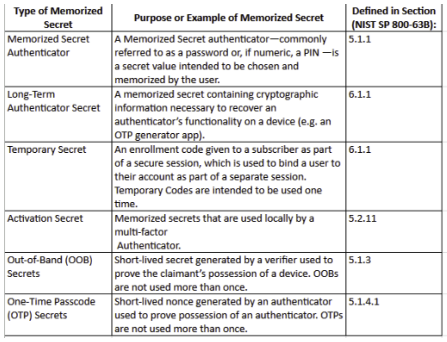
## Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

*Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023*

| | |
|---|---|
| ***Organization:*** | *DirectTrust Community* |
| ***Name of Submitter/POC:*** | *Kyle Neuman* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63-Base | 4.1 | 13 | 611 | The term Registration Authority was present in NIST SP 800-63-3 and removed in this revision. DirectTrust recommends re-introducing the term "Registration Authority" (RA) to bring clarity between the definitions. Introducing RAs that serve as a component of CSPs for ID proofing would align best with the way the industry core competencies exist in the wild. | Suggest adding the following language after the sentence ending in "number of entities":<br>"For example, identity proofing and enrollment activities may be outsourced to a third party, often called a Registration Authority." |
| 2 | 63-Base | 5.2.3.2-5.2.3.4 | 36-40 | 1292, 1335, 1374 | The decision trees displayed in NIST SP 800-63-3 base were very helpful tools to visualize and conceptualize the risk assessment processes necessary to evaluate the suitability each assurance level. We suggest adding back a version of those graphics. | We suggest adding back a version of those graphics. |
| 3 | 63-Base | 5.3.4 | 43 | 1465 | We would benefit from clarity concerning the scope of the Digital Identity Acceptance Statement. Should there be a separate digital identity acceptance statement for each application, or can an organization use a single digital identity acceptance statement that includes all the required criteria for each application? We also generally recommend requiring agencies to include the digital identity acceptance statement as part of a system authorization package. Otherwise, few agencies may have the necessary incentive and primer to carry out the processes defined in NIST SP 800-63-4 base. | Suggest editing the following sentence with the bold text below:<br>The Digital Identity Acceptance Statement documents the results of the digital identity risk management process for each application managed by the organization. |
| 4 | 63-Base | Appendix A | 47 | 1588 | We've experienced challenges in the industry around terminology that the base document has the ability to help address. There are two types of terminology issues: 1) Overloaded terms, where one term is used to describe multiple different things depending on how it's used, and 2) Synonyms, where multiple terms can be used to describe the same thing. We recommend including an additional appendix that disambiguates this terminology (as they are colloquially used) as a means of increasing comprehension and proper implementation in the wild.<br>Overloaded terms:<br>Token<br>Credentials<br>CSP<br>Authentication (authentication of identity vs authentication)<br>Account<br>Biometrics<br>Synonyms<br>Token<br>Other Terms<br>Relying Party<br>Registration Authority | We recommend an appendix that disambiguates terminology for readers with less experience and history in the digital identity space.<br>For example,<br>Overloaded Terms:<br>- Token: Used to describe an authenticator form factor and a federation assertion<br>- Credentials: Often used to describe authenticators (e.g. username and password) vs the more broad definition defined in 63 Base<br>- CSP: A CSP could be a Certification Authority, or an IdP, or some other credential issuer. When a CSP's services include a Verifier, the credential takes on a different form than a CSP without verifier functionality. We're finding that the industry is not entirely grasping these concepts. Visuals are very helpful.<br>- Authentication: Authentication of identity (term used in ID proofing) vs authentication using authenticators<br>- Account: An account will exist at a CSP/IdP (Subscriber account) and also at a Relying Party (such as an EMR or other data holder). Please add an adjective to the term account each time it is used.<br>- Biometrics: Used both in ID proofing and in authentication. We find that some folks in the industry get the role of biometrics confused when the term "biometrics" is used in different contexts. A discussion that teases apart the role of biometrics when used for IAL vs AAL would be helpful.<br>Synonyms<br>- Token is often used as a synonym for an assertion in the context of OAuth.<br>- An Authorization Server may be a synonym for an IdP in the context of OAuth.<br>Other Terms to Consider<br>- Relying Party: A relying party can also be a CSP (asserting party) depending on the transaction<br>- Registration Authority: Many organizations call a service provider that only does identity proofing a Credential Service Provider despite the service provider not supporting NIST SP 800-63B requirements. We believe the appropriate term for |
| 5 | 63A | 2.1 | 4 | 396 | Identity resolution is important for CSPs to maintain. However, to an increasing degree, CSPs are relied upon by commercial and government relying parties to transmit verified attributes not only to convey a verified identity, but also to resolve that identity within their system. This is commonly known in healthcare as patient matching. Please see comment 8. | Identity resolution: determine that the claimed identity corresponds to a single, unique individual within the context of the population of users and relying parties the CSP serves; |
| 6 | 63A | 4.1 | 6 | 454 | Should be the minimum necessary to accomplish identity proofing and identity resolution. Please see comment 8. | Suggest editing the following sentence with the bold text below:<br>The identity proofing process involves the presentation and validation of the minimum attributes necessary to accomplish identity proofing and identity resolution. |
| 7 | 63A | 4.1.1 | 9 | 485 | | "…verifying that the applicant…" |
| 8 | 63A | 4.2 | 9 | 491 | A brief discussion concerning identity resolution would be helpful to the RP community. In healthcare, CSPs do not collect the necessary attribute to match a patient identity across organizations. As a result, despite the user being identity proofed, they still cannot access or retrieve their healthcare data from an RP because the RP does not always receive the necessary attributes from the CSP to resolve the identity within their population of users. Patient matching is a major issue in healthcare and CSPs are in an excellent position to help address it. We recommend including suggestions to capture and enumerate identifiers present on evidence documents such as driver's license numbers, passport numbers and other identifiers that can be transmitted to relying parties in support of identity resolution. We also recommend NIST includes suggestions for CSPs to retain records of previous address information and possess mechanisms for updating attributes about users because this information is often used to resolve identities at RPs. A subscriber who has changed addresses recently may be unable to retrieve their medical data because the CSP only transmits their most recent address. In such cases, the RP may be unaware of the change and can only resolve the user's identity based on the previous address of the user | Suggest inserting the following language:<br>When defining a population or context, all CSPs and RPs within that context should collaborate and agree upon a set of attributes that are usable for RP identity resolution. As an example in healthcare, https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records. |

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td>9</td><td>63A</td><td>4.3.4.1</td><td>12</td><td>609</td><td>Conflicts with the last bullet under fair requirements, which allows evidence to be expired within the last 6 months. Suggest updating this sentence to take that caveat into considerations.</td><td>Suggest editing the following sentence with the bold text below:<br><br>The CSP SHALL validate that the evidence is current through confirmation that its expiration date is within tolerance or that evidence without an expiration date was issued within the previous six (6) months.</td></tr>
<tr><td>10</td><td>63A</td><td>4.3.4.1</td><td>13</td><td>613</td><td>Recommend being more explicit about validation of the digital signature. The CSP must validate the digital signature and verify the trust of the signer back to a known and trusted Trust Anchor at an expected and documented level of assurance. Verifying the digital signature chains to an issuing authority does not necessarily provide confidence in the identity of the signer if the issuing authority is not trusted.</td><td>Add the word "validated":<br><br>The CSP SHALL use the validated public key of the issuing authority of the evidence to verify digitally signed evidence or attribute data objects.</td></tr>
<tr><td>11</td><td>63A</td><td>5.1.9.1</td><td>25</td><td>997</td><td>Trusted Referees have more authority in 63-4. We assume to objective is to increase equity in digital identity. While DirectTrust agrees with this priority, we also feel the parameters to control training should be carefully defined to reduce the chances of misissuance.</td><td>Suggest editing the following sentence with the bold text below:<br><br>The CSP SHALL establish written policies and procedures, which include specific training requirements for the use of trusted referees as part of its practice statement, as specified in Sec. 5.1.1.</td></tr>
<tr><td>12</td><td>63A</td><td>6.3.2</td><td>35</td><td>1291</td><td>Additional reasons the CSP may terminate an account include:<br>- Certification of the subscriber is no longer in the interest of the CSP<br>- The CSP receives a legal instrument from a competent court to revoke or terminate the User’s account.</td><td>Suggest adding the following bullet to the list:<br><br>- The CSP receives a legal instrument from a competent court to revoke or terminate the User’s account.<br><br>Suggest adding:<br><br>- The CSP may revoke a subscriber account for other reasons documented in the CSP's policies and procedures.</td></tr>
<tr><td>13</td><td>63B</td><td>5.2.2</td><td>32</td><td>1232</td><td>To simplify requirements, we believe all OTP and memorized secret verifiers should support rate limiting functions, regardless of the size of the secret (i.e. 64 bits of entropy or larger).</td><td>We suggest removing:<br><br>"When required by the authenticator type descriptions in Sec. 5.1," and we recommend requiring rate limiting in all cases.</td></tr>
<tr><td>14</td><td>63B</td><td>5.1.1</td><td>14</td><td>674</td><td>NIST SP 800-63 series specifies several types of secrets. DirectTrust believes it would be helpful to aggregate all of these secrets and their associated brief definitions in one place to help the reader compare and contrast each secret to better understand their purpose and differences. We believe the most appropriate place to briefly define and distinguish all types of memorized secrets is in 5.1.1, where two of the six secrets are already defined.</td><td>Suggest adding the table below following line 674:<br>
<table>
<tr><th>Type of Memorized Secret</th><th>Purpose or Example of Memorized Secret</th><th>Defined in Section (NIST SP 800-63B):</th></tr>
<tr><td>Memorized Secret Authenticator</td><td>A Memorized Secret authenticator—commonly referred to as a password or, if numeric, a PIN —is a secret value intended to be chosen and memorized by the user.</td><td>5.1.1</td></tr>
<tr><td>Long-Term Authenticator Secret</td><td>A memorized secret containing cryptographic information necessary to recover an authenticator’s functionality on a device (e.g. an OTP generator app).</td><td>6.1.1</td></tr>
<tr><td>Temporary Secret</td><td>An enrollment code given to a subscriber as part of a secure session, which is used to bind a user to their account as part of a separate session. Temporary Codes are intended to be used one time.</td><td>6.1.1</td></tr>
<tr><td>Activation Secret</td><td>Memorized secrets that are used locally by a multi-factor Authenticator.</td><td>5.2.11</td></tr>
<tr><td>Out-of-Band (OOB) Secrets</td><td>Short-lived secret generated by a verifier used to prove the claimant’s possession of a device. OOBs are not used more than once.</td><td>5.1.3</td></tr>
<tr><td>One-Time Passcode (OTP) Secrets</td><td>Short-lived nonce generated by an authenticator used to prove possession of an authenticator. OTPs are not used more than once.</td><td>5.1.4.1</td></tr>
</table></td></tr>
<tr><td>15</td><td>63B</td><td>6.3</td><td>48</td><td>1778</td><td>DirectTrust recommends adding maximum cryptoperiods for each applicable authenticator described by NIST SP 800-63B. The strongest and most mature authenticators, hardware-based PKI credentials, commonly employ expiration dates of no more than 6 years, and they are arguably the least likely to be compromised. Weaker authenticators such as OTP secret keys, look up secrets etc.. should also have a defined seedlife as defined in NIST SP 800-90Ar1. We believe the industry would benefit from NIST-provided guidance on when those authenticators' cryptographic material should be cycled. If certain authenticators can have infinite cryptoperiods, then it would be helpful to identify those and briefly reference or define the reason. If some CSPs support expiration of their cryptographic material and other don't, but they all assert the same AAL, then relying parties may be unknowingly relying on CSPs with varying levels of risk.</td><td>We suggest referencing NIST SP 800-57 for cryptoperiods of authenticator cryptographic secret key materials and define maximum seedlife as suggested in NIST SP 800-90Ar1.</td></tr>
<tr><td>16</td><td>63B</td><td>6.4</td><td>49</td><td>1792</td><td>If revocation requests are not authenticated, the CSP's subscribers are at risk of denial of service of their account. We also request more specificity around the maximum time allowed to respond to a revocation request. The word "promptly" is required, but is not specific enough to enforce in a meaningful or consistent way.</td><td>Suggest adding the following language:<br><br>All revocation requests shall be authenticated by the CSP prior to taking action.</td></tr>
<tr><td>17</td><td>63C</td><td>5.1.2</td><td>15</td><td>707</td><td>We are unaware of a federation authority that has successfully struck a multilateral trust agreement with all constituents. Such a construct is challenging to execute and would not scale due to the need for all parties to resign the multilateral agreement each time a new party is added. The federation authorities that we are aware of, including DirectTrust, strike bilateral agreements with each of the IdP/CSPs. All IdPs/CSPs are not signatories of the same agreement. Rather, the same bilateral agreement remains substantially similar for each new IdP/CSP that is a signatory, thereby achieving very similar goals to a multilateral agreement with much greater ease and flexibility to manage the federation. Please see the following paper on this subject:<br>https://www.jstor.org/stable/29763044</td><td>Suggest adding the sentence:<br><br>As a variation of the Multilateral Trust Agreement Model, some federation authorities may execute substantially similar agreements with each IdP, CSP and RP in the federation, thus yielding the legal effect of a Multilateral Trust Agreement without requiring all parties to resign the agreement each time a new party is added.</td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | 63C | 5.1.2 | 16 | 720 | A Federation Operator may not be aware of all the RPs that rely on the Trust Framework, thus making the collection of RP signatures on an agreement difficult or impractical. Furthermore, RPs are rarely signatories of the trust agreement because the federation authority often exists to serve relying parties and mitigate relying party risks. Relying parties may elect not to carry out revocation checking, for example, at their leisure and at their own peril with no additional risk to the rest of the federation. If a breach occurs due to this sort of relying party negligence, the relying party is liable for their damages and damages to any affected subscribers. As a result, requiring relying parties to be a party to the trust agreement brings little value and only hampers the benefits of the federation and federating trust. It is worth noting further that most relying parties that rely on a federation authority (Trust Framework) tend to participate in highly regulated industries that impose strict requirements on how subscriber data is managed and protected (e.g. HIPAA) and are often required to demonstrate conformance with those regulations through other means. | Suggest removing the bullet:<br><br>RPs adhere to requirements for handling subscriber attribute data, such as retention, aggregation, and disclosure to third parties. |
| 19 | 63C | 5.3.4 | 23 | 904 | We assimilate an "Allowlist" to a Trust List (or Trust Store) for IdPs. In order to thwart a trusted impersonation attack, the Allowlist should also contain the xALs that the RP will accept from each IdP. This characteristic is often overlooked. A IdP that is trusted for one assurance level at the RP, may not be trusted for all assurance levels at the RP. This level of granularity is paramount for proper trust store and Allowlist management | Suggest editing the following sentence with the bold text below:<br><br>When placing an IdP in its allowlist, the RP SHALL ensure that the IdP abides by the provisions and requirements in these guidelines. RPs may include xALs accepted from each IdP, as defined in section 6 of 63C. |
| 20 | 63C | 5.4 | 24 | 934-937 | This is a common problem in healthcare identity. Its known as patient matching, where the subscriber authenticates with their IdP and an assertion is provided to the RP concerning the subscriber and the subscriber's attributes. The challenge is, no single globally unique identifier exists and sending demographic data is both a privacy concern and unreliable for identity resolution. Please see comment 8. Is there a different federated identifier for each RP? What happens when a subscriber moves to a different IdP but doesn't know what their federated identifier was at their previous IdP? Do IdPs coordinate federated identifiers? We feel this article describes the challenges in healthcare related to identity resolution very well:<br>https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records | |
| 21 | 63C | 5.4.2 | 28 | 1026 | We do not recommend that RPs delete subscriber accounts just because the account is revoked at the IdP. There are many reasons that an IdP account could be revoked that may have nothing to do with the relationship that the subscriber has with the RP. For example, the subscriber may merely wish to switch IdPs if the RP federates with multiple IdPs, in search of a more favorable service. Deleting the account at the RP could harm the subscriber in this context. For example, it would be inappropriate to delete the Subscribers account within an Electronic Health Record system managed by an RP just because the subscriber's account was revoked at an IdP, especially if the RP federates with multiple IdPs or CSPs. | We suggest removing requirements related to the deletion of a subscriber account in an RP system if the Subscriber account is revoked at an IdP. |