by either Party to the other, all disputes, claims, questions, or differences shall be finally settled by arbitration administered by arbitration. Any controversy or claim arising out of or relating to these Rules, or the breach thereof, shall be settled by arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules (including the Optional Rules for Emergency Measures of Protection), and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

2.05(a)(iv) Intellectual Property Disputes

Notwithstanding the foregoing, any controversy or claim arising out of or relating to these Rules, or the breach thereof involving intellectual property rights shall not be subject to arbitration.

2.06 Governing Law

This Trust Framework, including any directly included or incorporated by reference Formal Policy, Official Document, Agreement, Requirement or other Rule, shall be governed by and interpreted in accordance with the laws of Delaware, and exclusive venue for any and all disputes under law or jurisprudence hereunder, including mediation or arbitration, shall lie in the state or federal courts located in the State of Delaware.

2.07 Confidentiality

Nothing in this Trust Framework requires confidentiality other than the following:

- Any information provided as part of the Certification process or Certified Services that is mutually agreed by the applicant and the Federation Operator and/or the Policy Authority to be confidential;
- Information that is sensitive, proprietary, mission critical, high value or otherwise may pose a security risk to the ID Federation and is designated as Confidential by the Federation Operator and/or the Policy Authority; or
- By application of Section 2.9 of this Trust Framework, the terms of any Existing Commercial Contract, including the terms of any Non-Disclosure Agreement or other terms related to confidentiality or trade secrets shall continue to govern.

Nothing in this Trust Framework is intended to affect the obligations of the Parties under Existing Commercial Contracts.

2.08 Incorporation of Documents

In order to be incorporated into this Trust Framework, the Trust Framework must incorporate a specific named document or the document must explicitly state that it is incorporated into the Trust Framework.

2.09 Order of Precedence

In the event of a conflict between any Existing Commercial Contract, on the one hand, and this Trust Framework, including the Participation Agreement, on the other, the Existing Commercial Contract shall govern in all respects. In the event of a conflict between the Participation Agreement and this Trust Framework then the terms of the Participation Agreement shall govern.

2.10 Amendment

This Trust Framework, including all Policies incorporated by reference, may be amended by the Board of Directors from time to time in accordance with the Trust Framework Amendment and Change Management Policy, which is hereby incorporated by reference and is attached hereto at Appendix E.

2.11 Survival

The following obligations shall survive termination or suspension: 1.04, 1.04(d), 1.06, 2.01, 2.02 (including all subparts), 2.04 (including all subparts), 2.05 (including all subparts), 2.06, 2.07, 2.08, 2.09, 2.11, and 2.12. The following obligations shall additionally survive suspension: 1.04(c).

2.12 Notice

All notices that are required or may be given pursuant to the Trust Framework must be in writing and shall be deemed duly given or made as of the date delivered personally, sent by a recognized courier service, sent by a recognized overnight delivery service, sent by facsimile or email (but only if followed by transmittal by a recognized courier service, by a recognized overnight delivery service or delivered in hand for delivery within three (3) business days) or sent by registered or certified mail, postage prepaid, to the parties at the following addresses (or to the attention of such other Person or such other address as any Party may provide to the other Party by notice in accordance with this section.

2.13 Assignment

The ID Federation may assign this Trust Framework in accordance with the Bylaws.

2.14 Definitions

All capitalized terms shall have the definition assigned in the Glossary, which is attached hereto at Appendix F.

Article 3: Technical

3.01 Use Cases

3.01(a) Technical Scope

The technical scope is defined by the Use Cases that are contained in the Appendices to this Trust Framework and application of the standards, specifications and configurations described in this Article 3. Unless otherwise noted, the provisions within Article 3 apply to Parties acting in the Role of an IdP and/or an RP.

3.01(b) Technology and Use Case Change Management

Use Cases may be active or pending. The process for proposing a Use Case, and establishing when a Use Case is actively supported within the then current scope of the ID Federation or when it is agreed to become actively supported pending a future sunrise date is specified in the Trust Framework Amendment and Change Management Policy. Use Cases that are active and pending are included within the Trust Framework, with their respective status so noted, including any applicable sunrise dates.

3.01(c) Technical Use Cases

The active and pending Use Cases are fully detailed in the ID Federation Use Cases Specification, which is hereby incorporated by reference into this Trust Framework and are attached hereto at Appendix G.

3.02 Standards Conformance (IdP & RP)

IdPs and RPs must conform to at least one of the following standards. (Links regarding these standards may be found on the ID Federation website.)

3.02(a) Standards

The identity standards used by ID Federation Participants are Security Assertion Markup Language (SAML) and Open ID Connect (OIDC)

3.02(a)(i) Security Assertion Markup Language (SAML)

SAML is an XML-based open standard for exchanging Authentication and Authorization data between an IdP and an RP. SAML was developed by the Security Services Technical Committee of OASIS (Organization for the Advancement of Structured Information Standards), and is available at https://www.oasis-open-org/committees/tc_home.php?wg_abbrev=security.

3.02(a)(ii) Open ID Connect (OIDC)

OIDC is a simple identity layer on top of Oauth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorized server, as well as to obtain basic profile information about the end-user in an interoperable and RESTlike manner. In technical terms, OpenID Conect specifies a RESTful HTTP API, using JSON as a data format. See OpenID Foundation (OIDF) for details.

3.02(b) Profiles

A profile defines a set of rules and constraints for a standard in order to facilitate the usage of that standard for common Use Cases. The high-level Use Cases in Section 3.01(c) are supported by the following common profiles.

3.02(b)(i) SAML

Web Browser SSO Profile

3.02(c) Attributes

Participation enables identity attribute sharing across Participant security domains to facilitate access to resources. Participants in the IdP Role are expected to provide authoritative and accurate attribute assertions to other Participants. Attributes are mutually agreed upon between each IdP and RP pair. ID Federation does not require specific attribute values, but it does require at least one attribute that is a unique identifier for the user responsible for a given transaction and at least one attribute that is a unique identifier for the organization or entity responsible for a given transaction. Relying Parties receiving attribute assertions from IdPs may choose to ignore those assertions not required to provide access.

3.02(c)(i) Minimally Recommended Unique Identifier Attributes

Email Address: If used, the email address must be valid. This is a globally unique value and is typically linked to other security controls outside of the Trust Framework, for example: first.last@somedomain.com.

Organization Identifier: The Federation Operator maintains a list of all Participants in the Participant Directory.

3.02(c)(ii) Optional Attributes

Optional attributes are allowed and must be mutually agreed upon between Participants. Examples of optional attributes are:

Given Name;
Surname;
Organization Name – this is the name of the Participating organization a person is affiliated with as mutually agreed upon between IdP and RP;
Any additional attributes which are deemed relevant between the two federating parties

GUID. Globally Unique Identifier used to identify information in computer systems. GUID can be used in addition to email address to uniquely identify a user. One scenario would be if a user's email address changes – sale of agency, name change, etc., the Relying Party could use GUID as a secondary key to match on for access to their systems. GUID's would be generated by the Identity Provider when the user is initially created

3.02(c)(iii) Attribute Uniqueness

Attributes are required to be assigned names in the form of a URL. This is to ensure uniqueness. For example: Attribute Name identifies an attribute called 'name' qualified by a namespace in the form of a URL. This is a predefined attribute type defined by Microsoft. If Participants require a 'name' attribute

with different semantics, something like this could be used: Attribute Name. See the appropriate standards for SAML and OIDC attribute naming requirements.

3.02(c)(iv) Multi Factor Authentication (MFA) Attributes

The following three attributes will be added to indicate the use of MFA, or absence of MFA, in the authentication procedure.

Attribute	Description	Value	
mfatype	MFA Type from IETF definitions*	String from IETF List in Appendix H	Required
mfasource	Name of MFA Vendor or Provider	Text	Optional
assurancelevel	NIST Assurance Level**	String from Assurance Level List in Appendix H	Required

* Internet Engineering Task Force (IETF) Authentication Method Reference Values
https://www.rfc-editor.org/rfc/rfc8176

**Assurance Levels from "NIST Special Publication 800-63B - Digital Identity Guidelines"
https://pages.nist.gov/800-63-3/sp800-63b.html#multifactorOTP

3.02(d)(i) De-Provisioning

When a user leaves an agency, a message will be sent to partner Relying Partied to remove the user from their system. The SCIM (System for Cross-Domain Identity Management) standard is used to automate the exchange of identity information between identity domains, and it will be used for this operation within the ID Federation Trust Framework. SCIM was released and is maintained by IEFT (Internet Engineering Task Force) and supports a number of identity management operations. Initially for ID Federation, the POST operation will be used to notify the Relying Party to remove the user. Below is a sample of the message:

POST https://system.carrier.com/soo/v1/user/<username>

"soo" to specify the interface is for use by the SignOn Once framework
v1 – would indicate which version of the framework to enforce
user – the resource type to manage (allows for flexibility should the framework be charged to expand to manage groups/roles/entitlements)
<username> - the federated ID (email) or an immutable ID for the resource (group, role, etc) to be managed by the request

Body of the request would include a JSON message such as

{action ; deprovision }

3.02(d)(ii) Provisioning

For future use

3.03 Technology Requirements for IdPs and RPs

Pre-requisites for Participation by an IdP or RP in the ID Federation:

IdPs must be able to generate digitally signed SAML or OIDC Tokens; RPs must be able to consume digitally signed SAML or OIDC Tokens; A PKI based certificate from a trusted public Certificate Authority;
Ability to create a connection end point;
Consume Metadata from federation partner including information on the federation end-point;
Establish secure transport layer to communicate (HTTPS);
Any additional attributes beyond what is specified in Section 3.02(c)(i) and (ii) are considered custom attributes and must be agreed upon between IdP and RP

3.03(a) Establishing Initial ID Federation Relationship Between IdPs and RPs

Once the pre-requisites are met, an IdP and an RP exchange Metadata to configure their respective technology products to participate in the federation.

3.03(a)(i) Metadata Exchange

After legal and business agreements are established, Participants in the ID Federation can exchange Metadata. Metadata can be exchanged dynamically via a link or out of band.

3.03(a)(ii) Time Synchronization

All Participants must implement an agreed upon level of time synchronization on all infrastructure providing IdP or RP services. Time synchronization is required to ensure that timeouts and expirations can be applied correctly across multiple systems and eliminate the risk of time drift generating connectivity issues. Clock synchronization is critical for ID Federation to be successful. It is recommended that partners participating in federation use a standard time sync tool, such as NTP pool or any central service the federation partners are signed up with. It is recommended the degree of tolerance should not exceed Stratum 3.

3.04 Security Requirements (IdP & RP)

This section includes the security requirements applicable to the ID Federation.

3.04(a) User IDs and Passwords

All Participants of the Trust Framework that will act as an IdP will adhere to the standard requirements for the implementation and administration of User IDs and passwords. The requirements were selected to meet regulatory and compliance guidelines as well as Information Security best practices. In addition, any entity providing a service or storing data on behalf of the Trust Framework must adhere to the requirements. A Participant may implement stricter security measures but is required to meet or exceed the requirements defined below to participate as a Trusted Partner. The following section is based upon NIST recommendations.

3.04(a)(i) User ID

User ID naming convention (applies to Trust Framework entity only)
Access privilege removal for inactive, suspended, and terminated User IDs by the IdP
An IdP must have a process to ensure credentials will never be sent to an RP where the User's ID is suspended, terminated, or revoked

3.04(a)(ii) Password

Password protected at rest
Hashed using SHA-256 or higher; or
Encrypted with AES algorithm with minimum 128-bit key

Passwords protected in motion (one of the following)
Hash or encrypt the password (using a seed to prevent replay), using algorithm/keylength requirements the same as passwords at rest;
Encrypt the channel using TLS as defined above

Password strength standards
Must be seven (7) or more characters in length; Must contain at least three of the following:
Uppercase letter; Lower case letter;
Number;
Special character

Password Expiration

Password must expire every sixty (60) days

Lock out after failed Authentication attempts
Account must lock after five (5) invalid login attempts;
No automated unlock permitted;
A standard process must be in place to manage password resets executed by a system administrator or delegated administrator

Password Reset and Changes
A user must provide their current password or answer a preselected security question to change or reset their password;
A standard process must be in place to manage password resets executed by a system administrator or delegated administrator

Password Reuse
A password history must be maintained and none of the previous twelve (12) passwords may be selected for reuse;
A new password may not be changed again for forty-eight (48) hours in prevention of password recycling

3.04(b) Certificate

One of the primary tools aimed at ensuring confidentiality, integrity, and availability will be the utilization of a Public Key Infrastructure. This approach requires a pre-existing relationship between Participants

and the utilization of digital signatures from a reputable Certificate Authority. It is at the discretion of each Participant whether to accept digital certificates from an individual Certificate Authority.

3.04(b)(i) Certificate Authority

While the ID Federation does not endorse any particular Certificate Authorities, acceptable Certificate Authorities must be agreed to by the integrating Participants for each implementation.

3.04(b)(ii) Certificate Expiration

Certificate will be issued for no longer than one (1) year.

3.04(b)(iii) Certificate Management
Each organization must obtain its own certificates. Certificates are validated on use to meet date, name, issuer and revocation requirements.

3.04(c) Delegation

Delegation by Identity Provider Proxies is permitted in the Trust Framework to the restrictions set forth in Section 1.01(b)(1).

3.04(d) Logging and Monitoring

All IdPs and RPs are required to deploy appropriate logging mechanisms for the purpose of providing audit, traceability, troubleshooting and threat identification of identity-related activities, including but not limited to the success or failure of Authentication events.

All IdPs and RPs are required to deploy appropriate log monitoring and alerting mechanisms for the purpose of identifying and responding to potential threats and attacks. The term of retention for logging shall be agreed upon between IdP and RP.

3.04(e) General Enterprise Security Controls

Creating a secure environment is foundational to business relationships and is not limited to federated transactions. The requirements within Section 3.04 above speak to those which are directly related to federation. Numerous other security measures will be taken into consideration with any implementation between two external entities, including without limitation the following:

Enterprise-WideSecurityControls
Risk management program, including vulnerability management;
Security & compliance management;
Human resources security;
Third party relationships;
Offshore security (i.e. outside the U.S.);
Physical security;
Access control for internal users;
Password policy for internal users; Data
security;
Remote access security;
Change management;
Operations management: network monitoring & capacity management; Anti-malware;
Logging;
Business continuity management (BCP and DR)

SecureDevelopment
Valid software development life cycle (SDLC) process; Inclusion of the OWASP Top 10 in testing, examples:
- Session management;
- Input validation;
- Cross-site attacks;
- Error handling

SecurityTesting Penetration testing; Vulnerability scanning; Remediation and mitigation ProductionIsolation
Production and non-production system isolation; Carrier separation

IncidentHandling
Incident response plan, including breach response

PlatformVulnerabilityManagement Operating System (OS) patching;
Configuration management;
Vulnerability scanning

3.05 Central Services

3.05(a) Introduction

The Policy Authority supports the provision of certain central services by the Federation Operator that aid in the implementation of federated technology. In addition to the information laid out in this documentation, additional services will be provided to those Members of this organization. Details for these services are provided below.

3.05(b) Participant Directory

A Participant Directory will house Participant data which will be accessible by ID Federation Participants.

3.05(b)(i) Contents

Minimally, the contents of the Participant Directory will contain the following information fields (some of which are only applicable to certain Role(s):

	Data Attribute	IdP	RP	Liaison
IDFI	IDFI Role	•	•	•
	IDFI URI	•	•	•
	IDFI Organization Name	•	•	•

	Membership Agreement	•	•	•
	Dues	•	•	•
Organization	Organization Name	•	•	•
	Organization HQ Location	•	•	•

	Data Attribute	**IdP**	**RP**	**Liaison**
	Contact Info	•	•	•
Technical Certification	Participation Agreement	•	•	•
	Assessment Completion	•	N/A	N/A
	Certification Result	•	N/A	N/A
	Section 3.04 Rules	•	•	N/A
	Federation Standard and Version (SAML, OIDC)	•	•	N/A
	Endpoint URL(s) per App	Optional	•	N/A
	Server Certificates (and Certificate Authority)	•	•	N/A
	Attribute List	•	•	N/A
	Sample XML	•	•	N/A

3.05(b)(ii) Modifying & Notifications

The information contained within the Participant Directory must be kept current. It is the sole responsibility of the Participants to provide current and accurate information. The ID Federation assumes no responsibility for its accuracy and relevance. The server certificates have expiration dates and must be properly updated beyond the initial federation set up. It is the responsibility of each Participant to notify other Participants, as relevant, of updated information.

3.05(b)(iii) Removal

When a Participant is terminated in accordance with Section 1.04, the data they have provided will be inactivated for a period of six (6) months, and after which, it will be purged.

Article 4: Appendices

The Appendices set forth below are attached hereto and incorporated herein. Appendices may be changed from time to time by the Policy Authority as permitted hereunder or pursuant to the Change Management procedure set forth in the Trust Framework. Any changes will be posted on the ID Federation Website. Regardless of whether or not a notice of change has been sent out to all Participants, the Participants shall have the obligation of complying with any changes.

Appendix A: Certification Policy

Appendix A

Certification Policy

Defined terms used in this document will have the meanings provided in this document or in the Trust Framework Glossary.

1. Introduction

This policy describes the processes and rules governing certification by the ID Federation of Certified Services provided by Identity Providers.[1]

2. General Meaning of Certified Services

Certification means that the Assessor has established that the Participant's service has met the Security Requirements by one of the methods described in Section 5 of this document. In order to have a Certified Service, the following conditions must be met:

(i) The entity seeking certification represents that it is complying with the Technical Requirements and the Security Requirements set forth in the Trust Framework;

(ii) The entity is a Member in good standing of the ID Federation; and

(iii) The certification has been approved by the Board of Directors.

3. Certification Process

An Identity Provider may have one or more Certified Services. Certification shall be conducted by an Assessor. The Identity Provider and the Assessor shall enter into a Certification Agreement containing specific terms and conditions for certification and the applicable fee for certification.

4. Requirements for Certification

The Identity Provider seeking certification for a service must meet the following requirements at the time of application:

(i) The Identity Provider must have signed a Participation Agreement that has been accepted by the ID Federation; and

(ii) The Identity Provider must be a member in good standing.

---

[1] Identity Providers are certified by the ID Federation and are granted the right to use the ID Federation Certification Trust Mark with the word "Certified IdP" after the mark. Relying Parties are not certified, and they are granted the right to use the ID Federation Membership Trust Mark without the "Certified IdP" designation.

5. Methods for Certification

An entity seeking certification of a service may utilize one of the three methods described below to establish that the certifying service adheres to the security requirements defined in the Trust Framework:

(i) The Identity Provider must complete the Trust Framework Security Assessment which is then reviewed by the Assessor. The Trust Framework Security Assessment is a survey based on the ISO 27001 standards and BITS shared assessment standards that evaluate the general security posture and security controls pertaining to ID federation implementation.

(ii) The Identity Provider must provide an ISO 27001 Certification specific to the processing location for the service.

(iii) The Identity Provider must provide a SOC 2 Type 2 Report specific to the processing location for the service that covers confidentiality, integrity, availability, and security.

6. Assessment Report

The Assessor shall provide a report to the Identity Provider indicating that the Identity Provider has met the requirements for certification or including a list of the issues that must be resolved in order to meet the requirements for certification. If the Identity Provider has met the requirements for certification, the Identity Provider may direct the Assessor to provide the report to the ID Federation Board of Directors. If the Identity Provider has not met the requirements for certification, the Identity Provider shall have the opportunity to resolve any issues within a one (1) year period following receipt of the report. In such event, additional fees may be required by the Assessor to complete certification.

7. Certification Decision

The ID Federation Board of Directors shall review and evaluate the Assessment Report and any other relevant information in making the final decision on certification of a service. The Board of Directors may include stipulations in its granting of certifications.

8. Requirements for Re-Certification

Identity Providers will be re-certified every three years based on the same methods as defined in section 5 of the certification policy.

This Certification Policy may be revised from time to time by the ID Federation Board of Directors. The Participant must review the ID Federation website or other means designated or approved by the Policy Authority from time to time for updates to the certification policy.

Appendix B

ID Federation Trust Mark Policy

1.0 Certification Trust Mark
The Certification Trust Mark, for use by authorized Participants, is intended to certify that the Participant has met specified standards allowing the Participant's participation in a trusted network of digital communications.

1.1 Certification Trust Mark Restrictions
In addition to the General Trust Mark restrictions identified in Section 3.0 below, the following restrictions apply to the use of the Certification Trust Mark:

1.1(a) The Certification Trust Mark may only be used to identify Certified Services.

1.1(b) Participants may not represent any service as being certified, conformant, or compliant, or use those terms in connection with any advertising unless and until the service is a Certified Service.

1.1(c) Use of the Certification Trust Mark is permitted only for so long as the Certified Service continues to comply with the standards under which certification was granted (as may be amended from time to time). In the event a Participant is terminated or suspended, all use of the Trust Mark must immediately cease and be removed from existing materials and online content until and unless the Participant is restored to active status.

2.0 Membership Trust Mark
The Membership Trust Mark, for use by Members and Participants, is intended to identify a Party’s participation or membership in the ID Federation.

2.1 Membership Trust Mark Restrictions
In addition to the General Trust Mark restrictions identified in Section 3.0 below, the following restrictions apply to the use of the Membership Trust Mark:

2.1(a) The Membership Trust Mark may only be used by current Participants and Members.

2.1(b) Use of the Membership Trust Mark is permitted only for so long as the Participant or Member continues to remain as a Participant or Member in good standing of the ID Federation. In the event a Participant is terminated or suspended, all use of the Trust Mark must immediately cease and be removed from existing materials and online content until and unless the Participant is restored to active status.

3.0 General Trust Mark Guidelines
All Trust Mark reproductions must be made pursuant to the general restrictions on use and appearance (height, spacing, and color). Refer to the Logo Style Guide on the ID Federation website.

Appendix C

Antitrust Policy

Those participating in ID Federation activities of any type should be aware of the need to exercise caution to avoid inadvertent violations of EU, international, national or state/province antitrust and anticompetitive laws. Violations of such laws can result in severe civil penalties (and in some jurisdictions, criminal penalties) for individuals as well as their employers.

Laws relating to antitrust and anticompetitive behavior can be quite complex, and differ from jurisdiction to jurisdiction. Consequently, it is not possible to summarize them in this policy, and you should therefore consult appropriate advisors at your own company for detailed guidance.

The following rules shall apply in connection with all ID Federation meetings, activities, and other forms of participation:

1. Agendas must be created, and minutes must be taken, for all ID Federation meetings. These agendas and minutes must then be submitted to ID Federation, along with any meeting materials, to document the topics discussed and any agreements reached.

2. Certain topics should never be discussed at, or in connection with, any ID Federation meeting or other ID Federation activity, nor should you ever form an agreement with any other ID Federation Member or any one else in connection with these topics. In particular, ***DO NOT at any time discuss, or agree upon:***

- Your current or future prices, or any strategies relating to pricing
- Any increase or decrease in prices, or other terms (e.g., discounts) relating to prices
- Your market shares or those of others
- Levels of investment or development, or changes to such levels Your
- current or future design or marketing strategies.
- How much or little you are capable of producing or will sell of any product or service
- Whether you have submitted a bid, or will or will not bid, in any given situation
- Where each of you will or will not sell any product or service
- Whether you will or will not deal with any third party

3. Do not disclose or discuss at or in connection with any ID Federation meeting or activity any terms upon which you will make any of your intellectual property rights available, except to the extent permitted or required under the ID Federation IPR Policy.

If at any time you become aware of any activity that may be in violation of any of the above rules, please bring them promptly to the attention of an ID Federation representative.

REMEMBER: All ID Federation activities must serve to promote, rather than restrict, competition to the benefit of consumers and the marketplace. Activities that do otherwise, or even appear to have the potential to do otherwise, may have serious consequences.

Appendix D

Intellectual Property Rights Policy

1. **Purpose.** The purpose of this Intellectual Property Rights Policy ("**Policy**") is to minimize the possibility of inadvertent infringement of the IPR of Members and third parties by using or implementing any ID Federation Specifications.
2. **Applicability.** All Members, representatives of Members, and third parties attending any technical meeting are subject to this Policy.
3. **Intellectual Property Rights.**
   3.1. **Patent Covenant.** Each Member agrees and covenants not to enforce or caused to be enforced any patent or patent rights against any Implementer for implementation of (i) any Required Element of Specification Version 1.0 or implementation of any Required Element of Specification Version 1.0 which is carried over to subsequent versions of the Specification. In addition, Members acknowledge that the covenant contained in this Section shall be applicable to subsequent versions of the Specifications and the ID
   Federation may request applicable written representations or other documentation from Member from time to time, including before and after meetings and at the time of adoption of future Specifications, in order to carry out this Section. Each current Member and any future Members are considered third party beneficiaries to the agreement and covenant of this subsection.
   3.2. **Copyright.** The copyright for Specification 1.0 shall belong to ID Federation. Each Member who contributed copyrighted materials to ID Federation for Specification 1.0 shall retain copyright ownership of its original work, while at the same time granting ID Federation a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the copyrights of Member or any Representative to reproduce, distribute, publish, display, perform, and create derivative works based on that original work for the purpose of developing Specification 1.0 under ID Federation's own copyright. In addition, Members acknowledge that the covenant contained in this Section shall be applicable to subsequent versions of the Specifications and the ID Federation may request applicable written representations or other documentation from Member from time to time in order to carry out this Section, including before and after meetings and at the time of adoption of future Specifications, in order to carry out this Specification.
   3.3. **Trade Secrets.** Members acknowledge that they are not disclosing trade secrets under the Trust Framework and other Members and the Id Federation are not under any obligation of confidentiality, unless otherwise agreed, as set forth in the Trust Framework.
4. **Process.** Member agrees to complete any documentation necessary to effect the representations contained in this Policy. Members may be required before or after technical meetings to complete a statement confirming Member's acceptance of the terms and conditions of this Policy.
5. **Definitions**. The definitions set forth below apply to this Policy. Other defined terms used in this Policy are as set forth in the Glossary.
   5.1. **"Implementers"** means any current or future Members or non-members who desire to use or implement Specification 1.0.
   5.2. **"Required Element"** means any element of Specification 1.0 that has not been identified as "optional." For the avoidance of doubt, if an Implementer may implement one of two or more alternative elements, then all such elements shall be deemed to be "Required Elements."
   5.3. **"Specification Version 1.0"** means Article 3 "Technical" of the ID Federation Trust Framework.
6. **Retained Rights**. Except as explicitly set forth in this Policy, each Member reserves any and all rights in its intellectual property.

Survival. This Policy shall survive any termination of a Member's membership in the ID Federation.

Appendix E

Amendment and Change Management Policy

The ID Federation Board of Directors will establish a process from time to time to implement any changes or amendments to the Trust Framework or the Formal Policies and Official Documents, the Participation Agreement and any other documents incorporated into the Trust Framework. A majority vote of a quorum of the ID Federation Board of Directors (as defined by Article IV of the By-Laws of ID Federation, Inc. as amended from time to time) is required for final approval of any proposed substantive change. Amendments to the By-Laws and the Certificate of Incorporation of ID Federation are subject to Article XIV of the By-Laws, as amended from time to time.

Appendix F

Glossary

Assessor - An Assessor is a third party identified by the ID Federation who is responsible for certifying the service of an applicant based on a neutral and independent assessment and testing as determined by the Policy Authority from time to time.

Authenticating Identity Provider - The Identity Provider that originally Authenticates the Individual User and generates the original Token in the process of Delegation.

Authenticate or Authentication - The verification that an Individual User is the person purportedly identified by a Token.

Authorization - The granting of role-based or other access controls and permissions to conduct transactions in or through an application, service or other system of a Relying Party.

Certificate Authority (CA) - A trusted third party organization that validates the identity of an organization before issuing a digital certificate and certifying ownership of that digital certificate to that entity. The digital certificates can be used to create digital signatures and public-private key pairs used to securely communicate and validity the identity of each party involved in an Internet transaction.

Certification Trust Mark - The federally registered trademark or servicemark designating Certified Services for an IdP.

Certified Services - An Identity Provider service that has been certified in accordance with the Trust Framework Certification Policy.

Certified Participant – A Participant that has at least one Certified Service in accordance with the Trust Framework Certification Policy.

Credential - The user ID and password, associated with a user account, which is used to confirm the identity of a person or software program in order to gain access to a resource.

Delegation - The process of transmitting Identity Attributes between an Identity Provider and Relying Party through a Identity Provider Proxy in the absence of a Trust Relationship between the Identity Provider and the Relying Party.

Existing Commercial Contract - A contract by which a Participant is involved in the provision of, sale, distribution licensing, or use of a financial or insurance related product or service with one or more other Participants and that is related to the Trust Framework.

Existing Commercial Relationship - The relationship between two or more Participants by which they are involved in the provision of, sale, distribution licensing, or use of a financial or insurance related product or service, e.g., the relationship between an agency and insurance carrier, or between either an agency or insurance carrier and a vendor. The contracts to do business with one another are indicia of an Existing Commercial Relationship. It is not assumed that Vendors have Existing Commercial Relationships with one another.

Federation Operator - The Federation Operator is responsible for day to day operations of the ID Federation, including provision of business services such as “first point of contact” telephone and e-mail communications for the ID Federation, on boarding new Participants and maintaining current records, including the Participant Database and Meta-Data repository.

Formal Policies and Official Documents - Policies and Official Documents that are formally incorporated by reference into the Trust Framework and are promulgated or approved by the Policy Authority, including the Intellectual Property Rights Policy, the Antitrust Policy, the Accreditation and Certification Policy and other Policies (available on the ID Federation website).

ID Federation - The entire federated identity system defined and governed by this Trust Framework, including the aggregate of all parties using or supporting the use of identity assertions in accordance with this Trust Framework in one or more Roles.

IDFI - This is the acronym for the ID Federation, Inc.

Identity Attributes - Information that uniquely describes an individual (i.e. First Name, Role, etc) (commonly called assertions or claims). While Identity Attributes might be common between individuals, all the attributes used together create a unique identity.

Identity Provider (IdP) - An Identity Provider (IdP) is a Participant that issues a Credential and Token to Individual Users and effectuates the passing of those Tokens to Relying Parties for purposes of asserting and Authenticating Individual User identity.

Identity Provider Proxy - An Identity Provider acting as a proxy for an originating identity provider by accepting a Token from the Authenticating identity provider and acting as a conduit to a target system hosted by a Relying Party.

Individual User (IU) - An Individual User is a single human being provisioned a Federation Token by a User Authority and issued that Token by an Identity Provider.

Member - An ID Federation member of any class.

Membership Trust Mark - The federally registered trademark or servicemark designating official [registered] Participation in the ID Federation.

Metadata - Commonly called data about data contents, Metadata is typically used to describe the structure of data not the actual data value.

Onboarding - Being added to the Participant Directory and approved for Participation in the ID Federation as an Identity Provider or Relying Party.

Participant - An Identity Provider, Relying Party or User Authority.

Participant Directory - An information directory such as a database or content management system that is administered by the Federation Operator containing information about each Identity Provider, Relying Party and User Authority that participates in the ID Federation, including every Certified Service and other relevant operational data related to the ID Federation.

Participation Agreement - The contract by which a Party agrees to abide by the Trust Framework, execution of which is a prerequisite to become a Participant in the ID Federation.

Party - A legal entity that is an applicant to become a Participant, is a Participant or has been a Participant in the ID Federation.

Policy Authority - The Board of Directors is the Policy Authority. The Policy Authority is responsible for promulgating the ID Federation Trust Framework and for the strategic, organic and other material

decisions making for activities operating under the Trust Framework, including approval of the requirements for Certified Services and Accreditation.

Relying Party - A Relying Party is a Participant that accepts and relies upon a Token of an Individual User that has been issued by an Identity Provider and received for the purpose of asserting and Authenticating the identity of the Individual User.

Role - Participation within the ID Federation occurs by parties that conduct one or more Roles, as specified and defined in the Trust Framework, namely an Identity Provider (IdP), a Relying Party (RP), a User Authority (UA) or an Individual User (IU). Additional Roles that support the ID Federation are the Governance Authority, the Federation Operator and the Assessor.

Rules - The Rules refer to the current Trust Framework as amended from time to time.

Token - A Token is a generic term intended to provide a packaged set of information which allows for Authentication between IdPs and RPs. Typical Tokens include but are not limited to IP/TCP channel data, Server Signatures, Authentication data, and Payload information.

Trust Framework - The term Trust Framework refers to the document titled “Identity Federation Rules for the Insurance & Financial Services Industry” and includes without limitation the Formal Policies, Official Documents, or Rules.

Trust Mark - The Certification Trust Mark and/or the Membership Trust Mark.

Trust Relationship - The business, legal, and technical agreements between two organizations supporting technical integrations where a party acting as an Identity Provider Authenticates Individual Users on behalf of the other party acting as a Relying Party.

User Authority (UA) - A User Authority (UA) is a Participant that provisions, maintains and de-provisions Tokens for Individual Users within its business.

Appendix G

ID Federation Use Cases Specification

High-Level Technical Use Cases

The High-Level Technical Use Cases below satisfy all of the business use cases outlined in Section 1.01 of this document as well as logical extensions of those business use cases which could exist, but were not described.

Table 1 below provides an indexed cross-reference for each of those business use cases, listing the high-level technical use case that addresses each business use case, followed by Detailed Use Case analyses for each of the high-level use cases.

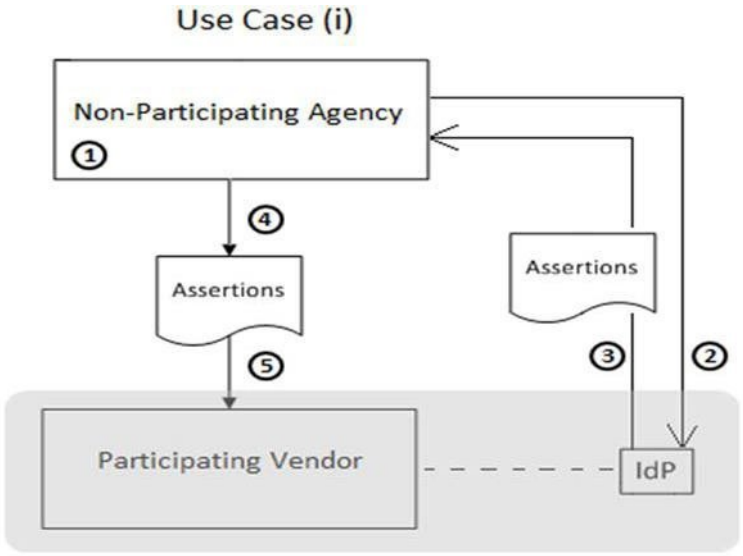
Table 1

Business#	Technical#	Use Case Description	Individual User
1	iv	Direct Carrier Quote on Carrier Website	IdP Agency Producer
2	iv	Direct Carrier Inquiry/Endorsement on Carrier Website	IdP Agency Producer
3	vi	Carrier Inquiry/Endorsement from Agency Management System to Carrier Website	IdP Agency Producer
4	vi	Comparative Quote from Agency Management System to Comparative Rater	IdP Agency Producer
5	vi	Comparative Quote directly from Agency Management System	IdP Agency Producer
6	vi	Comparative Quote directly from Comparative Rater	IdP Agency Producer
7	iv	First Notice of Loss on Carrier Website	IdP Agency Producer
8	vi	First Notice of Loss from Agency Management System to Carrier Website	IdP Agency Producer
9	ii	Customer Management (Account, CRM, etc.) on Vendor Application	IdP Agency Producer
10	vi	Book roll	IdP Agency Producer
11	iii	Direct Carrier Quote on Carrier Website	Non-IdP Agency Producer
12	iii	Direct Carrier Inquiry/Endorsement on Carrier Website	Non-IdP Agency Producer
13	i	Carrier Inquiry/Endorsement from Agency System IdP to Carrier Website	Non-IdP Agency Producer
14	i	Comparative Quote from Agency System IdP to Comparative Rater	Non-IdP Agency Producer
15	i	Comparative Quote directly from Agency System IdP	Non-IdP Agency Producer
16	i	Comparative Quote directly from Comparative Rater IdP	Non-IdP Agency Producer
17	iii	First Notice of Loss on Carrier Website	Non-IdP Agency Producer
18	v	First Notice of Loss from Agency System IdP to Carrier Website	Non-IdP Agency Producer
19	i	Customer Management (Account, CRM, etc.) on Vendor IdP Application	Non-IdP Agency Producer
20	viii	Book Roll from Agency System IdP to Carrier System	Non-IdP Agency Producer
21	iv or v or viii	Inquiry on Carrier Website via Agency or Vendor IdP	Non-IdP Consumer
22	i or ii	Inquiry on Agency / Vendor Portal via Agency or Vendor IdP	Non-IdP Consumer
23	iv or v of viii	Quote on Carrier Website via Agency or Vendor IdP	Non-IdP Consumer
24	i or ii	Quote on Agency / Vendor Portal via Agency or Vendor IdP	Non-IdP Consumer
25	i or ii	Comparative Quote via Agency or Vendor IdP	Non-IdP Consumer
26	iv or v of viii	First Notice of Loss on Carrier Website via Agency or Vendor IdP	Non-IdP Consumer
27	i or ii	First Notice of Loss on Agency / Vendor Portal via Agency or Vendor IdP	Non-IdP Consumer
28	iii or v	All Individual Users logging into Identity Provider System	Remote Worker
29	ii or iv or vi	Direct Login to Carrier/Agency/Vendor Website	IdP Agency Producer
30	i or iii or v	Direct Login to Carrier/Agency/Vendor Website	Non-IdP Agency Producer

Note: Consumers can act as Individual Users in any of the high-level use cases described below, but a participating User Authority must be responsible for requesting provisioning, managing access to, and de-provisioning the Credentials and Tokens issued by a participating Identity Provider.

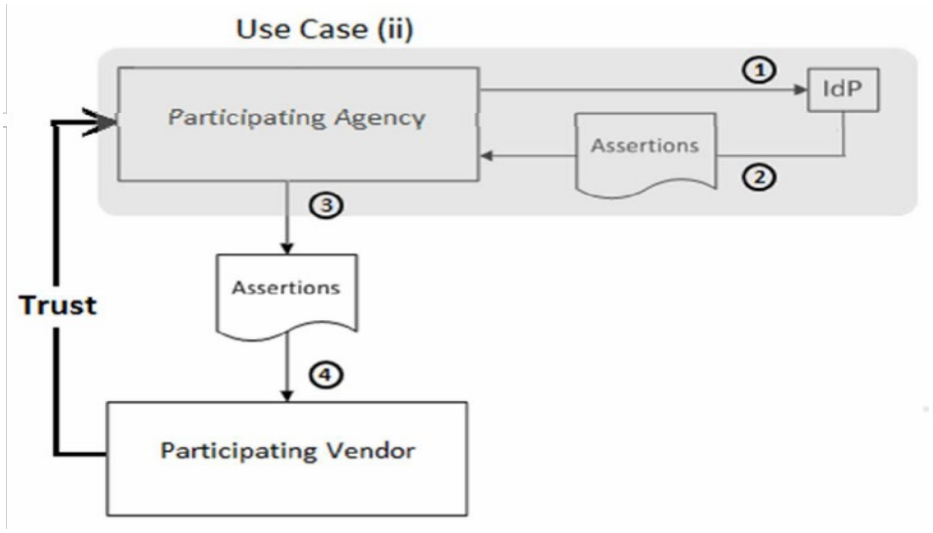
(i) Individual User accesses participating Vendor Systems (IdP & RPs) via non-participating Agency – "Non-Participating Agency to Participating Vendor"

1) Agency provides access to Vendor systems, but is not a Participant in the ID Federation
2) Vendor system (IdP) Authenticates Individual User via Vendor system login page
3) Vendor system (IdP) creates Individual User Identity Attributes
4) Vendor system (IdP) provides access to other participating Vendor systems (RPs) using Individual User Identity Attributes
5) Other Vendor systems (RPs) accept Individual User Identity Attributes from Vendor system (IdP)



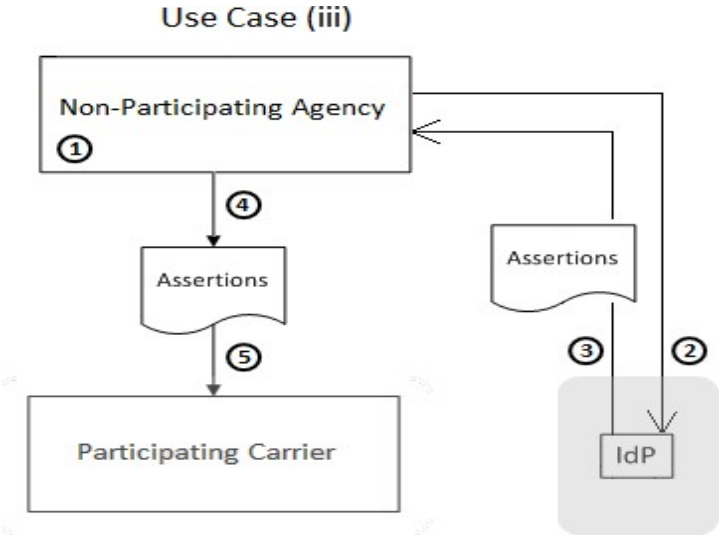
(ii) Individual User accesses participating Vendor systems (RPs) via participating Agency (IdP) – "Participating Agency to Participating Vendor"

1) Agency (IdP) Authenticates Individual User via Agency login page
2) Agency (IdP) creates Agency Individual User Identity Attributes
3) Agency (IdP) provides access to Vendor systems (RPs) using Agency Individual User Identity Attributes
4) Vendor systems (RPs) accept Individual User Identity Attributes from Agency (IdP)



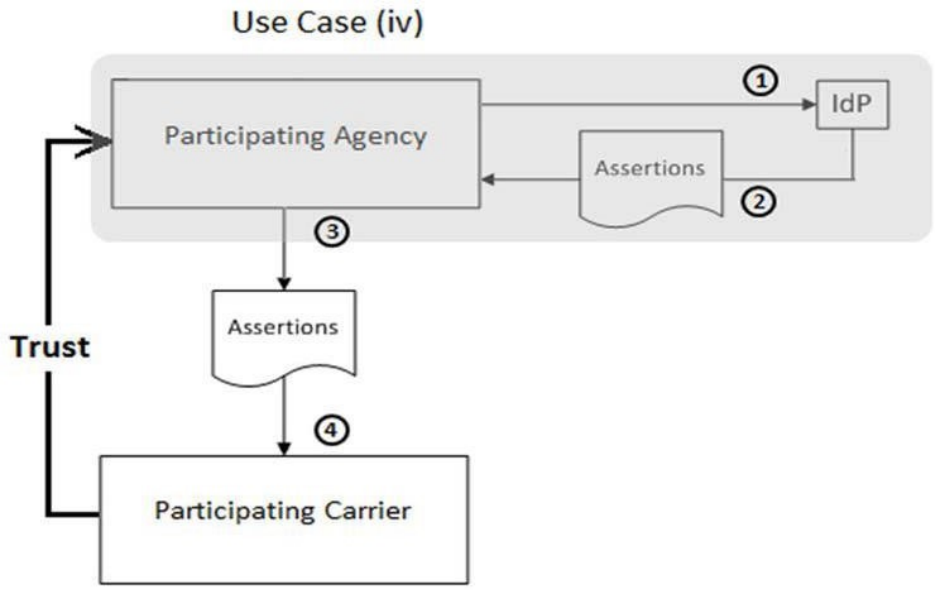
(iii) Individual User accesses participating Carrier systems (IdP & RPs) via non-participating agency – "Non-Participating Agency to Participating Carrier"

1) Agency provides access to Carrier systems, but is not a Participant in the ID Federation
2) Carrier system (IdP) Authenticates Individual User via Carrier system login page
3) Carrier system (IdP) creates Carrier Individual User Identity Attributes
4) Carrier system (IdP) provides access to Carrier systems (RPs) using Carrier Individual User Identity Attributes
5) Carrier systems (RPs) accept Individual User Identity Attributes from Carrier system (IdP)



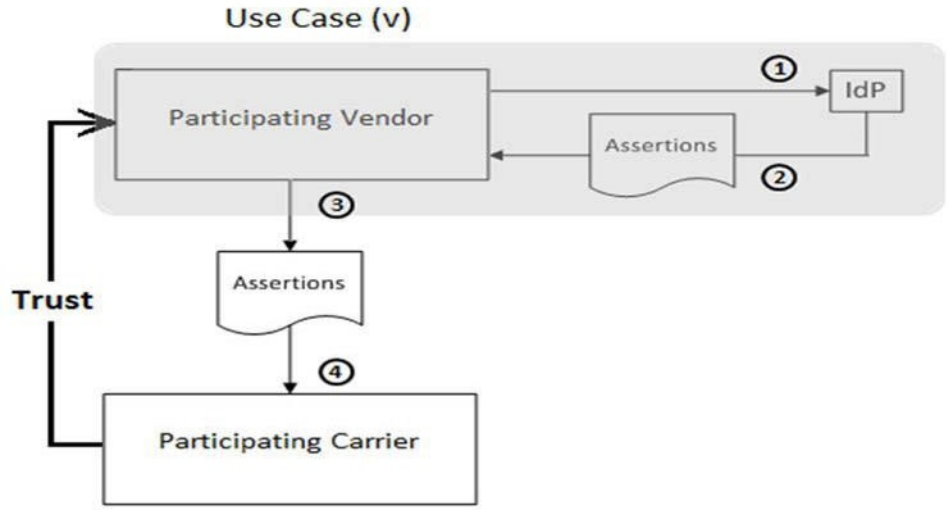
(iv) Individual User accesses participating Carrier systems (RPs) via participating Agency (IdP) – "Participating Agency to Participating Carrier"

1) Agency (IdP) Authenticates Individual User via Agency login page
2) Agency (IdP) creates Agency Individual User Identity Attributes
3) Agency (IdP) provides access to Carrier systems (RPs) using Agency Individual User Identity Attributes
4) Carrier systems (RPs) accept Individual User Identity Attributes from Agency (IdP)



(v) Individual User accesses participating Carrier systems (RPs) via participating vendor system (IdP) – "Participating Vendor to Participating Carrier"

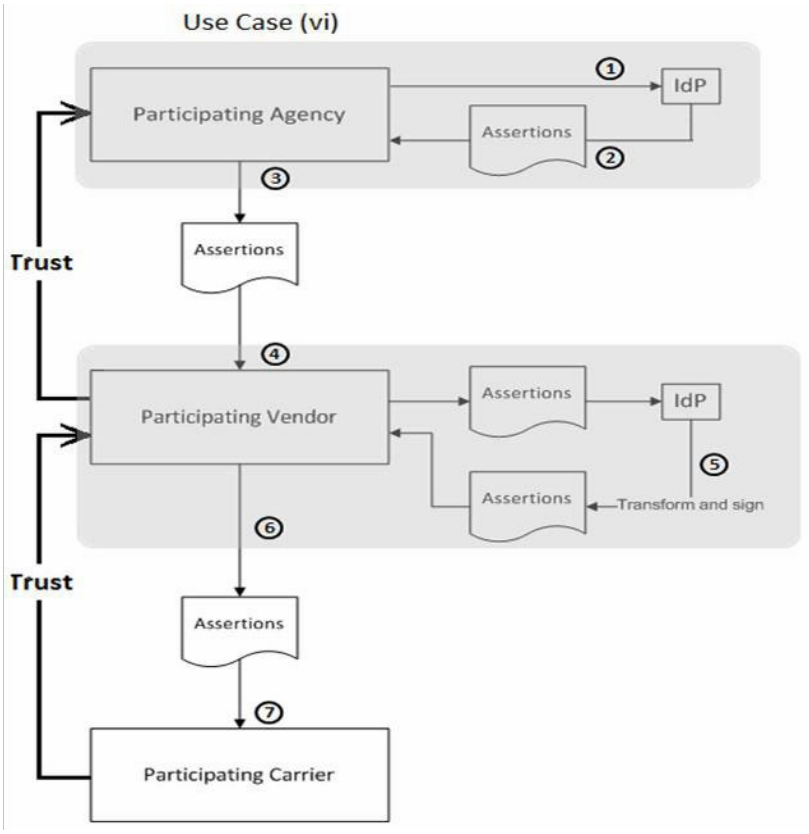
1) Vendor system (IdP) Authenticates Individual User via Vendor system login page
2) Vendor system (IdP) creates Vendor Individual User Identity Attributes
3) Vendor system (IdP) provides access to Carrier systems (RPs) using Vendor Individual User Identity Attributes
4) Carrier systems (RPs) accept Individual User Identity Attributes from Vendor system (IdP)



(vi) Individual User accesses participating Carrier systems (RPs) via participating Agency (IdP) and participating Vendor systems (IdP & RPs) – "Participating Agency to Participating Vendor to Participating Carrier"

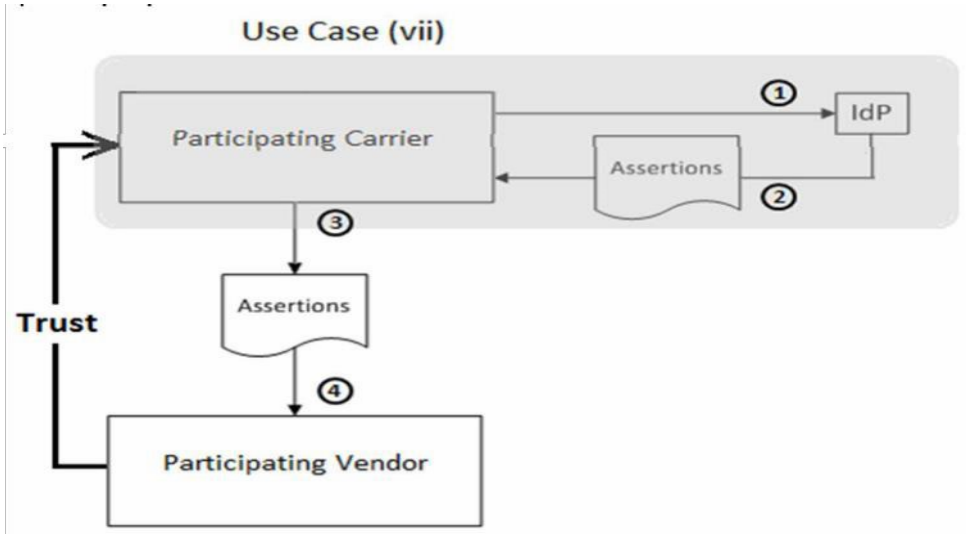
1) Agency (IdP) Authenticates Individual User via Agency login page
2) Agency (IdP) creates Agency Individual User Identity Attributes
3) Agency (IdP) provides access to Vendor systems (RPs) using Agency Individual User Identity Attributes
4) Vendor systems (RPs) accept Individual User Identity Attributes from Agency (IdP)

5) Vendor system (IdP) creates Individual User Identity Attributes using Agency Individual User Identity Attributes
6) Vendor system (IdP) provides access to Carrier systems (RPs) using Vendor Individual User Identity Attributes
7) Carrier systems (RPs) accept Individual User Identity Attributes from Vendor system (IdP)



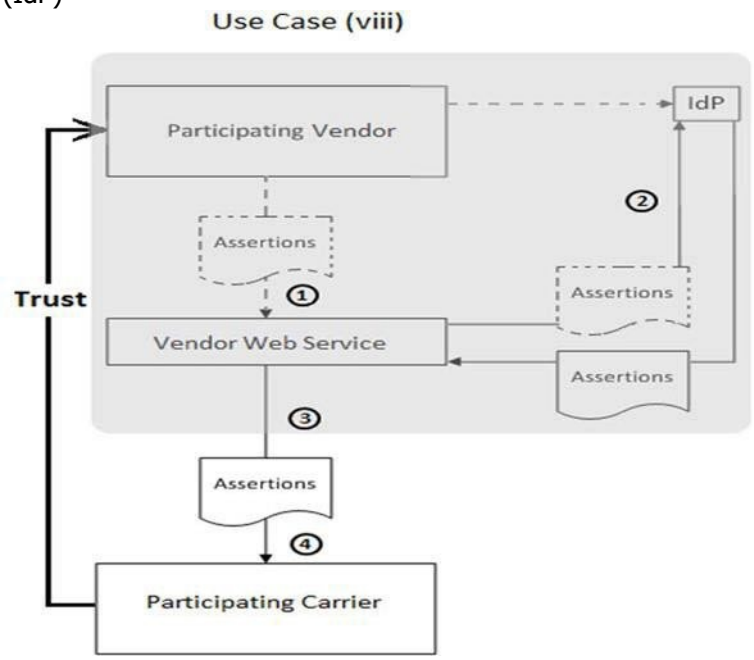
(vii) Individual User accesses participating Vendor systems (IdP & RPs) via participating Carrier system – "Participating Carrier to Participating Vendor"

1) Carrier system (IdP) Authenticates Individual User via Carrier system login page
2) Carrier system (IdP) creates Carrier Individual User Identity Attributes
3) Carrier system (IdP) provides access to Vendor systems (RPs) using Carrier Individual User Identity Attributes
4) Vendor systems (RPs) accept Carrier Individual User Identity Attributes from Carrier system (IdP)



(viii) Web Service accesses participating Carrier systems (RPs) via participating vendor system (IdP) – "Participating Vendor Web Service to Participating Carrier"

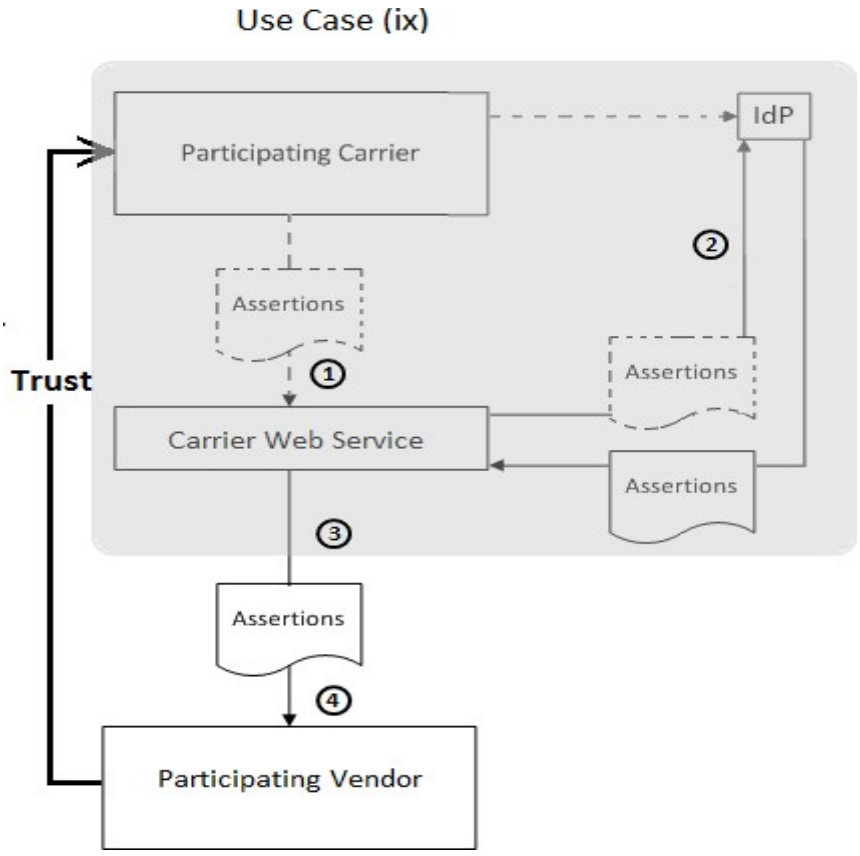
1) Vendor system calls Web Service with Individual User's original Identity Attributes
2) Web Service requests new Token containing original Identity Attributes from Vendor system (IdP)
3) Vendor system (IdP) provides access to Carrier systems (RPs) using Vendor Web Service Identity Attributes
4) Carrier systems (RPs) accept Web Service Identity Attributes from Vendor system (IdP)



(ix) Web Service accesses participating Vendor systems (RPs) via participating Carrier system (IdP) – "Participating Carrier Web Service to Participating Vendor"

1) Carrier system calls Web Service with Individual User's original Identity Attributes
2) Web Service requests new Token containing original Identity Attributes from Carrier System (IdP)

3) Carrier System (IdP) provides access to Vendor systems (RPs) using Carrier Web service Identity Attributes
4) Vendor systems (RPs) accept Web Service Identity Attributes from Carrier system (IdP)



Currently Out of Scope Use Cases

- Participating IdP attempts to accesses Participating RP via Non-Participant – "Non-Participant Pass-Through"
- Consumer (IdP) accesses Agency (RP)

Consumer (IdP) accesses Vendor (RP)

- Consumer (IdP) accesses Carrier (RP)

Appendix H

Multi Factor Authentication (MFA) – Code Lists

MFA Type (mfatype)

List based on Authentication Method Reference Values per the Internet Engineering Task Force (IETF). List below will be updated following changes to the June 2017 version of RFC8176.
https://www.rfc-editor.org/rfc/rfc8176

000 – No MFA

face - Biometric authentication [RFC4949] using facial recognition.

fpt- Biometric authentication [RFC4949] using a fingerprint.

geo - Use of geolocation information for authentication, such as that provided by [W3C.REC-geolocation-API-20161108].

hwk - Proof-of-Possession (PoP) of a hardware-secured key. See Appendix C of [RFC4211] for a discussion on PoP.

iris - Biometric authentication [RFC4949] using an iris scan.

kba - Knowledge-based authentication [NIST.800-63-2] [ISO29115].

mca - Multiple-channel authentication [MCA]. The authentication involves communication over more than one distinct communication channel. For instance, a multiple-channel authentication might involve both entering information into a workstation's browser and providing information on a telephone call to a pre-registered number.

mfa - Multiple-factor authentication [NIST.800-63-2] [ISO29115]. When this is present, specific authentication methods used may also be included.

otp - One-time password [RFC4949]. One-time password specifications that this authentication method applies to include [RFC4226] and [RFC6238].

pin - Personal Identification Number (PIN) [RFC4949] or pattern (not restricted to containing only numbers) that a user enters to unlock a key on the device. This mechanism should have a way to deter an attacker from obtaining the PIN by trying repeated guesses.

pwd - Password-based authentication [RFC4949].

rba - Risk-based authentication [JECM].

retina - Biometric authentication [RFC4949] using a retina scan.

sc- Smart card [RFC4949].

sms - Confirmation using SMS [SMS] text message to the user at a registered number.

swk - Proof-of-Possession (PoP) of a software-secured key. See Appendix C of [RFC4211] for a discussion on PoP.

tel - Confirmation by telephone call to the user at a registered number. This authentication technique is sometimes also referred to as "call back" [RFC4949].

user - User presence test. Evidence that the end user is present and interacting with the device. This is sometimes also referred to as "test of user presence" [W3C.WD-webauthn-20170216].

vbm - Biometric authentication [RFC4949] using a voiceprint.

wia - Windows integrated authentication [MSDN].

Assurance Level (assurancelevel)
NIST Special Publication 800-63B - Digital Identity Guidelines". List below will be updated following changes to the 03-02-2020 version.

https://pages.nist.gov/800-63-3/sp800-63b.html#multifactorOTP

Assurance Level Values
AAL1 – Assurance Level 1
AAL2 – Assurance Level 2
AAL3 – Assurance Level 2

Table of assurance levels from 03-02-2020 version

	AAL1	AAL2	AAL3
Permitted authenticator types	Memorized Secret; Look-up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-up secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret