Kantara Initiative Inc. has prepared the following set of comments on, and proposed changes to, your Special Publication 800-63 (Revision 3).

Input to these Comments and Proposed Changes came from members of:

- Kantara's Identity Assurance Work Group (IAWG),
- Kantara's Health Identity Assurance Work Group (HIAWG),
- Kantara's Assurance Review Board (ARB), as well as
- a Sub Group of the IAWG that developed Service Assessment Criteria (SAC) that will enable Assessors to assess Identity Services for compliance to parts A, B and C of SP800-63 at Level of Assurance 3.

Kantara's comments and proposed changes are based upon the experience of Kantara members in both developing SP800-63 compliant Identity Services and assessing that Identity Services are compliant with the requirements identified in SP800-63.

To ensure accurate identification of the specific text that our members wanted to comment upon, Kantara prepared PDF versions (with each line numbered) of all four parts of the Special Publication. These PDFs have been attached to the email that contained our comments to ensure NIST can identify the specific text being referenced in a comment.

Should NIST require clarification on any of Kantara's comments and proposed changes please do not hesitate to contact me by email.

Ken Dagg
Chair, Kantara Identity Assurance Work Group
kendaggtbs@gmail.com

General Comments on SP800-63

Comments in this section bear on 800-63 in its entirety.

Terminology

Comment: The use of terminology in SP800-63 is inconsistent across the document set but primarily between 63C and the other three documents.

Suggestion: Suggest reviewing the use of defined terms across the four documents to ensure consistent use of terminology.

Strong Issuer

Comment: NIST SP 800-63-3 Implementation Guidelines and 800-63-3 Conformance Criteria publications, appear to identify that identification credentials such as REAL ID and Federal Agency authorized identification credential equivalents (REAL ID, Enhanced ID, US Military ID) have a "special" status somewhere above STRONG evidence and somewhere below SUPERIOR evidence. These supplemental publications have invented a "STRONG+" category. STRONG+ evidence issuers, are in effect, deemed to employ sufficiently robust Identity Proofing processes that can be relied on by CSPs without requiring that CSPs explicitly evaluate those issuer Identity Proofing processes.

Suggestion: Consider explicitly stating the underlying conditions that would identify the issuers that are deemed to employ sufficiently robust ID Proofing processes. For example, for REAL ID cards, each State DMV is authorized by DHS to issue REAL ID cards. That authorization is the indication that the specific DMV complies with the REAL ID rules as enforced/evaluated by DHS.

Alternatively, NIST could explicitly list 'known strong' issuer programs TWIC, PIV-I, CAC, US Passport, PRC etc. This approach would imply that NIST recognizes the use of credentials issued by those programs as identification evidence at documented strengths used by applicants to claim an identity. The first option is preferred (reliance on authorization from a recognized authority).

Document Based Evidence

Comment: The Special Publication appears to be primarily based upon the use of document-based evidence.

Suggestion: Consider an explicit shift from document-based evidence towards electronic access to authoritative record evidence for identity proofing processes. For example, binding verification at IAL2 requires the CSP to physically compare the applicant to the strongest

presented evidence. However, if the CSP is able to compare the applicant to the authoritative record on file at the issuing source, the current 800-63-3A does not indicate that this is acceptable. Which raises the question: if the goals of Identity Proofing include confirmation that the applicant is the same individual as recorded in the authoritative source record, which is 'better': comparison to a physical document (or photo of a physical document if unattended) or comparison to a 'photo-on-file' of the applicant? We suggest the latter should be preferred.

Consent Receipt

Comment: Kantara Initiative and ISO SC 27/WG 5 have, for the last several years, been developing standards and specifications related to notice, consent and 'consent receipts'. These receipts are powerful personal record keeping records that enable the individual to understand where their data has been shared and to initiate recourse processes if necessary.

Suggestion: These publications should be used as inputs into future versions of 800-63 as they highlight and enhance the privacy-related requirements in the current 800-63-3 publication. In particular the concept of a 'consent receipt" (See Consent Receipt Specification 1.1.0. Kantara Initiative Consent & Information Sharing Work Group. 2018-02-20. Kantara Initiative Technical Specification Recommendation. https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/) is a personal record that memorializes events where a service provider has obtained consent of the individual for data processing.

Selfie-to-Credential Facial Matching

Comment: The use of selfie-to-credential facial matching has exploded in the market since NIST guidance was last updated in 2017. Groups including FIDO Alliance have launched new programs to develop performance requirements and certification programs for these new remote ID verification tools.

Suggestion: Consider providing performance metrics for selfie-to-credential face matching. It may be helpful for NIST to provide guidance as to the acceptable FAR/FRR of biometric matching in these tools.

Comments on 800-63A

Section 4.4.1.3 Validation Requirements

449-453: The CSP SHALL validate identity evidence as follows: Each piece of evidence SHALL be validated with a process that can achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

Comment: The use of the word “strength” can be ambiguous.

Suggestion: Suggest using “Level of Rigour” instead.

Comments on 800-63B

413-414: To satisfy the requirements of a given AAL, a claimant SHALL be authenticated with at least a given level of strength to be recognized as a subscriber.

Comment: This seems to be a very obscure requirement which, at best, states something which appears to be obvious. That is, the requirement seems to be effectively stating 'if you want to recognize a claimant as a AAL3 subscriber then you must authenticate at AAL3'.

Suggestion: Examine if this requirement is stating the obvious. If it is, determine if it can be eliminated or, if not, stated in a manner which makes it less obscure.

Section 4.3.2 Authenticator and Verifier Requirements

642-643: Relevant side-channel attacks SHALL be determined by a risk assessment performed by the CSP.

Comment: There is no explicit requirement to actually counter the identified threats.

Suggestion: Requirements for the CSP to address the identified side-channel attacks should be added.

Section 4.3.3 Reauthentication

657-658: Periodic reauthentication of subscriber sessions SHALL be performed as described in Section 7.2.

Comment: This is essentially the same as the requirement identified in lines 565-566, subject to the parameter change in sub-clause (a).

Suggestion: Determine if the two requirements are required or can be merged.

Section 5.1.4.2 Single-Factor OTP Verifiers

1075-1077: Single-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier, and SHALL be strongly protected against compromise.

Comment: The use of the phrase “strongly protected against compromise” is ambiguous as it is not measurable.

Suggestion: Requirements that imply rigour should have some basis of measurement or a reference source.

Section 6.1.2.3 Replacement of a Lost Authentication Factor

1805-1809: Those sent to a postal address of record SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes.

Comment: The values cited for confirmation codes are not consistent with those given in 63A Section 4.4.1.6 4) c) and 5) e). All these relate to proofing and binding yet, they are inconsistent and seem to have been arbitrarily set.

Suggestion: 63A and 63B should provide a single consistent basis for determining and applying these values if they are to be credibly received.

General Comments on 800-63C

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

C2E vs E2E

Comment: The conception of federation in 800-63C appears to be one suited for Consumer to Enterprise (C2E) types of use cases, either because the enterprises must meet substantial compliance obligations or to mitigate the risk to consumers of their sensitive personal information being misused. It does not appear to fit well with Enterprise to Enterprise (E2E) use cases, in which each Identity Provider (IdP) is operated as part of an organization’s enterprise services and represents the people associated with that organization (e.g., its employees), and Relying Parties (RPs) provide services needed by those people in pursuit of their relationship with the organization, e.g., doing their job. The European Union’s General Data Protection

Regulation (GDPR) recognizes this distinction. Examples of such federations include national federations in 68 countries that are joined into a global federation supporting the Research & Education (R&E) sector, and NIEF, which supports the US criminal justice sector.

Even the terminology of Subscriber connotes Consumer or Citizen and does not fit with E2E. “Subject” or “Principal” are more general terms applicable to both C2E and E2E uses of federation.

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 incentivize keeping the number of IdPs in a federation comparatively small. This is also counter to E2E, given the huge number of enterprises that may potentially benefit from NIST digital identity standards being applicable to their sectors. E2E federations may need to scale to include large numbers of organizations that operate IdPs, and often organizations in many different countries.

It is not clear that one set of requirements can effectively address both C2E and E2E uses of federation. Context matters in achieving security objectives.

Suggestion: 800-63C should recognize the distinction between C2E and E2E. Perhaps there should be separate C2E and E2E editions of 800-63C, or sections of 800-63C addressed specifically to one or the other. As one step in that direction, the 800-63 set of standards documents should replace “Subscriber” with “Subject” in recognition of the common circumstance that a person’s relationship with a given IdP is not elective but a requirement of their work or professional community.

Federated Security Incident Response

Comment: 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. 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.

Suggestion: 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.

Reliance on Existing Standards or Profiles

Comment: Some of the requirements of IdPs or RPs in 800-63C might be well addressed by following established industry standards or profiles. This would both reinforce their consistent adoption and reduce the burden on 800-63C to some degree.

Suggestion: Identify established industry standards or profiles where ever possible. One such, for SAML federations, is the SAML V2.0 Implementation Profile for Federation Interoperability published by the Kantara Initiative.

Socially Sensitive Terminology

Comment: Use alternatives to “whitelist” and “blacklist” throughout.

Suggestion: Use “allowlist” and “denylist” instead.

Specific Comments on 800-63C

Section 4 – Federation Assurance Levels

373-375: Additionally, the IdP SHALL employ appropriately-tailored security controls (to include control 373 enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or 374 equivalent federal (e.g., FEDRAMP) or industry standard.

Comment: This paragraph requires IdPs to meet certain security standards but is silent on any corresponding need for RPs. If the RPs countenanced in 800-63C 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.

Suggestion: Identify relevant security standards RPs must meet.

Section 4.1 – Key Management

387-389: “Government-operated IdPs asserting authentication at AAL2 and all IdPs asserting authentication 387 at AAL3 SHALL protect keys used for signing or encrypting those assertions with mechanisms 388 validated at FIPS 140 Level 1 or higher.”

Comment: What of CSPs who use services which are not FIPS 140-validated?

Suggestion: Address the possibility of a CSP using services that are not FIPS 140-validated.

Section 4.2 – Runtime Decisions

398-399: "All RPs in an IdP's whitelist SHALL abide by the provisions and requirements in the SP 800-63 suite.".

Comment: Since 63A and 63B address functions performed by IdPs, which provisions are intended by this statement to apply to RPs?

Suggestion: Clarify which provisions in the SP 800-63 suite (800-63A and 800-63B) are applicable to RPs for compliance with 800-63C.

Section 4.2 – Runtime Decisions (2)

Comment*: 403-405: "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."*

Comment: What this means is unclear. Does it mean authorization to release attributes about the Subscriber? Should the Subscriber's authority to make such decisions be limited to attributes that convey personal information about themselves?

Here and elsewhere reference is made to an "authorized party", though always in conjunction with the suggestion that that's usually the Subscriber. This is not defined in 800-63C. Who else might be authorized to make such decisions, and in what contexts? The answer to this question may hinge on whether C2E or E2E use cases are under consideration, and it must be consistent with principles articulated in the GDPR.

How do IdP discovery services figure in this requirement. That is, can the IdPs they present be considered as allowed (whitelisted)?

Suggestion: Clarify who has authority to permit or constrain release of which attributes under which circumstances. Ensure that the result is consistent with principles of consent articulated in the GDPR.

Section 4.2 – Runtime Decisions (3)

410-411: "All IdPs in an RP's whitelist SHALL abide by the provisions and requirements in the 800-63 suite."

Comment: Which requirements, and at what level? Also, creating an obligation of one organization with a unilateral step taken by another seems unwise.

Suggestion: Clarify which provisions and levels are indicated by the requirement. Resolve the situation where unilateral steps taken by one organization create obligations on a different organization.

Section 4.2 – Runtime Decisions (4)

417-419: "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."

Comment: Fails to take into consideration an IdP discovery mechanism not operated by the RP.

Suggestion: Incorporate IdP discovery not operated by the RP.

Section 4.2 – Runtime Decisions (5)

435-436: "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".

Comment: The Subscriber may not be the correct authority for deciding whether to release some attributes; they should only have discretion to suppress optional attributes that are personally identifying, (i.e., have some implication for their privacy).

Suggestion: Resolve to incorporate a Subscriber only having discretion to suppress optional attributes that convey personal information about the Subscriber.

Section 5.1 – Federation Models

Comment. Both the manual and dynamic models defined in this section are essentially bi-lateral in nature. Multi-lateral federation, the oldest and most widely deployed model of federation supporting E2E use cases, fits neither model.

Suggestion: 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 800-63C to avoid normative reference to such mechanisms.

Section 5.1.1 – Manual Registration

503-503: "Federation relationships SHALL establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship."

Comment: What party does this requirement encumber and what is that party required to do to satisfy the requirement? Also, why is there no corresponding statement in section 5.1.2?

Moreover, in E2E use cases, IdPs may support multiple constituencies and serve multiple missions, and 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.

Suggestion: This 800-63C requirement should identify which parties have responsibility for meeting this requirement, and it should recognize that the same level of IAL and AAL need not apply to all Subjects presented by an IdP.

Section 5.1.2 Dynamic Registration

510-512: "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."

Comment: What is the test for complying with this requirement? How does it relate to trustworthiness? It seems subjective and should be omitted.

Suggestion: Identify a test for complying with this requirement, or preferably, remove the requirement from any normative section.

Section 5.1.2 Dynamic Registration (2)

510-512: "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."

Comment: The reasoning behind 'registration' is unclear, since there are requirements for joining a federation stated elsewhere. Is the purpose of registration to allow parties onto an 'allow list' or does it means that only those on an 'allow list' can provide and make use of dynamic registration?

Suggestion: the purpose of registration should be clarified.

Section 5.1.2 Dynamic Registration (3)

510-512: "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."

Comment: The requirement states that configuration information SHALL be 'made available'. However , there is no requirement identifying means for trusting such information and knowing it to be genuine, not spoofing.

Suggestion: Identify a requirement for mutual authentication over such a connection.

Section 5.2 – Privacy Requirements

612-613: "Federation involves the transfer of personal attributes from a third party that is not otherwise involved in a transaction — the IdP."

Comment*:* This statement is false. Federation *may* involve transfer of personal information but need not. The IdP may well not be a third party but an element of an organization's enterprise services supporting the Subject's organization-related activities. And in any case, it does not add any normative value.

Suggestion: Remove the statement.

Section 5.2 – Privacy Requirements (2)

629-631: "When an IdP uses consent measures, the IdP SHALL NOT make consent for the additional processing a condition of the identity service.

Comment: The intent of this requirement is confusing. It almost seems to echo the GDPRish idea that access to an IdP service may not be contingent on the subscriber's consent to use their personal information for marketing, etc., even if that use is disclosed to the potential subscriber. If so, I don't like the idea as it effectively outlaws other legitimate business models.

Suggestion: ???

Section 6 - Assertions

730-742: "Although details vary based on the exact federation protocol in use, an assertion SHOULD be used only to represent a single login event at the RP. After the RP consumes the assertion, session management by the RP comes into play (see SP 800-63B Section 7); an assertion SHALL NOT be used past the expiration time contained therein. However, the

expiration of the session at the RP MAY occur prior to the assertion's expiration. See Section 5.3 for more information.

The assertion's lifetime is the time between its issuance and its expiration. This lifetime needs to be long enough to allow the RP to process the assertion and create a local application session for the subscriber, but should not be longer than necessary for such establishment. Long-lived assertions have a greater risk of being stolen or replayed; a short assertion lifetime mitigates this risk. Assertion lifetimes SHALL NOT be used to limit the session at the RP. See Section 5.3 for more information."

Comment: These statements fail to address the relationship between assertion lifetime and IdP session lifetime, and this appears to be the place in 800-63C at which to do so.

Suggestion: Address the relationship between assertion lifetime and IdP session lifetime, (i.e., there is none, as with RP sessions).

Section 6.3.1 – General Requirements

882-886: "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."

Comment: What constitutes a third party in a proxy's context can be complicated. In a E2E context a proxy may be used to present numerous services to the federation that are operated by a single organization, or that are operated by different organizations undertaking a common purpose, (e.g., Open Science Grid or the Laser Interferometer Gravitational-wave Observatory).

Suggestion: The various contexts in which federation proxies operate must be better understood and corresponding requirements articulated in the next version of 800-63C. 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

891-892: "They SHALL also be unguessable by a party having access to some information identifying the subscriber."

Comment: Although unguessability is the right objective, it may not always be possible to guarantee unguessability of a pseudonymous identifier from other information. This is similar to

the problem of re-identification of anonymized data on human subjects, which increasingly is an issue not of poor identifier construction but of the growing amount of data about people available publicly or for purchase, and the growing computing power with which to process that data. How should this criterion be assessed?

Suggestion: Focus the requirement on characteristics of acceptable construction of pseudonymous identifiers.

Section 6.3.2 – Pairwise Pseudonymous Identifier Generation

895-901: "Normally, the identifiers SHALL only be known by and used by one pair of endpoints (e.g., IdP-RP). However, an IdP MAY generate the same identifier for a subscriber at multiple RPs at the request of those RPs, provided:

- *Those RPs have a demonstrable relationship that justifies an operational need for the correlation, such as a shared security domain or shared legal ownership; and*
- *All RPs sharing an identifier consent to being correlated in such a manner.*

Comment: This text amounts to an optional SHALL.

Suggestion: A MAY clause should be used since it is effectively the alternative SHALL.

Section 7 – Assertion Presentation

918-919: "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."

Comment: This 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. Also, what forms of expression of an explicit request by an RP of an IdP should be considered to meet this requirement? In particular, must such requests be bound to the federation protocols in use in a manner that enables automated fulfillment of them (subject to IdP attribute release policies)?

Suggestion: Constrain the requirement to attributes that describe a living human. Address how it may be determined when an RP has made an explicit request for a set of attributes.

Section 7.3 – Protecting Information, and Section 9.3 – Data Minimization

1188-1189: "To support this RP requirement IdPs are, in turn, required to support attribute references."

Comment: Since there are an infinite number of potential attribute references that might be of use, what set of attribute references are required to be supported by an IdP? Also, are attribute references subject to the requirement of being explicitly requested as stated in section 7? If so, what standard defines how to formulate such a request? Should each Federation Authority identify or define such standards for use in their federation, and should they also define what attribute references are to be supported by their federation? Further, these statements are phrased as a requirement yet the statement in section 7.3, a normative section, does not use the standard terminology ("SHALL").

Suggestion: Either resolve the questions asked and use the SHALL terminology if this is a normative requirement, or preferably, move discussion of attribute references into an informative section of 800-63C.