InCommon Federation's Comments on NIST 800-63C Federation and Assertions

August 10, 2020

Table of Contents

Contacts for this Document

Janemarie Duh

Albert Wu

Tom Barton

Heather Flannigan

Ann West

General Comments

Comments in this section bear on 800-63c in its entirety or to substantial sections of it.

On the context of 800-63C and the nature of research and education multilateral federations

“Federation”, as described in 800-63C, seems to assume a bilateral, consumer-to-business (C2B) relationship where an IdP and a RP negotiate registration and connection with one another directly without a 3rd party facilitating a scaled out, n-to-n relationship. In this model, a Subscriber (user, person, customer, consumer, subject, principal) has a direct relationship with an RP by virtue of their status as a citizen. The Subscriber has complete control over the release of his/her information. An organization operates an RP and must either meet substantial compliance obligations or needs to mitigate the risk to a Subscriber of their sensitive personal information being misused. An IdP is only a technical platform a Subscriber uses to authenticate and access an RP. There appears to be assumption that there would be a very small number of commercial IdPs fulfilling this role.

This bilateral, C2B relationship does not accurately capture the more nuanced real-world interactions observed in multilateral federations deployments commonly found across national federations in 68 countries. R&E federations from these countries are joined into a global federation supporting the Research & Education (R&E) sector. In today’s R&E federations, each IdP is operated as part of an organization’s enterprise services and represents the people associated with that organization (e.g., its employees, students, and affiliates). RPs provide services needed by those people in pursuit of their relationship with the organization operating the IdP, e.g., doing their job or pursuing a degree. There are substantial business to business (B2B) implications. For example, the IdP-operating organization may have certain decision powers over the release of a person’s information to an RP because of data protection regulation, organizational policy, or contractual obligations. GDPR recognizes this distinction; 800-63C should, too.

The nature of a B2B, multilateral federation means standards embraced by such an ecosystem must scale to a large number of IdP-operating organizations. InCommon alone has over 560 registered IdPs. Globally, there are over 1,200 IdPs in the eduGAIN inter-federation. We believe that the NIST digital identity standards can potentially help R&E federations further improve trust and interoperability among participants. Given the close collaborative relationship between government and the R&E community, we certainly believe that it is imperative that any federal digital identity standards be implementable in the R&E sector. It is worth noting that this B2B multilateral federation model also appears in other industry verticals.

Alas, some of the requirements of a federation under 800-63C, to be born either by the Federation Authority or by its members, are costly and result in keeping the number of IdPs in a federation comparatively small. We urge 800-63C to be updated to accommodate

implementation complexity and cost considerations where federations need to scale to include large numbers of IdP-operating organizations, often organizations in many different countries.

Further, in a multilateral federation, a federation operator plays a significant role in ensuring scalable trust among participants. While 800-63C defines the concept of a Federation Authority, it does not capture all the activities of a federation operator. We urge the 800-63C authors to engage federation operators to define a federation operator's roles and responsibilities in the revision.

Finally, it is not clear whether one set of requirements can effectively address both the C2B and B2B interactions in federation. Perhaps there needs to be separate C2B and B2B editions of 800-6363C or sections added to the existing guidelines that address one or the other.

Federated Security Incident Response

Although IdPs are required by 800-63C to meet stringent security requirements, none are placed specifically on RPs. Moreover, there is no recognition of the need for security incident response procedures to function adequately in a federated context. A breach at one RP might be traced to a compromised credential at an IdP, which in turn might have been used to compromise other RPs. RPs should meet operational security requirements sufficient to enable their reasonable participation in security incident response beyond the confines of the organization operating the RP, and similarly for IdPs. Further, members of a federation should share an obligation to notify others of incidents that have a federation component and to participate in a coordinated response to such incidents. The IETF Security Events working group are developing standards for automated sharing of certain security information designed to support this need, and REFEDS has developed the SIRTFI Trust Framework, which addresses operational readiness and obligation to participate in federated security incident response.

Normative text is ambiguous

Multiple sections noted as "normative" in 800-63C contain ambiguous language that can lead to inconsistent, incompatible, possibly insecure implementations. At the same time, certain references to external requirements make implementations very challenging for agencies outside the federal government. Examples of this ambiguity can be found in our feedback on specific sections below. See comments in:

- Section 4: Federation Assurance Level (FAL)
- Section 4.2: Runtime Decisions
- Section 5.1: Federation Models
- Section 5.1.4: Proxied Federation
- Section 7: Assertion Presentation
- Sections 7.3 and 9.3

Build on Existing Standards or Profiles

Some of the requirements of IdPs or RPs in 63c might well be addressed by following established industry standards or profiles. This would both reinforce their consistent adoption and reduce the burden on 63c to some degree. Several examples, for SAML federations, are the SAML V2.0 Implementation Profile for Federation Interoperability and the SAML V2.0 Deployment Profile for Federation Interoperability, both published by the Kantara Initiative, and the SAML V2.0 Subject Identifier Attributes Profile Version 1.0 published by OASIS.

Socially Sensitive Terminology

Use alternatives to “whitelist” and “blacklist” such “allow list” and “block list” throughout.

Specific Comments

Comments in this section are in reference to specifically cited material.

Section 4: Federation Assurance Level (FAL)

RP should have security obligations as well as IdP

Regarding the last paragraph in section 4:

> *Additionally, the IdP SHALL employ appropriately-tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.*

This paragraph requires IdPs to meet certain security standards but is silent on any corresponding need for RPs. If the RPs countenanced in 63c are strictly those operated by federal agencies, then it may be reasonable to assume this happens by adherence to other requirements imposed on RPs. But for use outside of the federal government, any assumption of security practice by RPs must be explicitly stated. Alternatively, since a privacy risk assessment might be expected to produce conclusions about security measures necessary to meet privacy objectives, consider making an explicit requirement that the privacy risk assessments required of RPs produce identified security standards that must be met.

Definition is vague and difficult to consistently implement

While the FAL definitions in Section 4 appear straightforward on the surface, it goes on to state:

> *… the IdP SHALL employ appropriately-tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.*

That statement makes implementation impractical outside the federal government. There is no reference to what constitutes a qualified “industry standard”. This ambiguity is inconsistent with normative sections found in other 800-63 volumes, where definitions tend to be much more explicit.

Section 4.2: Runtime Decisions

Missing/ ambiguous requirements and definitions

Regarding the following sentence:

> *All RPs in an IdP’s whitelist SHALL abide by the provisions and requirements in the SP 800-63 suite.*

800-63A and 63B only address functions performed by IdPs. It is not clear from this sentence what requirements an RP must fulfill in order to qualify.

Regarding this statement:

> *“Every RP not on a whitelist or a blacklist SHALL be placed by default in a gray area where runtime authorization decisions will be made by an authorized party, usually the subscriber.”*

We are not clear what this sentence means. Also, there does not appear to be a definition for “authorized party” in 800-63C.

If this statement were to be applied to today’s R&E multilateral federations, “authorized party” could be interpreted as the organization operating the IdP, who the Subscriber (Subject, Principal) is affiliated with and accesses an RP within the context of their affiliation with that organization. Also, GDPR has expressly stated principles in this area. In any event, it is important to clarify “authorized party” when used in a normative section.

Regarding this sentence:

> *“All IdPs in an RP’s whitelist SHALL abide by the provisions and requirements in the 800-63 suite.”*

This doesn't clarify which requirements (and at what level) an IdP must meet. Further, it seems unclear who has decision rights to set these requirements. Requiring an IdP to have to abide by requirements unilaterally set by an RP pose scaling and operational problems when there are numerous RPs operated by a vast number of organizations.

IdP discovery and selection is not always performed at the RP

The sentence:

> *"The RP MAY remember a subscriber's decision to authorize a given IdP, provided that the RP SHALL allow the subscriber to revoke such remembered access at a future time."*

fails to take into consideration that an IdP discovery mechanism may not be operated by the RP. Indeed, InCommon, as well as a number of multilateral R&E federations around the world, operate IdP discovery services on the behalf of its participants. This is one of the areas in 800-63C where it fails to account for the needs found in multilateral federations.

The Subscriber is not always the attribute release authority in B2B relationships

Regarding this sentence:

> *"If the protocol in use allows for optional attributes, the subscriber SHALL be given the option to decide whether to transmit those attributes to the RP".*

The Subscriber may not be the correct authority for deciding whether to release some attributes. An example: an RP providing services to a university may request certain optional user attributes from users using the university IdP to sign into the RP. The university may decide based on its data protection policy to block the release of optional attributes, overriding the Subscriber's preference. A Subscriber should only have discretion to suppress optional attributes when there are no applicable policies overriding the individual preference.

Section 5.1: Federation Models

800-63C does not adequately account for multilateral federation model

Both the manual and dynamic models defined in this section are essentially bi-lateral in nature. Multilateral federation, the oldest and most widely deployed model of federation leveraging higher learning institution infrastructure to support global R&E collaboration use cases, fits neither model. This can be addressed by being less prescriptive of the means by which an IdP and an RP come into possession of each other's entity metadata or registration statements and how they come to trust subsequent transactions between them. Indeed, this is an area of active

innovation of federation technologies and policies, so it would be best for 63c to avoid normative reference to such mechanisms.

Ambiguous text in Normative Section

In 5.1.1 Manual Registration:

> *"Federation relationships SHALL establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship."*

It is unclear who exactly is responsible for establishing these parameters, and there is no corresponding statement in 5.1.2 Dynamic Registration. Perhaps this statement needs to be expanded to clarify roles and responsibilities, particularly when contrasting bilateral vs multilateral federation models and/or C2B relationship vs B2B relationship.

In addition, in R&E federations or similar B2B use cases, an IdP may support multiple constituencies and serve multiple missions. It need not apply the same identity proofing or credential management practices to all Subjects. Some Subjects, such as employees, have a higher quality of vetting and management, while others, such as guests, may have a lower standard applied, in line with the organization's assessment of its risks and purposes. The 63c requirement should recognize that the same level of IAL and AAL need not apply to all Subjects presented by an IdP.

In 5.1.2 Dynamic Registration:

> *"IdPs that support dynamic registration SHALL make their configuration information (such as dynamic registration endpoints) available in such a way as to minimize system administrator involvement."*

There are no testable requirements in this statement. This statement may belong in a non-normative section.

Section 5.1.4 Proxied Federation

More clarity needed for "Proxy"

The text in 5.1.4 provides a brief introduction of the term "proxy" as a technical architecture. It also alludes to a few vague "benefits" a proxy may offer. It doesn't, however, address real-word deployment implications. In practical deployments, the business model and the organization(s) operating the proxy relative to the IdP and/or RP it proxies have substantial impact on the requirements placed on a proxy, for example:

- A proxy may process/decorate authentication assertions sent by an IdP. It may also access user information sent by and IdP as it is transformed and forwarded to an RP. If

such a proxy is operated by a third party that is neither the IdP organization nor the RP organization, what are the security, privacy, and legal considerations/requirements?
- What is a proxy allowed to do when performing "technical integration" or "distribute communications"? What is it not allowed to do?
- How does an IdP trust an RP (and vice versa) if the transaction is being proxied by a third party? How do they trust the proxy?

If this remains a normative text, this section should be expanded to elaborate appropriate use and obligations of "proxy" based on, among other factors, the proxy-operating organization's relationship relative to the IdP and RP it proxies.

Section 5.2 Privacy Requirements

Regarding the statement:

> *"Federation involves the transfer of personal attributes from a third party that is not otherwise involved in a transaction — the IdP."*

This statement is false. Federation *may* involve transfer of personal info but need not. In the multilateral R&E federations, the IdP is most frequently a part of an element of an organization's enterprise services supporting the Subject's organization-related activities. There is not a "3rd party" in the transaction.

Section 6.3.1

Proxy and Third Party not well defined

Regarding the statement:

> *"The proxy SHALL NOT disclose the mapping between the pairwise pseudonymous identifier and any other identifiers to a third party or use the information for any purpose other than federated authentication, related fraud mitigation, to comply with law or legal process, or in the case of a specific user request for the information."*

Depending on how "proxy" and "third party" is defined in 800-63C (see response from Section 5.1.4 Proxied Federation), this statement may need adjusting. A large organization, such as a university, may operate a proxy to connect numerous services within the organization to the federation that are operated by a single organization. Alternatively, a number of different organizations undertaking a common purpose, e.g., Open Science Grid or the Laser Interferometer Gravitational-wave Observatory, may agree to share a single proxy. These use cases may introduce legitimate needs where a proxy needs to correlate identifiers. One source of information about real-world experience with proxies in the R&E sector is Federated Identity Management for Research Collaborations version 2.

Also, add security incident response as a permitted purpose, as was done in section 5.2.

Section 6.3.2 Pairwise Pseudonymous Identifier Generation

Regarding the sentence:

> *"They SHALL also be unguessable by a party having access to some information identifying the subscriber."*

This sentence may not belong in a normative section. While we agree with its intent, it is not clear how one measures "unguessable". We suggest focusing the requirement on characteristics of acceptable construction of pseudonymous identifiers, possibly leveraging existing standards such as the SAML V2.0 Subject Identifier Attributes Profile Version 1.0.

Section 7 Assertion Presentation

Regarding the statement:

> *"The IdP SHALL transmit only those attributes that were explicitly requested by the RP. RPs SHALL conduct a privacy risk assessment when determining which attributes to request."*

Be mindful of non-personal attributes

This requirement makes good sense when it is constrained to transmitting personal information, but privacy considerations are out of scope for attributes that do not describe a living human. IdPs can and do send non-person data during federated SSO, for example, an attribute conveying an IdP capability. Suggestion: clarify "attribute" meaning in 800-63C. If the concern is personal privacy, limit the statement's scope to personal data only.

The notion of requesting attributes is unclear

800-63C does not specify what constitutes an "explicit request" by an RP. There is no way for implementers to objectively measure compliance with this requirement.

For example, SAML defines a RequestedAttribute element in its schema. A SAML practitioner may easily infer this statement to mean that it requires a SAML RP to use the SAML RequestedAttribute element to perform this request. While the SAML RequestedAttribute mechanism helps systems automate attribute release configuration, it does not work at scale when data protection regulation, organizational data governance policies, and possibly contractual obligations intersect and are applied to real-world data release decision processes (see Attribute management in multilateral and/or federations) The text in section 7, as it reads today, can lead to unnecessary confusion and conflict during implementation.

R&E federations, including InCommon, have developed standards for bundled user data release using SAML entity attributes (REFEDS Research & Scholarship, commonly known as R&S Entity Category) to enable scaled and streamlined research access. The R&S entity category method does not make use of the SAML RequestedAttribute syntax. Although, since an RP must apply and qualify to be considered a part of the R&S category, this mechanism can be considered an "explicit request" from an RP.

We recommend that this section be updated to clarify how an RP or IdP might satisfy the "explicit requested" requirement.

Multilateral / B2B federations have complex attribute management needs

800-63C largely assumes a bilateral, consumer-to-business-style federation model. In this case, the text appears to imply that the IdP has no role other than to respond to an RP's request (and to execute the Subscriber's consent). In B2B federations, the Subject's home organization (and likely the IdP operator) has a significant role in determining what attributes are sent to an RP independent of an RP's request or a Subscriber's consent. A home organization entering into a business contract to use an RP's service may require certain attributes to be sent to the RP (e.g., for reporting and statistics tracking purposes). The home organization may also override a Subscriber's consent choice if they are using the RP to perform tasks as a part of their job function.

In particular, if the reader of 800-63C interprets the mention of "requested attribute", in the context of a SAML-based federation, to mean "use the SAML RequestedAttribute syntax", it would create an implementation conflict. In B2B federations, the IdP is the likely party to control what user information is released. Because of the complex user data ownership/stewardship/release rights described above, virtually no deployments within InCommon rely solely on the SAML RequestedAttribute syntax to determine user attribute release.

Further, in a multilateral federation, where there are numerous IdPs and RPs from different organizations, allowing an RP to unilaterally request attributes does not scale. There needs to be defined standard sets of attributes and valid conditions of use among participants. The REFEDS Research & Scholarship Entity Category is one such example.

Section 7.3 and Section 9.3

Ambiguous requirements in Normative sections

Regarding this statement in both sections:

> *"To support this RP requirement IdPs are, in turn, required to support attribute references."*

There are as yet no standard means for expressing a request for a function to be evaluated on a set of attributes and the result returned in lieu of the attributes on which the function is to be executed. Hence, each specific attribute reference that may be requested must have a definition that is shared across all federation participants as well as a defined means for presenting the result in an attribute assertion. Such things must exist before their use can be required.

One means by which this might be accomplished with existing technology is to establish one or more entity categories for this purpose. An entity category is essentially a defined practice that a federated transaction may follow, and entity category references are added to metadata or registration statements of the IdPs and/or RPs that implement the corresponding practices. An entity category can be used to define one or more specific attribute references (e.g., "is Subject at least 18 years of age (Y/N)?") as well as the manner by which the answer will be conveyed in an attribute assertion. RPs signal a request for certain attribute references by adding corresponding entity category references to their metadata or registration statements. Likewise, IdPs that support a given entity category signal their ability to execute its attribute references and provide results in the manner defined by the entity category by adding corresponding entity category references to their metadata or registration statements. In this manner a federation can establish specific attribute references that are supported and enable their use within federated transactions. Other means could be developed that are superior to this; it is offered as an illustration of what is needed before assessable requirements related to attribute references can be expressed.

About the InCommon Federation

Established in 2004 as part of Internet2's effort to establish trusted access to protected resources, InCommon Federation (InCommon) is a multilateral identity federation connecting over 10 million individuals across 770 participating universities, research collaborations, government departments, and commercial organizations. By championing standards development and adoption and supporting a diverse selection of software platforms, InCommon harnesses the identity and access management infrastructure investments made by hundreds of US higher learning institutions. Together, we enable researchers, teachers, and learners to collaborate and access online resources in a trusted and scalable manner.

Further, InCommon actively participates in the international R&E federation operator community (REFEDS) to develop and promote adoption of global trust and interoperability standards. It also

extends the value of InCommon participation by connecting participants to resources across 68 countries via the eduGAIN global inter-federation.

Much of our experience and best practice guidance aligns with NIST 800-63. Although there are significant gaps between the realities of academic identity federations and the guidance found in NIST 800-63C. In particular, the guidance often misses key issues experienced by multilateral federation operators. With that as background, we offer our feedback addressing these gaps found in NIST-800-63C. We further invite NIST to consult with InCommon and the broader global R&E federation participants during the 800-63 revision process.