MITRE External Identity Federation Trust Framework System Rules

Version 1.0, September 21, 2012

Draft and Commentary

Note: This document does not represent official MITRE policy and has been released as a draft for public discussion.

Commissioned by and for:
Justin Richer, Lead Computer Scientist
Social Computing Researcher; Multimedia and Collaboration, G061
202 Burlington Rd, M/S K320, Bedford, MA 01730
781-271-8176; jricher@mitre.org

Trust Framework Architect:
Dazza (Daniel) Greenwood, JD
Consultant Agreement No. 92207
CIVICS.com 650-504-5474 dazza@civics.com
1 Broadway, 14th Floor, Cambridge, MA 02142

MITREid External Identity Federation
Trust Framework System Rules

1. Business Rules

1.1. Scope

This Trust Framework applies to the use by MITRE personnel of OpenID 2.0 and OpenID Connect as described in Section 3, collectively called MITREid. This Trust Framework also applies to all non-MITRE users who connect to MITRE systems using the MITRE External Identity Federation.

[Commentary: The scope defined in this draft text reflects the current language at https://id.mitre.org/about which reads "MITREid is an OpenID Identity Provider for MITRE employees. Only current MITRE employees have identities provisioned on this identity provider, and identities are not available for registration. This server is a research prototype service provided with best-effort system availability."]

[Commentary: This section defines the scope and purposes of the federation. For example, if the underlying business scenario of the federation involved a multi-party consortia, such as the ID Federation, Inc (see idfederation.org), then the scope may be: "This identity federation system is provided for the purpose of enabling users of member organizations single-sign-on to designated applications and services of other member organizations."]

[Commentary: A Business Use Case is a way to define the intended business scope of the MITRE External Identity Federation and is a drafting technique that would be recommended if or when this research prototype matures into production grade operations. Business Use Cases describe the key supported interactions, including the transactions to be conducted, without detailed specification of technical details. While technical details are described in Technical Use Cases in Section 3, the nature of federated identity is such that some general reference to high-level technology may be referenced in the Business Use Cases. The Business Use Cases are intended to ensure alignment with the intended purposes of the federation and traceable continued achievement of the goals and objectives of the identity system. The Business Use Cases also provide a basis for establishing that the technology for opening up access to systems extends only so far as the owners of the underlying work intend and not necessarily as far as unbounded use of the technology can permit. More information on the Business Use Cases, in the context of the Legal and Technical Use Cases for federated identity systems, may be found at: www.civics.com/use-cases]

[Commentary: It is anticipated that the initial covered Business Use Cases will relate narrowly to 1) the use of OpenID 2.0 and OpenID Connect for access to the Handshake applications of the MITRE Partnership Network and 2) use by MITRE employees of MITRE issued OpenID 2.0 and OpenID Connect Derived Federated Credentials to access external web sites. It is expected that one or two partners, such as JPL, Lincoln Labs, or the Advanced Cyber Security Center, will be identified to act as an initial partners to test usage of this approach, including use of OpenID 2.0 or OpenID Connect and agreement to the partner Participation Agreement. While Version 1.0 of these Rules are intended to cover a relatively conservative scope of Business Use Cases, the design of this approach intentionally scales to include additional Business Use Cases over time, and provides a process for the considered and deliberate choice to expand or otherwise change the scope as needed. It is anticipated that other potential scenarios could include: 1) many more partner organizations joining, and the requisite scaling requirements of more production grade systems for operations and shared services, 2) more types of applications and services available for access through use of federated identity under these rules, and the consequent updates to the types of business transactions in the use cases and additional legal reviews and updates as needed, as well as the more robust technical implementation required and consequent amendment to the

types of standards, configurations, profiles and identity services offered, 3) usage of the MITRE identity system and rules approach, with optional "modular" sections that would pertain when the framework is used to interoperate with a heavily regulated and complex system, such as the approach used by FHA to provide access to the Nationwide Health Information Network (NwHIN), which requires use of an authorized Gateway which is subject to the DURSA multilateral legal agreement; this modular approach could be accomplished in the business section by adding the purpose, scope and corresponding use cases, in the legal section by ensuring the additional requirements are met for that scenario, and in the technical section by adding additional attributes, other security services and components expected at the end-points at and behind the NwHIN Gateway, 4) the emergence of other partners usage of a Trust Framework System Rules governing their use of federated identity, as anticipated in the National Strategy for Trusted Identities in Cyberspace promotion of a new ecology of Trust Frameworks suitable for particular industries, economic sectors and other so-called "circles of trust", and in this case the scope and use cases would include cross-certification and other methods for cross-boundary integration and harmonization of use cases through interstitial trans-federation agreements.]

[Commentary: Regarding potential scope in the longer term future: 1) In addition to collaborative systems of MPN, could also use a "modular" approach for adding adapters to interoperate with heavily regulated systems, for example the FHA approach to getting into NwHIN under DURSA (such that, for those interactions, a second layer of business, legal and tech rules and capabilities applied, and it would be possible with an attri[illegible]or other mechanism to delineate which end-point and other constraints were needed in those cases). In the case of a modular approach in the future, in effect, one or more attachments to the Trust Framework would service as contingent additional terms that further refine, modify and augment agreed base-line terms when the MITREid Trust Framework is used in particular and objectively defined contexts.]

1.2. Roles and Relationships

[Commentary: The Roles and Relationships are core to the Trust Framework and System Rules, and require further conversation and feedback to adequately define. Below is an initial list of typical and relevant roles found within identify federations.]

[Commentary: If and when an external partner organization is recognized as a White Listed Identity Provider or Relying Party for its employees or other approved Users, an approach to this section might be to point toward a document listing the current participating white listed partners and for that document, directory, or repository to include the names of parties playing each role, as well as the relevant meta data and other technical information that may be available. This approach is modeled in Addendum 3.]

1.2.1. Policy Authority

The Policy Authority is responsible for updating and interpreting this Trust Framework and designating or approving, directly or by delegated authority, the then current parties assuming the roles below.

1.2.2. System Operator

The system operator is responsible for implementing and administering MITRE External Identity Federation use by MITRE.

1.2.3. Identity Provider

An Identity Provider is responsible for issuing a Primary Credential or a Derived Federated Identity Credentials for Users. The MITREid Identity Provider is responsible for issuing Derived Federated Credentials for Users who are MITRE personnel.

A White Listed Identity Provider system is a service provider that has been approved by the System Operator as a pre-authorized Identity Provider such that MITRE Relying Party sites may

provide automatic authorization on first and all subsequent access to Users of Derived Federated Credentials issued by that Identity Provider.

1.2.4. User Authority
A User Authority is responsible for authorizing the issuance of Primary Credentials to Users.

1.2.5. User
A User is a single human who authenticates to any system covered by this Trust Framework, either using a Primary or Derived Federated Credential.

1.2.6. Relying Party
A Relying Party is a service provider that accepts or has accepted a Derived Federated Credential issued by an Identity Provider for the purpose of authenticating a User.

A White Listed Relying Party system is a service provider that has been approved by the System Operator as a pre-authorized Relying Party such that MITRE users are provided automatic authorization on first and all subsequent access to one or more Relying Party sites.

1.2.7. Certification Assessor

A Certification Assessor is an independent party approved by the System Operator that is responsible for certifying or recommending certification of Identity Providers, User Authorities and/or Relying Parties according to criteria set or adopted by the System Operator.

[Commentary: MITRE is pursuing Federal Identity, Credential, and Access Management (FICAM) accepted certification at this time for its OpenID 2.0 service for the purpose of gaining more information about this process and evaluating how best to adopt or adapt this process for use in its internal determination of which external parties to federate with and specifically which parties to add to White Lists.]

1.3. White, Black and Grey Lists

1.3.1. Grey List
Grey Listed sites include any Identity Provider or Relying Party that implements the standards in Section 3 and that has not been added to a White List or Black List by the System Operator. Any Grey Listed Relying Party may accept a Derived Federated Credential from any User and any User may use a Derived Federated Credential to access the site of any Grey Listed Relying Party.

If an Identity Provider is Grey Listed, then the Relying Party makes the decision on a per use or other basis whether to accept and rely upon credentials issued by that Identity Provider. If a Relying Party is on a Grey List then the User makes the decision whether to authorize the use of their Derived Federated Credential to access the Relying Party site.

1.3.2. White List
The System Operator, by approval of or delegated authority by the Policy Authority, may add a Relying Party site to the MITREid White List, thereby allowing automated authorization for MITRE Users.

1.3.3. Black List:
The System Operator may determine whether a site is in violation of these rules or otherwise disapproved for federation, and upon such determination may add that site to the MITREid Black List, thereby preventing a MITRE User from using their Derived Federated Credential to access such site and preventing Derived Federated Credentials from Black Listed Identity Providers from being used to access MITRE Relying Party sites under this Trust Framework.

1.4. Certification

Certification is a material consideration favoring the System Operator decision on inclusion of parties to a White List, but is neither required nor sufficient. The MITRE External Identity Federation Certification Policy is available at [TBD].

[Commentary: Please see discussion in Addendum 4, related to Certification, for more information on the context and purpose of this section.]

1.5. Business Processes and Practices

The following business processes and practices apply to the use of MITRE External Identity Federation [TBD].

[Commentary: At this time, the actual practices and procedures to operate and use MITRE External Identity Federation are largely ad hoc and tailored to the prototype scope of this initiative. However, eventually if and when use of MITRE Identity Federation becomes a regular, operational production grade element of MITRE systems, the recording of processes and practices applicable to key roles and parties will be important. It is typically best to note the details of these processes and practices in external documents, including guidance, FAQ and help files, which may be updated from time to time with little or no approval or notice, provided they do not violate any requirement or constraint in the System Rules or other applicable rules.]

2. LEGAL RULES

2.1. Application of These Rules

These rules apply to the issuance, use, acceptance of or reliance on Derived Federated Credentials within the MITRE External Identity Federation.

Neither this Trust Framework, nor any course between the Parties hereunder, shall constitute or create a partnership, joint venture, principal-agent relationship or employer-employee relationship between the Parties.

2.2. Authoritative Rules and Incorporation by Reference

The authoritative current version of the Trust Framework System Rules can be found at www.mitre.org/trustframework [note actual URL to be determined]. These Rules, including all documents explicitly Incorporated by Reference, provide standard default terms for use of the External Identity Federation, but in the event of a conflict between the terms of an existing contract between parties governing the terms of access to relevant applications or services, then the terms of the existing contract shall govern.

When the text of these Rules explicitly refers to a "document Incorporated by Reference" and includes a URL to the authoritative version of that document, then the content of that document shall have the same force and effect as if directly published within these Rules.

2.3. Liability, Warranties and Indemnification

THE MITRE CORPORATION MAKES NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, CAPABILITY, EFFICIENCY, MERCHANTABILITY, OR FUNCTIONALITY OF MITREid OR MITRE EXTERNAL IDENTITY FEDERATION OR ANY INFORMATION OR SERVICES COMPRISING OR RELATED TO MITREid OR MITRE EXTERNAL IDENTITY FEDERATION. IN NO EVENT WILL THE MITRE CORPORATION BE LIABLE FOR ANY GENERAL, CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, OR SPECIAL DAMAGES, EVEN IF MITRE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ANY NON-MITRE PARTY SUBJECT TO THIS TRUST FRAMEWORK AGREES TO INDEMNIFY AND HOLD HARMLESS MITRE, ITS AFFILIATES AND SUBSIDIARIES, AND THEIR RESPECTIVE DIRECTORS OR TRUSTEES, OFFICERS, EMPLOYEES AND AGENTS FROM ANY AND ALL INJURIES, LOSSES, CLAIMS AND DAMAGES TO ANY PERSON OR PROPERTY UNDER ANY THEORY OF LIABILITY AND IRRESPECTIVE OF THE CAUSE OF SAID LIABILITY, AND ALL COSTS AND EXPENSES INCLUDING WITHOUT LIMITATION, ATTORNEYS' FEES AND ANY OTHER LIABILITIES INCURRED BY MITRE AS A RESULT OF ANY NEGLIGENT OR WILLFUL ACTION OR OMISSION OF SUCH PARTY, HIS/HER EMPLOYEES OR AGENTS, OR ARISING OUT OF OR RESULTING IN ANY MANNER IN WHOLE OR IN PART FROM THE SUCH PARTY'S USE OF OR RELIANCE UPON MITREid OR MITRE EXTERNAL IDENTITY FEDERATION OR ANY INFORMATION OR SERVICES COMPRISING OR RELATED TO MITREid OR MITRE EXTERNAL IDENTITY FEDERATION.

2.4. Record Keeping and Reporting

The required log files for Identity Providers and White Listed Relying Parties under Section 3.6 of this Trust Framework must be protected and maintained in accordance with reasonable commercial practices or as specified in any applicable certification or agreement. Such log files must be made available to MITRE upon request when reasonably necessary to ensure MITRE External Identity Federation system integrity or for purposes of troubleshooting MITRE system issues.

[Commentary: This section can, of course, be vastly more complex and prescriptive. However, given the current preliminary state of the MITREid prototype and the general interest in making interconnection a relatively easy matter, the requirements on third parties for administrative and other uncompensated duties have been greatly reduced. In addition, in the event of a White Listed or other trusted partner, it is possible that an additional agreement may specify higher level obligation regarding record keeping.]

2.5. No Service Level Guarantee

Reasonable efforts are made to maintain service, however you may notice occasional outages or disruptions as MITREid is being continuously refined. Under this Trust Framework, support of MITRE External Identity Federation services as Identity Provider and/or Relying Party and/or otherwise may be modified or discontinued at any time and with no notice.

[Commentary: This term may need to be modified within the Trust Framework to provide a notice period before discontinuation of the service if MITRE intends for external parties to rely upon the service in the future. In addition, this term may need to be modified in the event MITRE enters into a trusted partner agreement with entities on a White List and with whom more stable service levels are negotiated. In the event of such an additional White List or other trusted partner agreement, the additional service guaranties would supersede the terms of this Trust Framework under Section 2.8, defining Order of Precedence herein.]

2.6. Amendment

MITRE reserves the right at any time to make changes to this Trust Framework at any time by posting an updated version of this Trust Framework to www.mitre.org/trustframework [note actual URL to be determined].

2.7. Minimum Terms

In the coding and implementation of MITREid services subject to this Trust Framework, Users should see the following terms [TBD]:

[Commentary: At this time, it is premature to include minimum mandatory terms. However, this section serves as a placeholder for the results of future discussion with MITRE corporate counsel and other officials regarding required end-User terms, such as liability limitations, links to broader terms or privacy policy, notice of information sharing, consent to "remember" login authorization and similar terms.]

2.8. Order of Precedence

In the event MITRE Corporation and another Party subject to this Trust Framework and any documents or policies incorporated by reference also are subject to another contract or other enforceable agreement and there is an inconsistency or conflict between terms of any of those documents, the inconsistency or conflict shall be resolved in accordance with the following order of precedence:

1. The Contract or other enforceable agreement between MITRE and the other Party or Parties
2. Any MITRE policy of other official document incorporated by reference into this Trust Framework
3. The Terms of Use and/or MITRE Privacy Policy of the site being accessed with a Derived Federated Credential
4. This Trust Framework
5. Any other documents, including technical standards, protocols or industry guidelines

2.9. Applicable Law

This Trust Framework will be governed by the laws of the Commonwealth of Virginia without regard to Virginia conflicts of laws rules.

[Commentary: Given that MITRE Corporation is incorporated in Delaware, it is possible MITRE legal counsel may seek Delaware or the law of another state to govern in this section. The reference to Virginia law reflects a clause on other MITRE contracts and therefore is used as the starting point for this draft.]

2.10. Notice and Points of Contact

Any notices, requests, demands or other communications transmitted to MITRE and related to this Trust Framework shall be in writing and shall be effective when delivered in person or mailed, postage prepaid, registered or certified, and addressed to the address stated below.

All communications to MITRE shall be addressed to:

Attention: [include name or department here], Mail Stop: [include mail stop here]
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
Phone: [include phone here]
E-mail: [include email here]

All technical matters shall be directed to:

Attention: Justin Richer,
Lead Computer Scientist
Social Computing Researcher; Multimedia and Collaboration, G061
202 Burlington Rd, M/S K320, Bedford, MA 01730
781-271-8176; jricher@mitre.org

3. TECHNOLOGY RULES

3.1. Technical Scope

3.1.1. Technical Use Cases

The following use cases are supported under this Trust Framework: [TBD]

[Commentary: For so long as MITREid is an early-stage research prototype, it is premature to focus on detailed documentation of supported use cases. However, this draft Trust Framework anticipates a future state at which external and internal parties will seek to implement and interoperate with MITRE External Identity Federation services and the important role of this document to facilitate and regulate adoption. To that end, the types of technical use cases that would be relevant and constructive to detail in the future are noted below.

- MITREid User Logs Into Grey Listed Relying Party
- MITREid User Logs Into White Listed Relying Party
- MITREid User Logs Into Black Listed Relying Party
- Non-MITRE User Logs Into MITRE External Identity Federation Enabled Site
- Non-MITRE CAC User Logs Into MITRE External Identity Federation Enabled Site
- MITRE Relying Party Site Implements MITRE External Identity Federation Access
- Non-MITRE Identity Provider Added to MITRE External Identity Federation White List
- Non-MITRE Relying Party Site Accepts MITREid User Login]

3.1.2. Technical Architecture

[Commentary: In this section, if desired, MITRE can describe its technical architecture. The current diagrams depicting initial architectural approach are included in Addendum 2.b below.]

3.2. Standards for Derived Federated Credentials for External Identity Federation

3.2.1. OpenID 2.0

3.2.1.1. Protocol Version

3.2.1.1.1. All Identity Providers and Relying Parties MUST support the OpenID 2.0 Authentication protocol as defined in http://openid.net/specs/openid-authentication-2_0.html

3.2.1.2. Attributes

3.2.1.2.1. All Identity Providers MUST support the OpenID 2.0 Attribute Exchange 1.0 protocol as defined in http://openid.net/specs/openid-attribute-exchange-1_0.html

3.2.1.2.2. Identity Providers MUST make attributes available using the following schema URLs from axschema.org:

- Base URL: http://axschema.org/
- Preferred username: http://axschema.org/namePerson/friendly
- First name: http://axschema.org/namePerson/first
- Last name: http://axschema.org/namePerson/last
- Full display name: http://axschema.org/namePerson
- Business email address: http://axschema.org/contact/email
- Business phone: http://axschema.org/contact/phone/business

3.2.2. OpenID Connect

3.2.2.1. Protocol Version

3.2.2.1.1. OpenID Connect Final Standard
All Identity Providers and Relying Parties MUST support the OpenID Connect final standard as defined by http://openid.net/connect

3.2.2.2. The MITRE OpenID Connect server supports the final version of the OpenID Connect protocol as defined by http://openid.net/connect Protocol Profile.
The MITRE OpenID Connect server will support the following flows and options

- Basic client profile (code flow) as defined by http://openid.net/specs/openid-connect-basic-1_0.html including:
  - Authorization Code flow
  - UserInfo Endpoint with "openid" schema
  - Asymmetrically signed id_token (with RSA)
- Additionally, the MITRE server supports the following optional components of OpenID Connect:
  - Asymmetrically signed Request Objects (via RSA)
  - Server keys published via JWK and X509
  - Access tokens signed with RSA by server
  - Dynamic client registration
  - Server discovery

3.2.2.3. Claims
The following claims are supported from the UserInfo Endpoint with semantics defined in http://openid.net/specs/openid-connect-messages-1_0.html

- user_id, guaranteed unique and stable per user
- name
- given_name
- family_name
- preferred_username
- email
- email_verified
- phone_number

3.3. White, Black and Grey Lists
The technical configuration accompanying implementation of White and Black list determinations made in accordance with this Trust Framework System Rules are noted in this section.

3.3.1. Grey List
No additional configuration is required for any Grey List site or service.

3.3.2. White Listed Identity Providers
White Listed Identity Providers have their Trust Root for OpenID 2.0 or Issuer for OpenID Connect reflected in the Relying Party.

3.3.3. White Listed Relying Parties
White Listed Relying Parties have their Trust Root for OpenID 2.0 and/or their Client ID for OpenID Connect configured in the Relying Party system.

[Commentary: When a Relying Party has provided a “Login With MITRE Button”, in effect that Relying Party has White Listed MITREid as an Identity Provider.]

3.3.4. Black Listed Identity Providers

Black Listed Identity Providers have their Trust Root for OpenID 2.0 or Issuer for OpenID Connect configured to be denied in Relying Party system.

3.3.5. Black Listed Relying Parties
Black Listed Relying Party's have their Trust Root for OpenID 2.0 and their redirect URI for OpenID Connect configured to be denied in the Relying Party system.

3.4. Information Security

3.4.1. Token Signing
All OpenID Connect and OAuth2 tokens MUST be signed with the public key of the Identity Provider that has issued the token.

3.4.2. JWK Discoverability
All public keys MUST be discoverable as per the JWT Web Key (JWK) specification.

3.5. Meta-Data Exchange

3.5.1. All OpenID 2.0 servers MUST be discoverable from the public internet using the Yadis protocol defined in OpenID 2.0

3.5.2. All OpenID Connect servers MUST be discoverable from the public internet using the Simple Web Discovery (SWD) and XRD/Webfinger protocols as defined in OpenID Connect.

3.5.3. All OpenID Connect servers MUST allow for manual registration of OpenID Connect clients.

3.5.4. All OpenID Connect servers SHOULD allow for dynamic client registration.

[Commentary: The purpose of using "SHOULD" in this rule is because in the specification the criteria is a "MAY" and this feature is not always implemented. However, we do favor its use.]

3.6. Event Logging

3.6.1. Identity Provider Event Logging
An Identity Provider MUST log the following events:

- User approves a site
- User logs in to an Identity Provider
- User uses an Identity Provider to log into a Relying Party
- User denies log in to a Relying Party
- User revokes access to a Relying Party

3.6.2. The System Operator shall maintain records of the Identity Provider log files related to MITRE Users and required under Section 3.6.1 in accordance with MITRE Records Management Procedure IM 4.3.1.1.

3.6.3. White Listed Relying Party Event Logging
A White Listed Relying Party MUST log the following events:

- User selects an Identity Provider to login to a Relying Party
- User uses an Identity Provider to login to a Relying Party
- User denies the authentication transaction

APPENDIX 1: GLOSSARY AND ACRONYMS

Glossary

- **Derived Federated Credential**: A credential derived from a Primary Credential identifying the User of a Primary Credential for purpose of federated login to a Relying Party system.
- **Identity Provider**: An Identity Provider is the role of a Party responsible for issuing Primary Credentials and/or Derived Federated Identity Credentials for Users.
- **MITRE External Identity Federation**: The MITREid Identity Provider and MITRE Relying Party sites as well as both Identity Providers and Relying Parties that are external to MITRE and issue or accept Derived Federated Credentials used or accepted by MITRE.
- **MITREid**: MITREid is the MITRE Party conducting the role of Identity Provider responsible for issuing OpenID 2.0 and/or OpenID Connect Derived Federated Credentials for Users who are MITRE personnel, in accordance with the User Authority for MITRE.
- **Onboard:** A process by which a Party joins a Federation and becomes bound by that Federation's system rules and/or Trust Framework, if applicable.
- **Party**: A legal entity that conducts a Role in accord with these Trust Framework System Rules.
- **Primary Credential**: Digital information issued by a User Authority to a User that authoritatively binds identity attributes about that User to a means of authentication possessed and controlled by that User.
  Relying Party: A Relying Party is the role of a Party who is a service provider that accepts or has accepted a Credential issued by an Identity Provider for the purpose of authenticating a User.
- **System Operator**: The System Operator is the role of a Party responsible for implementing and administering an Identity Federation.
- **User**: A User is a Party that is a single human being who authenticates to any system covered by this Trust Framework, either using a Primary or Derived Federated Credential.
- **User Authority**: A User Authority is the role of a Party responsible for the issuance of Primary Credentials to Users.

APPENDIX 2: LINKS TO REFERENCED TECHNICAL STANDARDS, SPECIFICATION AND PROTOCOLS

OpenID 2.0:
Authentication (core): http://openid.net/specs/openid-authentication-2_0.html
AX: http://openid.net/specs/openid-attribute-exchange-1_0.html
PAPE: http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html

OpenID Connect:
Basic client profile: http://openid.net/specs/openid-connect-basic-1_0.html
Messages (abstract structure): http://openid.net/specs/openid-connect-messages-1_0.html
Standard (http binding): http://openid.net/specs/openid-connect-standard-1_0.html
Discovery: http://openid.net/specs/openid-connect-discovery-1_0.html
Dynamic Client registration: http://openid.net/specs/openid-connect-registration-1_0.html

SWD: http://tools.ietf.org/html/draft-jones-simple-web-discovery

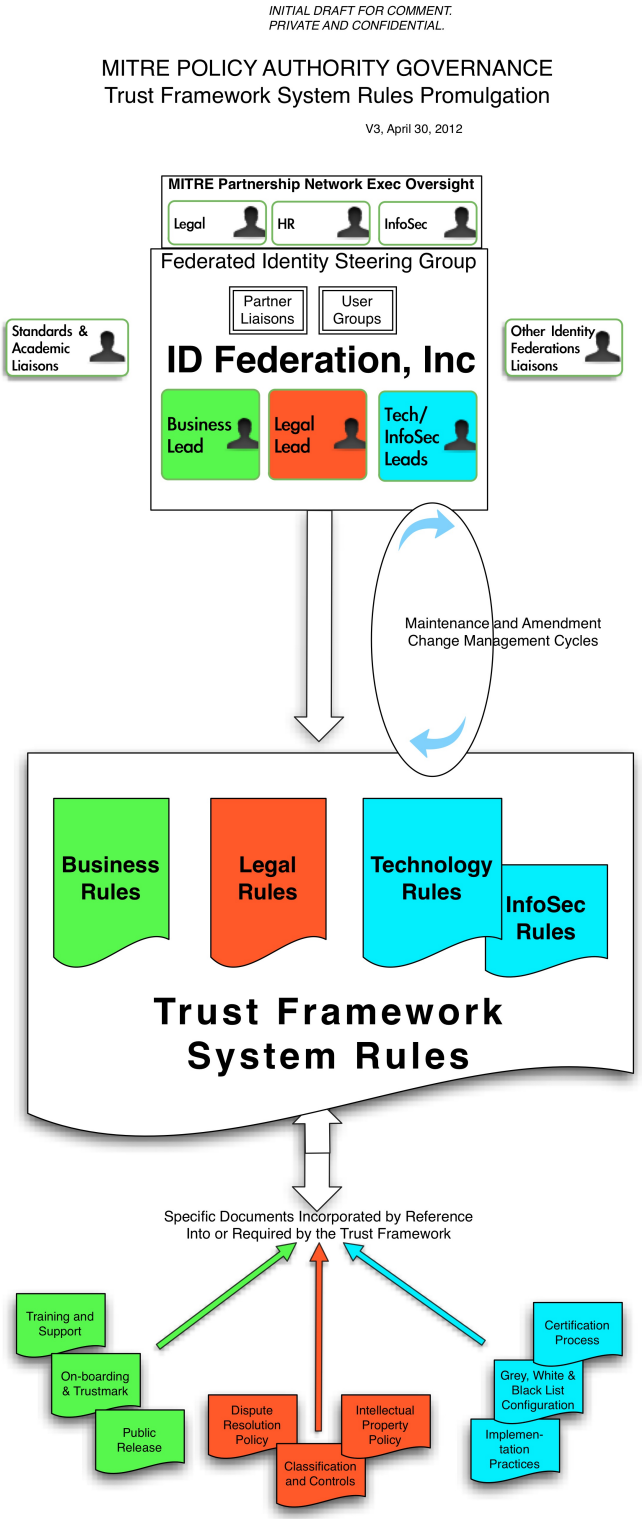
OAuth2:
Core: http://tools.ietf.org/html/draft-ietf-oauth-v2
Bearer: http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer

JSON Object Signing and Encryption:
JWT (tokens): http://tools.ietf.org/html/draft-ietf-oauth-json-web-token
JWS (signing): http://tools.ietf.org/html/draft-ietf-jose-json-web-signature
JWE (encryption): http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption
JWK (keys): http://tools.ietf.org/html/draft-ietf-jose-json-web-key
JWA (algorithms): http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms

Accompanying Documentation (Not Included Within or Referenced From Trust Framework)

Addendum 1. Governance

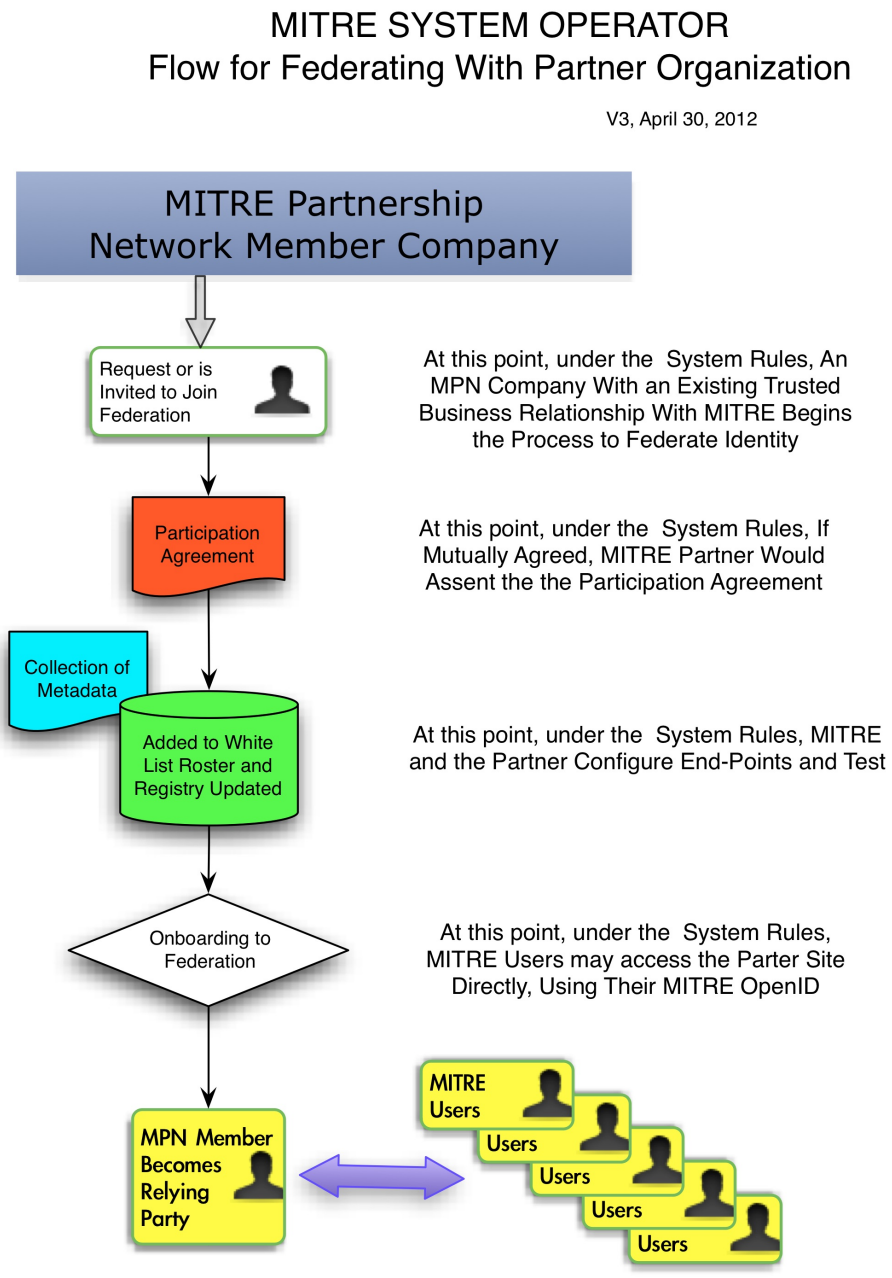
Below is an example of a possible flow for promulgation of the Trust Framework System Rules:



Addendum 2.A Operations: White Listing a Relying Party

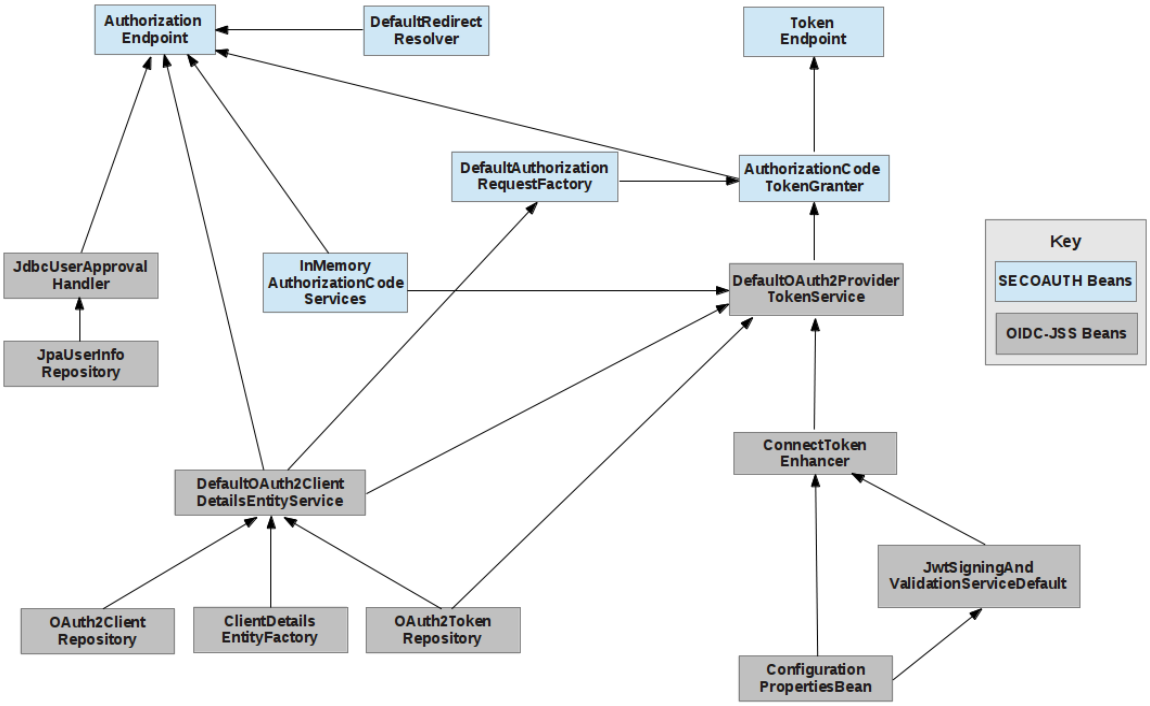
Below is an example of a possible flow for trusted MITRE partners to become "White Listed" federated identity Relying Parties:

INITIAL DRAFT FOR COMMENT.
PRIVATE AND CONFIDENTIAL.



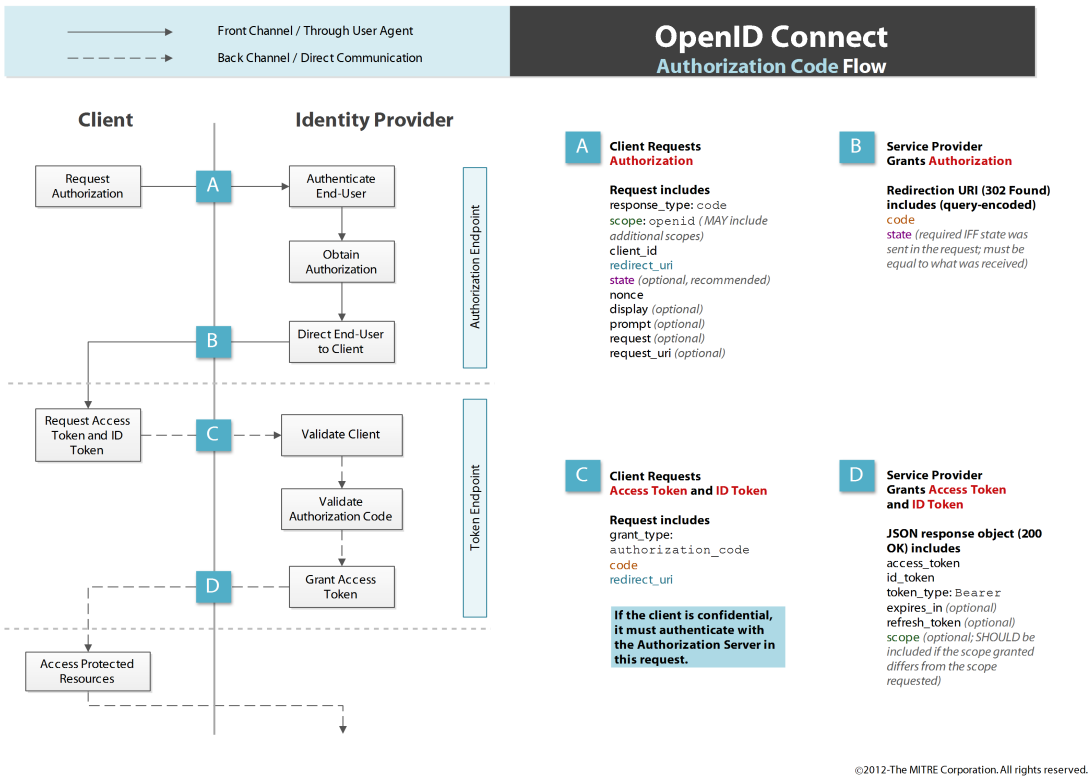
Addendum 2.B Technical Architecture

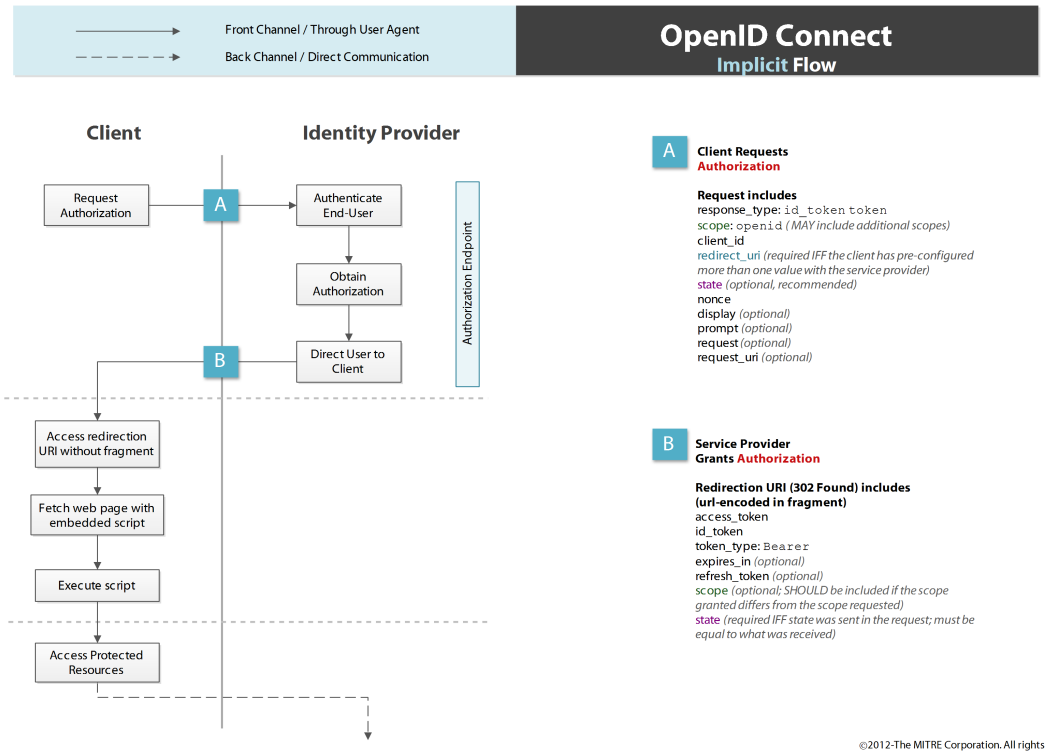
Below is an example of how the MITREid technical architecture could be depicted:

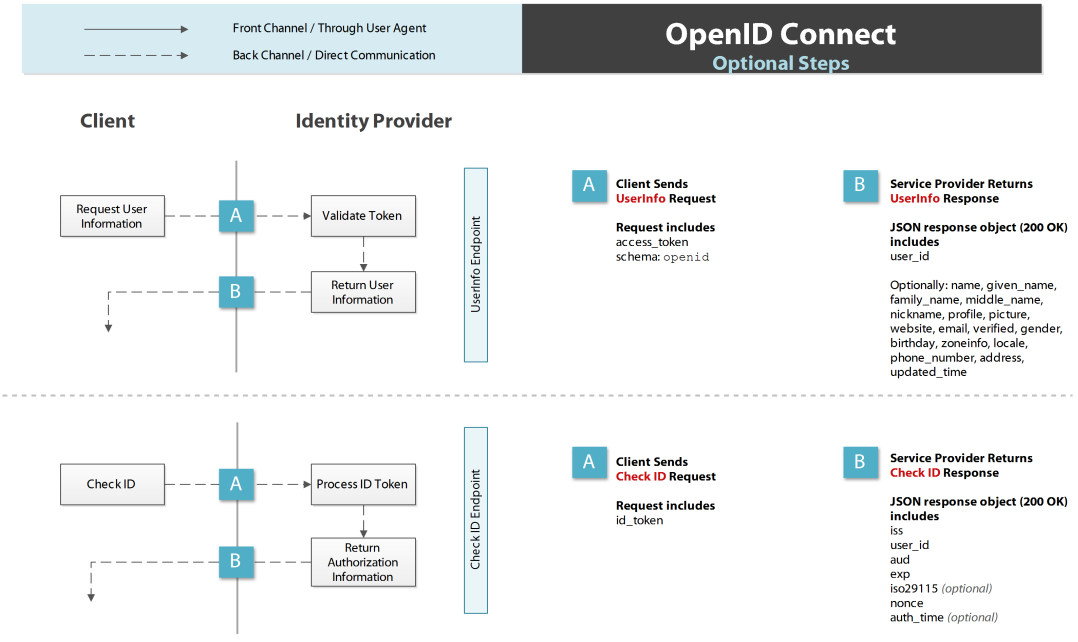


Addendum 2.C OpenID Connect Authorization Flow

The diagram below is included in the MITRE GitHub repository for OpenID Connect code:







Addendum 3: Current Directory Roster of Parties Conducting Roles Under This Trust Framework

Policy Authority

As of September 14, 2012, the Policy Authority is MITRE Corporate Legal Office.

System Operator

As of September 14, 2012, the System Operator is MITRE Partnership Network team.

Identity Provider

As of September 14, 2012, the Identity Provider for Users that are current MITRE personnel is MITRE Partnership Network using MITREid. Primary Credentials are issued to current MITRE personnel in accordance with MITRE Human Resources applicable policies and procedures.

As of September 14, 2012, there is no authorized Identity Provider for non-MITRE personnel.

User Authority

As of September 14, 2012, the User Authority for MITRE personnel is the MITRE Corporation, operating in accordance with MITRE Human Resources guidance and policy.

As of September 14, 2012, there is no authorized User Authority for non-MITRE personnel.

As of September 14, 2012, the User Authority for CAC holders is the Defense Human Resource Activity of the United States Department of Defense.

Users

[Note User's here, including link to their respective end-point URLs]

Relying Parties

[Note Relying Parties here, to the extent they are known by logging, agreement or otherwise.]

Addendum 4: Potential MITREid Accreditation and Certification Approach

Certification of federated identity services is a common method for both Identity Providers and Relying Parties to determine or help determine which other parties' services to accept or rely upon. FICAM policies define certification of federated identity services for federal government use (see: http://www.idmanagement.gov/pages.cfm/page/ICAM) and the National Strategy for Trusted Identities in Cyberspace (aka NSTIC) has led to several federally funded pilots and an Identity Ecosystem Steering Group that are leading toward a national public sector and privacy sector approach to federated identity services certification (see: http://www.idecosystem.org/). In addition, it is expected that eventually, federal agencies will be required to accept externally issued identity credentials for login to agency websites and certification plays a key role in that initiative. At this time, however, given the MITRE-enterprise centric scope and research prototype nature of the MITREid and MITRE External Identity Federation services, it is premature to speculate on the appropriate role or weight to apply to certification. However, it is clear that certification is likely to be a constrictive and expected aspect of use or acceptance of identity federation in the future, and so at this time MITRE is pursuing FICAM recognized certification of its OpenID 2.0 service via a Kantara accredited assessor and this draft Trust Framework System Rules document anticipates certification of external Identity Providers or Relying Parties as a factor in the White List decision by MITRE System Operator.

Potential criteria when assessing certification for an external Identity Provider for use by MITRE Relying Party sites might include:

- External OpenID 2.0 servers should make available attributes with the same set of schema URLs and semantics
- External OpenID 2.0 servers must comply with the OpenID 2.0 Authentication Protocol OpenID 2.0 (defined at http://openid.net/specs/openid-authentication-2_0.html)
- External OpenID Connect servers must support the final version of the OpenID Connect protocol as adopted by the working group
- External OpenID Connect servers must support the Basic Client profile
- External OpenID Connect servers should support at least the same set of claims noted in Section 3.2 of the Trust Framework System Rules.

Determination of which Certification Assessors may be sufficient to determine or recommend certification should follow further discussion and agreement about the potential role and weight certification will receive for purposes of MITRE External Identity Federation.