2024 InCommon Federation Proxies Working Group Report

Repository ID: TI.xxx.x
Persistent URL: <TBD>
Sponsor: InCommon Technical Advisory Committee (TAC)
Published: January 30, 2025; community consultation draft

Editors:

Gray Hudgens, University of Florida*; https://orcid.org/0009-0009-4502-9396*
Derek Eiler, *Nevada System of Higher Education; https://orcid.org/0009-0008-4587-4218*
Amanda Ferrante, *EBSCO*; *https://orcid.org/0009-0008-9960-1776*
Mark Rank, *Cirrus Identity; https://orcid.org/0000-0001-8930-9247*
David Walker, *Independent; https://orcid.org/0000-0003-2540-0644*
Warren Anderson, LIGO;
Albert Wu, *Internet2; https://orcid.org/0000-0001-7570-0923*

with contributions from Tom Barton

Subject Tags:
InCommon, federation, federation proxy, trust framework

Content

Executive Summary

The Federation Proxies Working Group aims to clarify the role of Federation Proxies (FPs) and their impacts on the federation trust model.

1. **Definition of Roles and Responsibilities**:
    - FPs introduce complexity by redistributing traditional roles in federations.
    - The FP Operator bears responsibilities like SP discoverability and facilitating trust and collaboration between entities.
    - FP Operators must maintain accurate and transparent contact and operational practices to prevent delays and miscommunication.
2. **FP Capabilities and Trust Impact**:
    - **Infrastructure Proxies** focus on static, low-impact tasks like protocol translation or RP integration.
    - **Community Proxies** handle more complex operations, including identity augmentation and trust framework extensions, with a higher impact on federation trust.
3. **Guidance for FP Operators**:
    - Maintain alignment with InCommon policies and good-standing membership.
    - Implement transparent practices by documenting proxy operations, expected attributes, and protocol translations in public URLs.
    - Follow privacy and security standards (e.g., SIRTFI, HECVAT) and coordinate incident response.
4. **Recommendations for InCommon Federation**:
    - Update federation policies to account for FPs as unique actors.
    - Mandate FP self-identification and publication of proxy practices.
    - Develop specific policy guidance for Infrastructure and Community Proxy operations.
    - Enable explicit support for FPs in the Federation Manager tool while maintaining the current practices of distinct SP and IdP EntityIDs – possibly requiring that the FQDN portion of the EntityIDs match.
5. **Next Steps for the Federation Community**:
    - Evaluate existing FPs against the Infrastructure-Community Proxy continuum.
    - Engage Community Proxy operators for further insights.
    - Explore inter-federation implications and impacts of emerging technologies like verifiable credentials.

Introduction

The Federation Proxies working group has been working to further the understanding of proxies currently deployed in the InCommon Trust Federation and propose recommendations for deployments going forward.

Federation proxies are a complex topic, as they are active elements in the middle of the exchange of identity information between entities (IdPs and SPs), thereby having the ability to observe and modify that information. While this collection of "proxied" entities should have autonomy for their internal operation, it falls to the FP operator, as these entities' representative, to uphold federation policy in situations involving the federation. Prescriptive changes to federation practice or policy would necessarily require the input of stakeholders from a variety of perspectives, including IdP operators, proxied entity operators, FP operators, federated service stakeholders, and of course Federation Operators such as InCommon.

From prior efforts, successfully developing and delivering policy guidance around FPs "… will likely require communications strategies that reach beyond InCommon's common focus of central IT organizations to researchers, libraries, and other academic functions and disciplines."

The stated goals were to:

- Review the insights and recommendations in TAC's "Formalizing the Role of Federation Proxies within the InCommon Federation" report **[FR]**, including relevant details from the Authentication and Authorisation for Research and Collaboration (AARC) Blueprint Architecture.
- Draft a "more precise vocabulary for articulating major concepts, components, and interactions" for FPs per recommendations in **[FR]**.
- Draft a "Federation Proxy Practices Statement" that addresses the key elements from the 2023 work.
- Seek a variety of FP perspectives, e.g. operators and managers of Virtual Organizations (VOs), library services, and hub-and-spoke Identity Providers (IdPs).

Glossary

Relying Party (RP). An entity that relies upon a verifier's assertion of a subscriber's identity, typically to process a transaction or grant access to information or a system **[NIST-800-63C-4].** In a lot of SAML environments, this would be referred to as a "Service Provider," but as this space grows to more than just SAML, we are going to stick to terms that are used more broadly, and are covered by NIST definitions.

Federation Proxy (FP). A component that acts as a logical RP to a set of IdPs and a logical IdP to a set of RPs, bridging the two systems with a single component. These are sometimes referred to as "brokers." **[NIST-800-63C-4]**

Federation Proxy Operator. The organizational entity that is responsible to the federation for a Federation Proxy. Note that the entity providing technical/operational support of the proxy may not be the Federation Proxy Operator, rather its services may have been contracted by the Federation Proxy Operator.

Service Provider (SP). As touched on with Relying Parties, this term has different meanings, depending on context. For this paper, we will be sticking to the following: A technology-based entity that provides services within a federation.

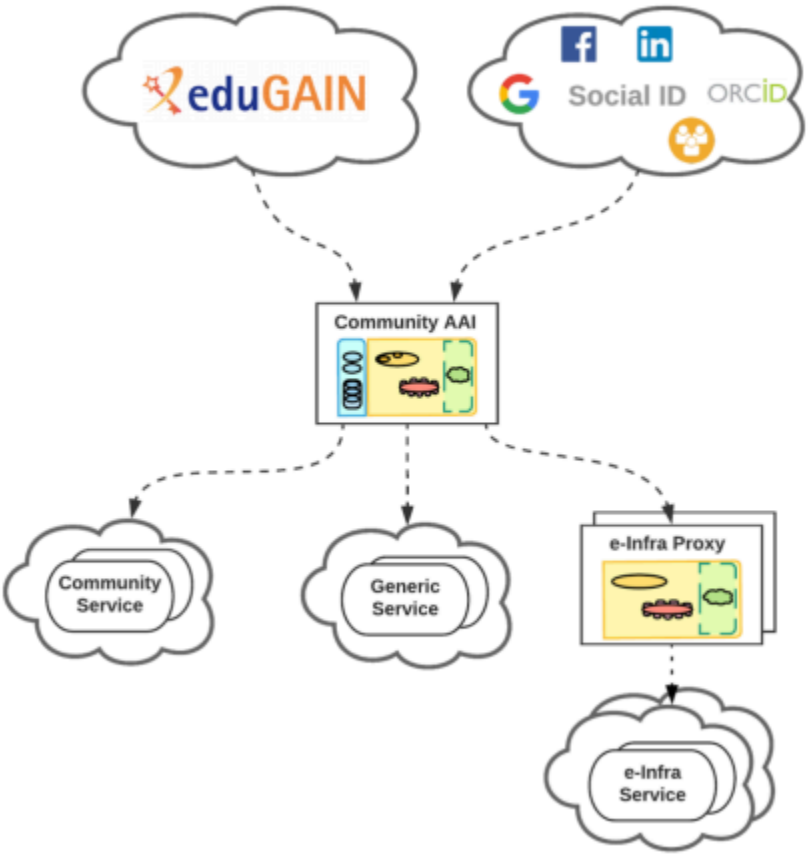
About Federation Proxies

An overview of Federation Proxy categories

Section 2.2 of the AARC Blueprint **[AARC-BLUEPRINT]** outlines two broad categories of use for Federation Proxies (FP) within the larger architectural patterns discussed by the Blueprint: Infrastructure and Community.

We summarize and compare the functions of these two FP categories in **Table 1** below. These categories are not absolutes but are generalizations that exist on a continuum. What was once an Infrastructure Proxy may develop into a Community Proxy over time as its constituent services evolve to meet the needs of its end-user community.

Visual representation of Federation Proxies (Fig 2.3 of [AARC-BLUEPRINT])



For this report, the additional elements working with the Federation Proxy will not be discussed. While those elements are important, that level of detail isn't needed for this discussion. Also out of scope for this discussion are the additional issues raised when authentication proxy functionality is combined with other types of technology such as firewalls, networking appliances, or virtualization tools.

Distinguishing Capabilities of Federation Proxies

The long list of Federation Proxy features can be lined up along a trust impact continuum. On one end, features have a low impact on the Federation's trust model. These are typically static translation or simplification features to help RPs simplify their participation in the Federation. On the other end are features performing sophisticated (complex) policy and

data embellishment that if not properly implemented and managed, erode trust in the Federation. **Table 1** lists common Federation Proxy features and their impact on Federation Trust.

Table 1. Federation Proxy Features and Their Impact on Trust

The following table lists typical features of a Federation Proxy. They are grouped according to each feature's impact on a federation's ability to maintain trust given today's policies.

Federation Proxy Features	**Impact on Trust**
Protocol Translation such as from SAML to OIDC, or SAML to CAS, where there is straightforward one-to-one semantic mapping.	Low
Protocol Translation of sensitive assertions such as identity proofing, authentication context, etc., where protocols vary significantly in semantics, for example, SAML AuthnContext vs. OIDC Authentication Methods References (amr) values.	Complex
Multilateral Federation Interop: Consume/parse metadata aggregate for an RP that is unable to parse metadata aggregate.	Low
Multilateral Federation Interop: support sign-ins from multiple IdPs - enables an RP only capable of supporting one IdP to work with multiple IdPs.	Low
Provide IdP discovery / a uniform discovery interface for RPs.	Low
Adapt cryptographic controls between FP and target RPs[1], for example: 1. Accommodate signing or encryption requirements for individual RPs that differ from the SAML V2.0 Deployment Profile for Federation Interoperability **[SAML-Interop]**	Low

[1] It is assumed both the FP Operator is making informed security decisions in a transparent fashion related to any accommodations for RPs, and traffic between the FP and target RP is minimally protected with transport layer security (TLS).

2. Accommodate RPs that do not support SAML V2.0 cryptographic methods	
Enforcing security controls on incoming IdP assertions such as: 1. MFA signaling 2. Required attributes 3. Enforcing acceptable cryptographic methods 4. Introducing trusted IdP metadata for target RPs 5. Scope-checking attributes	Low
Acting as a centralized Relying Party integration point for a dynamic group of incoming IdPs such as: 1. Abstract the configuration of target RPs from frequent changes when IdPs are added or removed. 2. Implement a uniform set of attributes, i.e., graceful error checking and handle missing values from IdP, e.g., turn a “null” into an empty string; or return an error response to IdP.	Low
Static Assertion Transformation or Remapping such as: 1. Remapping attributes, e.g. RP is a commercial product and cannot be configured to understand eduPerson. The FP performs that transformation. 2. Re-writing the authentication context based on asserted attribute signals, e.g., RP requires a different MFA signaling and cannot be configured to process REFEDS MFA signals. The FP performs that transformation. 3. Re-writing NameId based on asserted attribute signals. These actions enable static protocol bridging, connecting an RP that does not support InCommon interoperability specifications to the Federation.	Low

Policy-driven Assertion Transformation, Modification, Filtering, or Blocking depending on the IdP, RP, or end user based on external policy rules, e.g., a classic virtual organization operated federation proxy per AARC Blueprint **[AARC-BLUEPRINT]**.	Complex
"RP Aggregator" - register one entity in the federation to represent multiple RPs 1. All RPs are either directly operated or directly accountable for the operation via third-party agreement by the same organization as the entity's accountable party, but 2. RPs have different authentication, assurance, and attribute needs.	Low[2]
"RP Aggregator" - register one entity in the federation to represent multiple RPs 1. RPs are not all directly operated by the same organization as the entity's accountable party 2. Whether the RP accountable parties are InCommon participants matters here. More investigation on federation trust needed.	Complex
Data Injection with external attribute authorities, account linking, persona management, identifier minting, or others such as: 1. Establishing a persistent "community identity" where one doesn't exist 2. Elaborating the assertion based on externally stored persona data separate from the incoming IdP 3. Elaborating the assertion based on data collected during a linking or registration operation on "first use"	Complex
Triggering out-of-band business processes such as: 1. provisioning, 2. account linking, 3. embellishing identity/access information,	Complex

[2] The proxy needs to register one entity for each combination of authentication, assurance, and attribute needs, e.g., if the proxy represents two RPs, one requiring MFA and Personalized Access attributes, the other does not require MFA and is Anonymous Access, they need to register as two entities -> IdP makes authentication and attribute release decision based on entity. When you conflate multiple use cases, the IdP cannot take the appropriate action at sign-in time.

4. additional asynchronous end-user onboarding workflow In such a way that the RP does not see the original IdP assertions. It only sees the modified claims/assertions from the FP.	

There exists a continuum of capabilities for Federation Proxies:

- On one end are **Infrastructure Proxies** which exist to facilitate the inclusion of services into a federation. To do this, they have simple capabilities to interface their constituent services into interactions with IdPs of the federation. An infrastructure proxy "looks" like a Relying Party to the federation.
- On the other end are **Community Proxies** which exist to facilitate users' access to services. To do this, they have a set of capabilities to enhance the identity information provided by federation IdPs (and, potentially, non-federation IdPs, such as those provided by social networks) to enable access to constituent services. The facilitated services may be provided within the community, but may also be provided by others, including the federation. A community proxy "looks" like a Relying Party to the federation, but it may also look like an IdP when its community supports access to other federation Relying Parties.

The following sections provide greater detail on the extremes of the Federation Proxy continuum.

The Infrastructure Proxy Continuum Side

Infrastructure Proxies:

1. Possess limited low-impact Federation Proxy capabilities (see **Table 1**).
2. Apply technical changes only to an end-user assertion presented by a source Identity Provider (IdP) for a given audience of end users.
3. Maintain the semantic meaning of the assertion based on the information contained in the source IdP assertion, and the infrastructure context of the Infrastructure Proxy.

This Report recommends that implementations toward the Infrastructure Proxy side have the FP Operator also act as the operator, either directly or through binding agreements, of

the downstream SPs. This leads to a trust framework that spans both the FP and the target SPs.

For these reasons, the motivations for the InCommon Federation, and more specifically the Federation Operator, to be aware of Federation Proxies operating toward the Infrastructure Proxy extreme are **modest** and align to the following:

1. Enforcing the roles and responsibilities of the FP Operator.
2. Enforcing the FP Operator's InCommon Federation obligations to downstream SPs.
3. Encouraging the FP Operator to enumerate the full utility of all of the services that are exposed by the FP to the InCommon Federation.

The Community Proxy Continuum Side

A Federation Proxy operating toward the Community Proxy side aligns closely with the proxy element of a Community Authentication and Authorization Infrastructure (AAI) as defined by the AARC Blueprint **[AARC-BLUEPRINT]**. They operate both as technical elements and as business logic brokers to maintain an audience of end users by:

1. Possessing multiple Federation Proxy capabilities composed of both low-impact types and complex types (see **Table 1**).
2. Applying Federation Proxy capabilities to an end user assertion from a source Identity Provider (IdP) for a given audience of end users.
3. Changing the semantics of the source IdP assertion in ways that can be opaque without outside knowledge of the FP Operator practices.
4. Community Proxies also operate under more diverse trust frameworks as outlined in **Appendix A**.

For these reasons, the motivations for the InCommon Federation, and more specifically the Federation Operator, to be aware of Federation Proxies operating toward the Community Proxy side are **significant** and align to the following, some of which are the same as for the Infrastructure extreme:

1. Enforcing the roles and responsibilities of the FP Operator.
2. Enforcing the FP Operator's InCommon Federation obligations to downstream SPs.
3. Encouraging the FP Operator to enumerate the full utility of all of the services that are exposed by the FP to the InCommon Federation.
4. Encouraging the FP Operator to be transparent to the InCommon Federation about the operating practices of the FP.

5. Encouraging the FP Operator to be transparent to the InCommon Federation about the extent to which the operating practices of the FP Operator also apply to the SPs receiving assertions made by the FP.

Roles and responsibilities

Historically, the roles and responsibilities of the Federation Operator, Identity Provider, and Relying Party are well defined. However, introducing a Federation Proxy adds a layer of abstraction that shifts some roles to the FP Operator, or at the very least introduces opportunities for shared responsibility. Roles and responsibilities ascribed to the FP Operator will vary based on its functions and goals, such as whether it can be characterized as an Infrastructure Proxy or Community Proxy.

For example, the discoverability of available SPs is typically considered the responsibility of the Federation Operator first, with support from the SP's metadata. The direct relationship between the Federation and the SP allows for the fulfillment of this responsibility. However, the Federation does not know of an FP's downstream SPs which are not themselves members of the Federation. In this scenario, SP discoverability is a function that can only be fulfilled by the FP Operator.

Technical and security contact information for an SP or IdP is currently published via federation metadata and is discoverable via tools such as REFEDS MET[3]. When an SP or IdP is behind an FP, another layer of obfuscation, complication, and potential delay, is placed between relying parties in the federation, hindering cooperation and trust between federation subscribers. Therefore an FP Operator is obligated to maintain accurate contact information and potentially fill a coordinating role between its proxied SPs and IdPs. This is likely already being done by an FP Operator in the interest of maintaining their community or infrastructure. However, the Federation Operator, federated IdPs outside the FP's control, and end-users may be unaware that the FP Operator's published contact information is not the best point of contact for quickly resolving a trust incident with a proxied SP.

When an FP is in the mix, a lack of agreed-upon roles and responsibilities risks degraded experiences or services for all entities, including end-users. **Appendix B** attempts to articulate shifting roles and opportunities for shared responsibility when an FP is involved, from the perspective of the Federation Operator.

[3] https://met.refeds.org/

Guidance for Federation Proxies

The following are recommendations to Federation Proxy Operators and their Infrastructures and Communities under the overall principle that they should have autonomy "inside" their Infrastructures and Communities while aligning with trust-related federation policies and practices when interacting with "outside" federation participants.

Many of these recommendations have been chosen to align with international efforts, such as "Scalable Negotiator for a Community Trust Framework in Federated Infrastructures" (SNCTFI) **[SNCTFI-V1]** from the international AARC community. As these efforts evolve, it is expected that InCommon policy will also evolve to preserve that alignment.

Federation Proxy Operator General Operational Practices

1. Maintain InCommon Federation membership in good standing:
    a. Represent to the public federation the interests of proxy and associated private federation entities.
    b. Take action on public federation inquiries, policy changes, or enforcement actions.
    c. Be accountable to the public federation for the actions of the proxy and associated private federation entities.
2. Operate the proxy deployment, supporting systems, and private federation entities with due care to include:
    a. Make available attestation of privacy and security operating practices (either self-assessed or via third-party), for example, HECVAT, SOC2, or other recognized frameworks.
3. Apply the principles of **[SAML-Interop]** and other public federation practice guidance to public federation RP/IdP interfaces:
    a. To the extent practical, adopt said guidance for private federation entities.
4. Coordinate incident response with the public federation:
    a. Maintain an Incident Response procedure and regularly (at least annually) exercise the procedure.
    b. Adopt **[SIRTFI]**, "Security Incident Response Trust Framework for Federated Identity" (Sirtfi), and conduct routine exercises as part of internal Incident Response testing.
5. Ensure appropriate use of proxied information beyond the stated needs of the proxy and within the spirit of the InCommon Federation's policies and procedures.

Transparency of Practices

Each EntityID registered in the federation for an FP must provide its proxy practices in the document referenced by its <mdui:informationURL>. The following information must be published at this URL:

- Primary use/intended purpose of the proxy, e.g.:
    - Protocol translation from SAML to OIDC
    - Facilitation of access to community resources
- List of all downstream RPs accessible via the FP[4], including the following for each RP:
    - EntityID, human-readable name, and a brief description of the RP.
    - URLs pointing to any noteworthy data agreements between the IdP operator, proxy operator, and downstream RP operator.
    - Support contact information, if different than what is registered in the metadata for the FP itself.
    - Security contact information, if different than what is registered in the metadata for the FP itself.
    - Expected attributes to be consumed by this EntityID.
    - Expected attributes to be released by this EntityID.
- Any protocol translations performed by the FP, e.g. SAML to OIDC.

Registering Services

When registering new proxies/services to the federation, the FP Operator will follow these guidelines:

1. Establish separate federation entityID(s) per varying expectations/requirements of IdPs, so that all downstream RPs are matching. Each of these expectations/requirements should be included in the published metadata, using SAML standards.
    a. Differing authentication requirements. The FP may choose to enforce MFA based on varying security needs of the downstream RP being accessed, or

[4] Information about some RPs may be considered restricted or "need-to-know", e.g. to discourage bad actors outside the FP's community from enumerating internal resources of a sensitive nature. Some RPs may exist solely for administration or community management by the FP operator. In any such cases, it is still valuable for the Federation Operator to know how many RPs are downstream of the FP. Full disclosure for such RPs is optional, but we recommend erring on the side of disclosure.

perhaps due to varying compliance needs of IdP cohorts. REFEDS documents guidance **[REFEDS-MFA]** for how to request and respond with MFA.

b. Differing attribute expectations (including entity categories). When adhering to recommended privacy-preserving practices, an RP will signal support for the Personalized, Pseudonymous, or Anonymous entity category based on the attribute bundle required to deliver the platform's intended experience or functionality. In a scenario where an SP sells or provides access to products where different attribute bundles are required to support essentially differing functionality, then the SP must do so via multiple entityIDs. Similarly, when an FP is brokering access to downstream RPs where different attribute bundles are required to support essentially differing functionality, then the FP must do so via multiple entityIDs. REFEDS documents guidance **[REFEDS-EC]** for requesting and asserting various entity categories.

c. Differing assurance profile expectations/requirements. REFEDS documents guidance **[REFEDS-ASSURANCE]** for requesting and meeting different assurance requirements.

d. Differing expectations for signing and encryption.

2. Each registered entityID will have its own Proxy Practices Information URL in the published metadata. More detailed information about the Proxy Practices Information URL is found in the **Transparency of Practices** section.

User Attribute Management

The FP Operator should follow these practices concerning user attributes.

- Registered EntityIDs should include the full list of requested attributes that can or must be used.
- If the proxy performs attribute manipulation for transmission to downstream RPs, a summary of this manipulation should be published at the Proxy Practices Information URL. More detailed information about the Proxy Practices Information URL is found in the **Transparency of Practices** section.

Protocol Translation

Any protocol translation (examples: SAML to OIDC or SAML to CAS) should be documented at the Proxy Practices Information URL. More detailed information about the Proxy Practices Information URL is found in the **Transparency of Practices** section.

Recommendations for InCommon Federation Operator

The Working Group recommends that InCommon take the following actions to address the reality that a Federation Proxy is a distinct actor with a unique impact on the federation trust model and federation operations.

1. Promulgate best practices for the operation of Federation Proxies (FPs), particularly those from the AARC.
    a. Document and promulgate any InCommon-specific interpretations and extensions of those best practices.
2. To avoid dilution of InCommon's current trust-related policies, establish policy guardrails for the operation of FPs, particularly those included in this report for Community and Infrastructure Proxy Operators and the members of their Communities and Infrastructures.
3. To clearly identify/account for FP deployments in the Federation:
    a. Require federation participants to self-identify as FPs based on published criteria. This identification should become an element of policy. Refer to **Appendix B** for a simple self-identification test.
    b. Require FP operators to publish metadata such that the <mdui:InformationURL> points to a public webpage that includes the information detailed in the **Transparency of Practices** section of this report.
    c. Provide a capability in InCommon Federation Manager allowing an FP Operator to register both RP and IdP metadata; and associate them with each other as components of an FP.
4. Revise **[InC-TRUST]** to reflect the reality of Federation Proxies. That is, introduce the Federation Proxy as an actor in the InCommon trust model. Refer to **Appendix A**.

Recommended Next Steps for the Federation Community

We recommend the InCommon Federation community, via future Working Groups, continue addressing the impact of Federation Proxies by addressing the following areas.

- Benchmark known FP deployments against the FP continuum described in this report.
- Open call for FP Operators on the Community Proxy end of the FP continuum to participate in further work.
- Interfederation considerations.
- Impacts of other federation technologies, e.g. verifiable credentials.

References

[AARC-BLUEPRINT] Evolution of the AARC Blueprint Architecture
https://aarc-community.org/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf

[FR] Formalizing the Role of Federation Proxies within the InCommon Federation
http://doi.org/10.26869/TI.169.1

[InC-TRUST] Trusted Relationships for Access Management: The InCommon Model
http://doi.org/10.26869/TI.3.2

[NIST-800-63C-4] Digital Identity Guidelines - Federation and Assertions
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.2pd.pdf

[REFEDS-MFA] REFEDS Multifactor Authentication Profile
https://refeds.org/profile/mfa

[REFEDS-EC] Entity Categories
https://wiki.refeds.org/display/ENT/Entity-Categories+Home

[REFEDS-ASSURANCE] REFEDS Assurance Framework
https://wiki.refeds.org/display/ASS/Assurance+Home

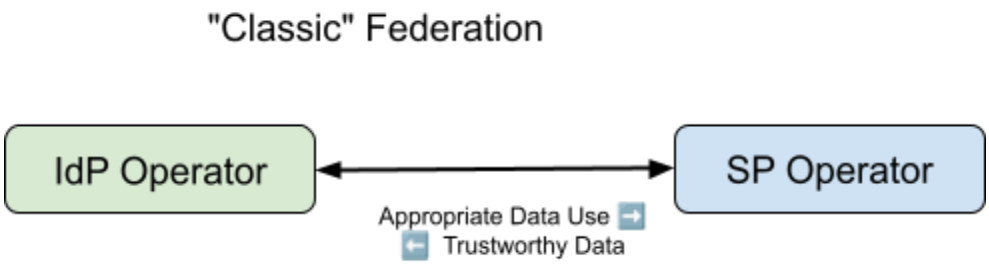
[SAML-Interop] SAML V2.0 Implementation Profile for Federation Interoperability
https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html

[SNCTFI-V1] Scalable Negotiator for a Community Trust Framework in Federated Infrastructures(Snctfi)
https://aarc-community.org/wp-content/uploads/2017/07/Snctfi-v1.0.pdf

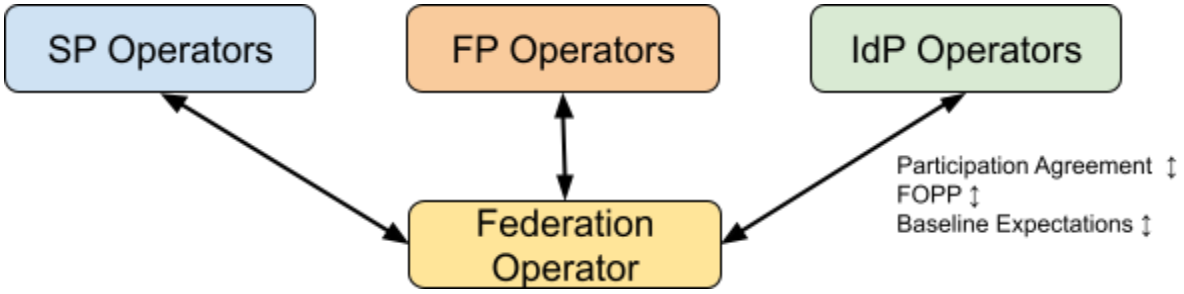
[SIRTFI] Security Incident Response Trust Framework for Federated Identity (Sirtfi)
https://refeds.org/sirtfi

Appendix A: How Federation Proxies Change the InCommon Trust Model

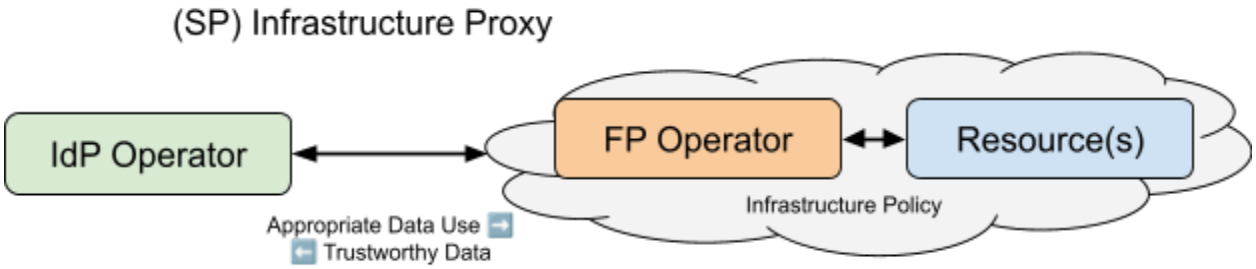
As described in Trusted Relationships for Access Management: The InCommon Model **[InC-TRUST]**, there are two trust relationships regarding the exchange of identity information between the federation participants operating an IdP and an SP:



The SP Operator trusts the IdP Operator to provide trustworthy data, and the IdP Operator trusts the SP Operator not to misuse the data it receives. There are also trust relationships between both IdP and SP Operators and the Federation Operator to ensure the trustworthiness of information about the IdP and SP (*e.g.*, service endpoints, public keys, certifications earned, organizational contacts, *etc*.)

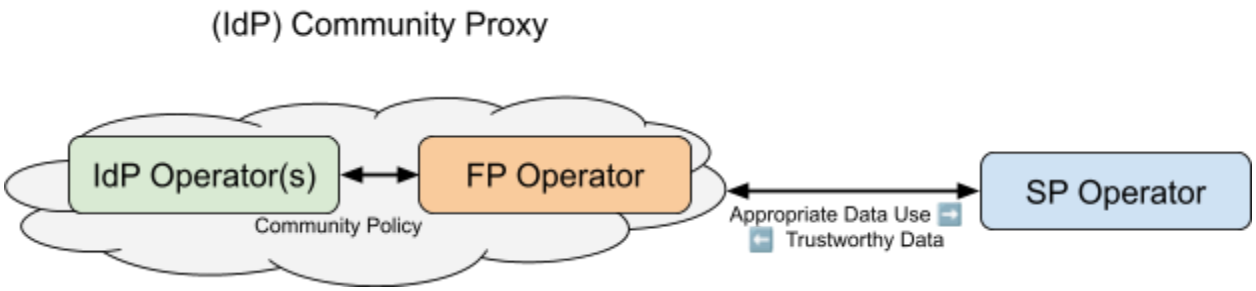


The introduction of federation proxies modifies these trust relationships in the following ways. The required federation trust remains the same, but there are additional actors participating in the exchange.



An Infrastructure Proxy enables access to services within the Infrastructure from a federation IdP's user community. As mediated by its FP, the Infrastructure must support the same trust relationships as an SP in a classic federation.

Analogously, a Community Proxy enables one or more user communities to access federation SPs (and/or services within a federated Infrastructure).



In this case, the Community, mediated by its FP, must support the same trust relationships as an IdP in a classic federation.

So, nothing new?

Well, no. The issue is that Infrastructures and Communities cannot always be assumed to be within a single management domain (presumably the operator of the FP). When it is, we can fall back to the classic federation model, however…

When differing policies govern multiple management domains, the Federation Operator's policies and processes for ensuring the trustworthiness of the information it provides to IdP and SP Operators must be modified to address the potential complexity within Infrastructures and Communities. This report recommends the first steps for doing that.

Appendix B: Roles and Responsibilities of a Federation Proxy

Capability	Federation Operator	SP Behind the Proxy	IdP	Federation Proxy	Notes
Central WAYF service	X			X	The ideal centralized Where Are You From (WAYF) user experience could be influenced by: 1. Guidance provided by the Federation Operator, and 2. Core functions provided by the Community Proxy, such as a central UI and UX for a consistent access point to downstream SPs.
SP discovery	X			X	In specific scenarios, this function can only be fulfilled by the FP. Examples: 1. The SPs downstream of the Federation Proxy are not members of the originating Federation. 2. The target SPs don't support discovery. 3. There is a mix of protocols in play and the Federation Proxy is facilitating access.
Test infrastructure/service	X			X	If the SPs downstream of the Federation Proxy are not members of the originating Federation, then this function can only be fulfilled by the Federation Proxy.

Collecting, processing, validating and publishing metadata	X			X	If the SPs behind the FP are not in the federation, then this responsibility can only be fulfilled by the FP, as it pertains to those SPs.
Readiness guidance and enforcement	X			X	Is a federation responsible for defining “FP readiness,” and FP defines readiness for mediated SPs?
Define, support and enforce attribute release entity categories	X			X	This document specifically references entity categories, known to the InCommon community, that request the release of a given attribute bundle from the IdP. The FP should assert membership with a specific attribute release entity category based on the needs of its downstream SPs. In a scenario where SPs behind an FP require varying attribute bundles, the FP may consider using distinct entityIDs.
End-user support	X	X	X	X	End-user support and incident response become more complex with there is a Federation Proxy element. Depending on the operational practices of the FP Operator, some or all of the user support/incident response functions typically handled by the SP Operator may be delegated to the FP Operator.
Security incident response	X	X	X	X	The FP is responsible for some data in transit and at rest. If data is being transmitted to downstream SPs, then it’s

					recommended for FP to be involved in incident response.
Comply with laws and regulations relevant to their community		X	X	X	Entities that transmit, collect, and/or store specific classes of data have responsibilities based on their community and/or region. Specific details, such as regulatory or legal compliance requirements, are outside the scope of this document.
Manage identities, including local accounts		X	X	X	Whether the FP manages local accounts has implications for some other roles and responsibilities. If the FP creates and stores local accounts, they are likely to want to pay more attention to incident response, compliance, etc.
Authenticate community member			X		The FP does not authenticate the community members.
Attribute release and assertion			X	X	The assertion with the associated released attributes originates with the IdP. Depending on the FP deployment, there may be an assertion by the FP that is materially different from the IdP.