Credential Service Provider
Capabilities Description Template

**May 2024**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author of Changes** | **Description** |
| March 2024 | 1.0 | GSA/FAS/ITC | First Version |
| May 2024 | 1.1 | GSA/FAS/ITC | Added privacy related questions  |

**Table of Contents**

[1 Introduction 1](#_Toc159962086)

[2 General Information 3](#_Toc159962087)

[3 System Operations 5](#_Toc159962088)

[4 Identity Data Collection and Verification 9](#_Toc159962089)

[5 Identity Data Exchange 12](#_Toc159962090)

[6 Authenticators 13](#_Toc159962091)

[7 Credential Lifecycle Management 16](#_Toc159962092)

[8 Assertions 18](#_Toc159962093)

[9 Credential Validation 20](#_Toc159962094)

[10 Additional Information 22](#_Toc159962095)

[Appendix A: NIST SP 800-63B Authenticator Types 24](#_Toc159962096)

[Appendix B: Source Documents 27](#_Toc159962097)

**List of Tables**

[Table 1: General Information 3](#_Toc159962098)

[Table 2: Services Provided 4](#_Toc159962099)

[Table 3: System Operations 5](#_Toc159962100)

[Table 4: Identity Data Collection and Verification 9](#_Toc159962101)

[Table 5: Identity Data Exchange 12](#_Toc159962102)

[Table 6: Authenticators 13](#_Toc159962103)

[Table 7: Credential Lifecycle Management 16](#_Toc159962104)

[Table 8: Assertions 18](#_Toc159962105)

[Table 9: Credential Validation 20](#_Toc159962106)

[Table 10: Additional Information 22](#_Toc159962107)

[Table 11: NIST SP 800-63B Authenticator Types 24](#_Toc159962108)

# Introduction

This template provides technical guidelines for commercial providers and mission partners to offer a consistent mechanism for third party credential service providers (CSPs) to document their operations while accounting for distinct use cases with differing needs. Additionally, it identifies key considerations and desired best practices for operations. The template covers security and privacy, system operations, data collection, data exchange, authenticators, credential lifecycle management, assertions, and credential validation. This template is intended to assist as part of decision-making processes for contracting, federation, and other use of CSPs. It provides a consistent format for input to government entities who may be conducting standardized risk assessments during procurement and purchasing decisions. Moreover, this assessment is designed to expand and clarify gaps in the current CSP evaluation process by expanding upon the Identity and Authenticator (I&A) requirements specified in NIST SP 800-63 to include the underlying security of how the systems that may sign assertions used in federation, or in binding the identity to the authenticator, are operated.

Security and privacy requirements are based on NIST SP 800-53 and NIST SP 800-171.

NIST is in the process of updating SP 800-63 and draft versions of the update have been made available for public comment. CSPs are encouraged to include descriptions of their processes as they relate to the updated draft documents. Vendors should expect this document to be revised when the updated SP 800-63 documents are finalized.

The “Target” statements in the tables are not to be interpreted as requirements, but rather to be considerations both for the provider to indicate the type of details expected to be included in the response, and for the government evaluator to consider when reviewing the response.

For the purposes of this document, “credential” and “credential service providers” are as defined by NIST SP800-63 as follows:

* **Credential** is “An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.”
* **Credential service provider** or **CSP** is “A trusted entity whose functions include identity proofing applicants to the identity service and the registration of authenticators to subscriber accounts. A CSP may be an independent third party.”

**Section 2 General Information**, in addition to providing contact information about the CSP provides guidance on which of the following tables are applicable to the services offered by the CSP. The tables in Section 2 should be filled out by all providers.

**Section 3, System Operations**, is only applicable for CSPs that collect identity information for identity proofing.

**Section 4, Identity Data Collection and Verification**, is applicable for CSPs that verify or validate the identity data collected for identity proofing. Information required describes the processes used.

**Section 5, Identity Data Exchange**, is applicable for CSPs that rely on a different provider for identity verification.

**Section 6, Authenticators**, is applicable for CSPs that bind authenticators to subscriber digital identities.

**Section 7, Credential Lifecycle Management**, is applicable for CSPs that provide credential lifecycle management.

**Section 8, Assertions**, is applicable for CSPs that provide federation assertions.

**Section 9, Credential Validation**, is applicable for CSPs that provide credential validations.

**Section 10, Additional Information**, is applicable for all CSPs.

# General Information

The Service Description in the following table should provide details such as what components are included, whether they are only offered as part of a full service or can be integrated with other services, type of authenticators, and assertions that can be provided during authentication. Additional details will be requested in following applicable tables.

For any biometric components of the offering, include a pointer to results of National Voluntary Laboratory Accreditation Program (NVLAP) biometrics testing.

Additional relevant information about available interoperability reports or demonstrations of capabilities such as participation in W3C demonstrations, IETF Hackathons, Agency Pilots, NCCoE projects, etc., may be included along with Certifications/Assessments in the following table.

Table 1: General Information

|  |  |
| --- | --- |
| **CSP Name** | **Organization Contact Information** |
| <enter response here> | <enter response here> |
| **Service Description: Provide a brief narrative description of the service(s) provided by your organization** |
| <enter response here> |

|  |
| --- |
| **Certifications/Assessments: List any Government or Commercial Certifications (e.g., FIPS 140 Validation, FedRAMP Authorization, inCommon Membership, Kantara Approval)** |
| **Certifying Organization** | **Description of Certification/Assessment and What is Certified/Assessed, if available include link to publicly available report** |
| <enter response here> | <enter response here> |
| **Applicable Privacy Laws and Regulations: List what privacy laws and regulations your company adheres to (e.g.: California Consumer Privacy Act (CCPA), other state laws, the European Union’s General Data Protection Regulation (GDPR)** |
| <enter response here> |
| **Data Privacy Officer: If your organization has appointed a Data Privacy Officer. Provide a description of their responsibilities.** |
| <enter response here> |

Table 2: Services Provided

|  |
| --- |
| **Services Provided: Check All That Apply and Complete Associated Tables** |
| **Does the service provide identity proofing?** |  | Yes | [Table 3](#bookmark=id.3dy6vkm) [Table 4](#bookmark=id.4d34og8)Table 10 |
|  | No, identity information is self-asserted | N/A |
|  | No, identity information is provided by the federal agency or other client | [Table 3](#bookmark=id.3dy6vkm) [Table 5](#bookmark=id.17dp8vu)Table 10 |
|  | No, identity information is provided by a third party (note that Tables 1 and 3 must be completed by the service provider, and Tables 1 and 2 must also be completed by the third party) | [Table 3](#bookmark=id.3dy6vkm) [Table 4](#bookmark=id.4d34og8)[Table 5](#bookmark=id.17dp8vu) Table 10 |
| **Does the service enroll authenticators to a subscriber account?** |  | Yes | [Table 3](#bookmark=id.3dy6vkm) Table 6 [Table 7](#bookmark=id.qsh70q)Table 10 |
|  | No, service only supports identity proofing and provides validated identity information to credential issuers | [Table 5](#bookmark=id.17dp8vu)Table 10 |
| **Does the service leverage previously enrolled authenticators to validate identity?** |  | Yes | Table 3 Table 8 [Table 9](#bookmark=id.2p2csry)Table 10 |
|  | No, validation is the responsibility of the federal agency or other client | N/A |
| **Does the service provide identity assertions?** |  | Yes | Table 3 Table 8Table 10 |
|  | No  | N/A |

# System Operations

Complete the tables by describing the processes used to provide reliability and to protect system components from external attackers and insider threats. Processes to be covered include the systems, configuration, personnel, and auditing capabilities. If more than one process is supported, describe differences, or create a new row for each distinct process. If a process is described in a different table, referencing that table is sufficient; the process does not need to be described twice. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 3: System Operations

|  |
| --- |
|  |
| **3.1 Identify documentation that describes processes, procedures, and controls** |
| **Target*** Processes should be performed according to documented policy, standards, and practices.
* The documented practices should include how the provider handles system errors
 |
| <enter response here> |
| **3.2 Describe any independent auditing, including frequency and scope of audit** |
| **Target*** Systems should be audited against written documented practices by a qualified independent third party (include either identity of third-party auditor, or at a minimum the required qualifications)
 |
| <enter response here> |
| **3.3 Define how applicant identity data is protected from unauthorized access, how it is encrypted and who has access** |
| **Target*** Access to data collected from applicants as part of identity proofing should be restricted to trusted personnel.
* Data collected from applicants may only be used to support the credential issuance process or for other purposes that the applicant has explicitly agreed to.
* If applicant identity data may be used for any other purpose or shared or monetized after the transaction, describe what these potential uses are and how applicant consent is obtained.
* Policies for data retention and destruction should be documented and followed.

**MINIMUM REQUIREMENT**: encryption is FIPS 140-3 certified |
| <enter response here> |
| **3.4 Define how data is protected in transit when sent between system components, operators, and applicants** |
| **Target*** All transactions should occur over authenticated protected channels, e.g. VPN, TLS1.3
 |
| <enter response here> |
| **3.5 Identify roles and describe requirements for each trusted role involved in identity proofing and credential issuance including background checks, training, segregation of duties between roles** |
| **Target*** Operators who support identity proofing should be trained to detect potential fraud.
* All personnel filling trusted roles should receive training on all aspects of the role they are expected to perform.
* If automated processes are used for verification of documentation, including fraud detection, please describe.
* Describe training received, including how often training is refreshed and how often personnel undergo the training.
* Describe training in applicable privacy laws and regulations, California Consumer Privacy Act (CCPA), other state laws, and the European Union’s General Data Protection Regulation (GDPR)
 |
| <enter response here> |
| **3.6 Describe protections for access** |
| **Target*** Personnel filling trusted roles should use multi-factor authentication for all remote access to system components.
* Endpoints used by personnel to access system components should have protections to minimize risk of system takeover by non-trusted personnel
 |
| <enter response here> |
| **3.7 Describe the types of events that are logged and what reviews are performed on audit logs to monitor for anomalous behavior** |
| **Target*** Security auditing capabilities of the operating system and applications should be enabled at all times while systems are operational.
* Audit logs should contain information sufficient to review all actions taken by the system to ensure they are made by authorized parties and for legitimate reasons.
* Audit log reviews should be performed using an automated process and should include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities.
* System configuration and operational procedures should be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified before review.
* Audits should be retained for a specified period and include a predetermined set of records as set forth in the audit plan
 |
| <enter response here> |
| **3.8 Describe any archive practices, what records are archived, how long they are retained, and how they are disposed** |
| **Target*** Archive records should be sufficient to determine the proper operation of the service and the validity of any identities proofed.
* Archives should be retained for a specified period and include a predetermined set of records as set forth in the archive plan.
* Archives should be protected from unauthorized access and from tampering.
* Archives should be securely destroyed after the required retention period.
 |
| <enter response here> |
| **3.9 Describe computer security controls that protect the overall integrity of system operations** |
| **Target*** System components should authenticate the identity of individuals holding trusted roles before permitting access to the system, data, or applications using a credential at least as strong as the highest authenticator assurance level supported by the system.
* System components should manage privileges of users to limit users to their assigned roles.
* System components should enforce domain integrity boundaries for security critical processes.
* System components should require use of cryptography for session communication and database security.
* Mutual authentication should be required both between system components and between users and components, e.g., VPN, mTLS.
* System components should preserve the confidentiality of all Personally Identifiable Information (PII) collected about applicants or subscribers.
 |
| <enter response here> |
| **3.10 Describe life-cycle controls that ensure the integrity of hardware and software used to perform system operations** |
| **Target*** Procure hardware and software in a fashion to reduce the likelihood that any particular component was tampered with.
* Develop custom hardware and software in a controlled environment using a development process that is defined and documented.
* Prevent malicious software from being loaded onto system components by obtaining software from documented sources and scanning for malicious code.
* Purchase or develop hardware and software updates using the same manner as original equipment, and ensure that all installation is performed by trusted and trained personnel.
* Document hardware and software lifecycle control to ensure vulnerabilities are patched and products are not used past end of life support.
* Document and control system configuration, including implementation of mechanisms to detect unauthorized modification of software or configuration.
 |
| <enter response here> |
| **3.11 Describe network controls that protect against unauthorized access to system components or data** |
| **Target*** Implement boundary controls that deny all but the necessary services to system components and any remote workstations used to administer system components.
* Disable unused network protocols, ports and services.
* Ensure that remote access for administration requires mutual authentication and data encryption.
 |
| <enter response here> |
| **3.12 Describe any physical controls that protect against unauthorized access to system components or data** |
| **Target*** If the service is operated in a cloud environment, identify any FedRAMP or other relevant certifications the cloud provider has.
* If the service is operated in a data center, physical access controls should be implemented that:
	+ Ensure that no unauthorized access to the hardware is permitted.
	+ Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
	+ Be manually or electronically monitored for unauthorized intrusion at all times.
	+ Ensure an access log is maintained and inspected periodically.
	+ Require two-person physical access control to both the cryptographic module and computer systems.
 |
| <enter response here> |

# Identity Data Collection and Verification

Complete the tables by describing the processes used to perform identity data collection and verification. If more than one process is supported, describe differences or create a new row for each distinct process. If the process is remote, include a description of liveness detection. If a process is described in a different table, referencing that table is sufficient, the process does not need to be described twice. For Identity Assurance Level (IAL) IAL3 please complete both IAL2 and IAL3 target assessments. Include whether steps are automated or manual and what assistance is available in the case of a failed process. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 4: Identity Data Collection and Verification

|  |
| --- |
| **4.1 Select which identity assurance levels are supported by the service** |
|  | IAL1 |  | IAL2 |  | IAL3 |
| **4.2 Describe the process for collecting identity information** |
| **Target*** In-person, supervised remote, or remote are acceptable for IAL1 and IAL2, only in-person or supervised remote can be used for IAL3.
* Obtain permission from the applicant for any permitted use of the applicant’s identity data.
* Collect and record identity evidence as described in NIST SP 800-63A.
* Limit collection of PII to the minimum necessary to resolve to a unique identity record.
 |
| <enter response here> |
| **4.3 Specify all data elements that are collected as part of the identity proofing process** |
| **Target*** List all subscriber attributes that are collected or generated as part of the process.
* For each attribute, state whether the data value is retained after completion of the process.
 |
| <enter response here> |
| **4.4 If any data collected is retained in an associated user account, describe how the user can access their account and update or delete information** |
| **Target*** List all subscriber attributes that are retained as part of the account.
* Describe how the user authenticates to update or request deletion of the information in the account or the account itself.
* How is unauthorized access prevented?
* What multi-factor authentication is supported?
 |
| <enter response here> |
| **4.5 Describe the process for validating identity evidence provided by the applicant at each IAL supported** |
| <enter response here> |
| **4.6 Describe the process for verifying the claimed identity to the applicant presenting the evidence for each IAL supported** |
| <enter response here> |
| **4.7 Describe the process for confirming the applicant’s address of record, include information about what types of addresses are acceptable and confirmed and how notifications are sent, if applicable. (eg. postal, email, telephone) for each IAL supported** |
| <enter response here> |
| **4.8 Describe the process for collecting and confirming applicant biometrics** |
| **Target*** Biometrics are optional for IAL1 and 2, if biometrics are not collected then put “N/A” in the table.
* The operator should view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.
* A biometric sample should be collected at the time of proofing (e.g., facial image, fingerprints) for the purposes of nonrepudiation and re-proofing.
 |
| <enter response here> |
| **4.9 Provide available information for pass/fail rates and mitigations** |
| **Target*** Describe any failover processes in place to support applicants that do not pass initial identity verification checks.
* Identify the pass/fail metrics for identity verification. If different processes are supported, provide individual rates for each process along with overall rates for successful identity verification.
* Describe how this solution has demonstrated equitable outcomes in pass/fail rates across racial, socioeconomic and gender demographics.
* Describe how pass/fail metrics, including false positive or false negative rates, are captured and analyzed.
 |
| <enter response here> |
| **4.10 If applicable, describe how the system supports the following** |
| Does the system provide services to minors under the age of 13? Or for those between the ages of 13-17? |
| <enter response here> |
| **Target – if Yes**System should meet additional special considerations under Children's Online Privacy Protection Act (COPPA) and other laws. Describe how are age limits are enforced, when appropriate. |
| <enter response here> |
| Describe special considerations given to minors who are unable to meet the evidence requirements for identity proofing.  |
| <enter response here> |
| Does the system use trusted referees? |
| <enter response here> |
| **Target – if Yes*** The provider should describe how a trusted referee is determined and the lifecycle by which the trusted referee retains their status.
* The trusted referee should be proofed at the same IAL as the applicant.
* The provider should describe the minimum evidence required to bind the relationship between the trusted referee and the applicant
 |
| <enter response here> |
| **4.11 Describe, if applicable, what alternative ways can be used by an applicant who does not possess the required identity evidence to complete the identity proofing process?** |
| <enter response here> |
| **4.12 List what languages are supported, both for support and any web based instructions.**  |
| <enter response here> |
| **4.13 If applicable, how is age verified if customer RP application requires age verification?** |
| <enter response here> |

# Identity Data Exchange

If a solution is provided by multiple entities working together, or the CSP relies on a different provider for identity verification, complete the table by describing the processes used to exchange identity data between the entity that performs identity verification and the entity that issues and validates credentials. If more than one process is supported, describe differences or create a new row for each distinct process. If a process is described in a different table, referencing that table is sufficient, the process does not need to be described twice. Refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 5: Identity Data Exchange

|  |
| --- |
| **5.1 Describe the process used to establish agreements between the business partner that performs identity verification and the partner that issues and validates credentials** |
| **Target*** If identity data is collected by human resources and credentials are issued by information technology departments within a single organization, no signed agreement is required, but any data transfer processes should be described.
* Trust agreement should specify the parties and the data that is to be exchanged.
* If the agreement is between two legally distinct organizations, the agreement should be signed by individuals with authority to bind the organization.
 |
| <enter response here> |
| **5.2 Describe the circumstances where applicant identity data may be shared outside of the entity that collected it** |
| **Target*** Describe the circumstances where applicant identity data may be shared outside of the entity that collected it, including whether identity data may be sold or monetized after collection.
* Circumstances should comply with data use permissions obtained from applicants.
 |
| <enter response here> |
| **5.3 Describe the process for establishing trust between the systems** |
| **Target*** Systems should use credentials that achieve authenticator equivalent to Authenticator Assurance Level (AAL) AAL2.
* Process to exchange system credentials should be out of band.
 |
| <enter response here> |
| **5.4 Describe the process used to exchange data between the systems** |
| **Target*** Systems should mutually authenticate each other prior to providing any applicant identity data.
* Data should be transferred using a process that ensures data integrity.
* Data should be encrypted in transit.
 |
| <enter response here> |

# Authenticators

Complete the tables by describing the supported authenticators and processes used to bind authenticators to subscriber digital identities. If a process is described in a different table, referencing that table is sufficient, the process does not need to be described twice. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 6: Authenticators

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| **6.1 Select which authenticator assurance levels are supported by the service** |
|  | AAL1 |  | AAL2 |  | AAL3 |
| **6.2 For each type of authenticator used, describe how the authenticator meets the requirements specified in NIST SP 800-63B for that authenticator type (Sections listed below refer to 800-63B)** |
| **Target*** Biometric – Section 5.2.3
* Memorized Secret – Section 5.1.1
* Look-up Secret – Section 5.1.2
* Out-of-band Device – Section 5.1.3
* One-Time Password Software – Section 5.1.4
* One-Time Password Device – Section 5.1.4
* Biometric Activated One-Time Password Software – Sections 5.1.5 and 5.2.3
* Memorized Secret Activated One-Time Password Software – Section 5.1.5
* Biometric Activated One-Time Password Device – Sections 5.1.5 and 5.2.3
* Memorized Secret Activated One-Time Password Device – Section 5.1.5
* Cryptographic Software – Section 5.1.6
* Cryptographic Device – Section 5.1.7
* Biometric Activated Cryptographic Software – Sections 5.1.8 and 5.2.3
* Memorized Secret Activated Cryptographic Software – Section 5.1.8
* Biometric Activated Cryptographic Device – Sections 5.1.9 and 5.2.3
* Memorized Secret Activated Cryptographic Device – Section 5.1.9
 |
| <enter response here> |
| **6.3 List supported authenticators** |
| **Target*** Appendix A contains a list of all authenticators and authenticator combinations from NIST SP 800-63B for each authenticator assurance level.
* Identify each authenticator type or combination of authenticators supported on its own row.
 |
| <enter response here> |
| **6.4 If any of the authenticators is a memorized secret or uses a memorized secret, describe requirements for the memorized secret and how these requirements are enforced** |
| **Target*** If chosen by the subscriber, the memorized secret should be at least 8 characters in length.
* If chosen by the credential service provider or token using a random number generator approved by NIST for use by Federal agencies, the memorized secret should be at least 6 characters in length and may be entirely numeric.
* No other complexity requirements for memorized secrets should be imposed.
 |
| <enter response here> |
| **6.5 If any of the authenticators is a memorized secret, describe requirements for storing and maintaining memorized secret information** |
| **Target*** The credential service provider should not permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant or prompt the subscriber to use a specific type of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.
* When processing a request to establish or change a memorized secret, the credential service provider should compare the prospective secret against a list that contains values known to be commonly used, expected, or compromised; and if a chosen secret is found in the list, the credential service provider should advise the subscriber that they need to select a different secret, provide the reason for rejection, and require the subscriber to choose a different value.
* The credential service provider should implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account.
* The credential service provider should force a change of memorized secret if there is evidence of compromise of the authenticator.
* Credential service providers should store memorized secrets in a form that is resistant to offline attacks, including the use of salting and hashing.
 |
| <enter response here> |
| **6.6 Describe the process for enrollment of subscribers and binding of subscriber digital identities to authenticators** |
| **Target*** Communication between the applicant and credential service provider should be via an authenticated protected channel.
* If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant should identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant’s phone number, email address, or postal address of record.
* If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets should be delivered to the applicant within a protected session.
* Credential service providers should maintain a record of all authenticators that are or have been associated with each identity, including any user-provided authenticators; the record should contain the type of authenticator and date the authenticator was bound to the account.
* When any new authenticator is bound to a subscriber account, the credential service provider should ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with the AAL at which the authenticator will be used.
* Binding of multi-factor authenticators should require multi-factor authentication (or equivalent at identity proofing).
* The credential service provider shall bind at least one, and should bind at least two, physical (something you have) authenticators to the subscriber’s online identity, in addition to a memorized secret or one or more biometrics at enrollment.
* The credential service provider should require the subscriber to authenticate at the AAL at which the new authenticator will be used before adding a new authenticator to a subscriber’s account.
* If the subscriber’s account has only one authentication factor bound to it, the credential service provider should require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.
 |
| <enter response here> |
| **6.7 Describe how AAL2 specific requirements will be met if AAL2 is supported, otherwise put N/A**  |
| **Target*** Cryptographic authenticators should use NIST approved cryptographic algorithms.
* Cryptographic authenticators should be validated to meet the requirements of FIPS 140 Level 1 or higher.
* If a device such as a smartphone is used in the authentication process, then the unlocking of that device cannot be considered one of the authentication factors.
* At least one authenticator should be replay resistant.
 |
| <enter response here> |
| **6.8 Describe how AAL3 specific requirements will be met if AAL3 is supported, otherwise put N/A** |
| **Target*** Cryptographic authenticators should use approved cryptographic algorithms.
* Multifactor authenticators should be hardware cryptographic modules validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security.
* Single factor cryptographic devices should be validated at FIPS 140 Level 1 or higher overall with at least FIPS 140 Level 3 physical security.
* If a device such as a smartphone is used in the authentication process, then the unlocking of that device cannot be considered one of the authentication factors.
* At least one authenticator should be replay resistant.
* At least one authenticator should be verifier impersonation resistant.
	+ Establish an authenticated protocol channel with the verifier.
	+ Strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output.
	+ Require that the credential service provider validates the signature or other information used to prove verifier impersonation.
	+ Use cryptographic algorithms approved by NIST for use by Federal agencies to establish verifier impersonation resistance.
* Authentication and reauthentication processes should demonstrate authentication intent from at least one authenticator.
* Be verifier compromise resistant with respect to at least one authentication factor.
 |
| <enter response here> |

# Credential Lifecycle Management

This section is not about management of an identity or relying party account, rather it pertains to whether or not the CSP provides lifecycle management of credentials. When relying on external credentials, it is important to know whether a credential is still considered valid, not just that it was verified and enrolled at least once in the past. If the CSP only validates identity or issues credentials that never expire and are considered valid forever, this section would be “Not Applicable.” The term “revoked” indicates the credential should be considered no longer valid.

Complete the tables by describing the processes and protocols to maintain, re-issue, revoke and otherwise manage credentials after issuance. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 7: Credential Lifecycle Management

|  |
| --- |
| **7.1 Describe the circumstances where a credential issued to a subscriber will be revoked or otherwise invalidated** |
| **Target*** The credential must be revoked when the binding between the subscriber and the authenticator is no longer considered valid.
* If the credential represents association with a specific organization, the credential must be revoked if the subscriber is no longer affiliated with that organization.
* The credential must be revoked if any names or other identifying information contained in the credential are no longer valid.
* The credential should be revoked or suspended if there is reason to believe that any authenticator associated with the credential has been compromised.
* The credential must be revoked upon request by the subscriber.
* The credential may be revoked if it has not been used for a period of time that exceeds limits established with the subscriber at the time of initial issuance.
* The credential may be revoked at the end of a validity period specified at the time of original issuance; however, the subscriber should be notified prior to the revocation date.
 |
| <enter response here> |
| **7.2 Describe who can request that a credential be revoked or otherwise invalidated** |
| **Target*** The credential service provider may revoke credentials within the terms of any agreement between the provider and the subscriber.
* The subscriber may request revocation of their own credentials.
* If the credential represents association with a specific organization, then designated individuals within that organization may request revocation of credentials, as defined by the agreement between the CSP and the organization.
* Other parties may notify the CSP or subscriber of suspected compromise of authenticators associated with the credential for action by the CSP or subscriber.
 |
| <enter response here> |
| **7.3 Describe the process for revoking or otherwise invalidating a credential** |
| **Target*** The identity of the requestor must be verified.
* The revocation request must identify the credential to be revoked and explain the reason for the request.
* If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then the suspension should be reversible if the subscriber successfully authenticates to the CSP using a different valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.
 |
| <enter response here> |
| **7.4 Describe the process for subscribers to obtain replacement credentials or authenticators if they lose access (e.g., token loss, forgotten password, malfunctioning device)** |
| **Target*** If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator should be either a memorized secret or a physical authenticator.
* If a subscriber loses all authenticators of a factor necessary to complete multifactor authentication and has been identity proofed at IAL2 or IAL3, that subscriber must repeat the original identity proofing process.
* Describe any accepted abbreviated process, if applicable, e.g., biometric match to a biometric on file.
 |
| <enter response here> |
| **7.5 Describe any routine refresh processes, if applicable** |
| **Target*** Subscriber identity should be re-established and the binding between the subscriber and the credential should be revalidated using the same process as initial issuance periodically.
* If the authenticator technology includes an expiration date, the CSP should have processes to notify/remind subscribers prior to expiration.
* If the CSP chooses to change the technology or algorithms used in credentials, the CSP must notify subscribers.
 |
| <enter response here> |

# Assertions

Complete the tables by describing the processes and protocols to create and provide assertions between the credential service provider and the relying party. If more than one process is supported, describe differences or create a new row for each distinct process. CSPs only need to complete tables that are applicable to the FAL levels supported by the CSP. If a process is described in a different table, referencing that table is sufficient; the process does not need to be described twice. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 8: Assertions

|  |
| --- |
| **8.1 Select which federation assurance levels (FALs) are supported by the service** |
|  | FAL1 |  | FAL2 |  | FAL3 |
| **8.2 Describe the contents of assertions (FAL1, FAL2, and FAL3)** |
| **Target*** The assertion should contain subject identifier, issuer identifier, relying party identifier, issuance time, expiration time, assertion identifier, and subject authentication time.
* The assertion should specify the AAL of the originating authentication event and the IAL of the identity proofing.
* The assertion may include additional subject attributes provided that the use of those attributes is in accordance with data use permissions obtained from the subject and the attributes were requested by the relying party.
 |
| <enter response here> |
| **8.3 Describe how assertions are digitally signed (FAL1, FAL2, and FAL3)** |
| **Target*** Assertions should be cryptographically signed by the issuer.
* The assertion signature should either be a digital signature using asymmetric keys or a message authentication code (MAC) using a symmetric key shared between the relying party and the issuer.
* Signatures should cover the entire assertion, including its identifier, issuer, audience, subject, any associated attributes (e.g. IAL, AAL), and expiration.
* All signature algorithms should be currently approved by NIST for use by Federal agencies.
 |
| <enter response here> |
| **8.4 Describe other security and privacy controls on assertions (FAL1, FAL2, and FAL3)** |
| **Target*** Assertions should include protections to prevent attackers from manufacturing valid assertions or reusing captured assertions at disparate relying parties.
* Assertions should use audience restriction techniques to allow a relying party to recognize whether it is the intended target of an issued assertion.
 |
| <enter response here> |
| **8.5 If applicable, describe how the system supports the following (FAL1, FAL2, and FAL3)** |
| Does the system support front channel assertions? |
| **Target – if Yes*** The assertion should be FAL2 or FAL3.
* Communications between the credential service provider and the relying party should be protected in transit using an authenticated protected channel.
* Communications between the subscriber and either the credential service provider or the relying party should be made using an authenticated protected channel.
 |
| <enter response here> |
| Does the system use assertion references? |
| **Target – if Yes*** The assertion reference should not contain information about the subscriber, should be single use, should be limited to use by a single party, and should be resistant to tampering and fabrication by an attacker.
* Conveyance of the assertion reference from the credential service provider to the subscriber, and from the subscriber to the relying party should be made over an authenticated protected channel.
* Conveyance of the assertion reference from the relying party to the credential service provider, and the assertion from the credential service provider to the relying party should be made over an authenticated protected channel.
* The credential service provider should verify that the party presenting the assertion reference is the same party that requested the authentication.
 |
| <enter response here> |
| **8.6 Describe processes and cryptographic algorithms used to encrypt assertions (FAL2 & FAL3)** |
| **Target*** The assertion should be encrypted using either the relying party’s public key or a shared symmetric key.
* If the assertion is encrypted with a shared symmetric key, the symmetric key should be different for each relying party and should be established using a secure process, symmetric keys are generally established during the registration of the relying party.
* If the assertion is passed through third parties, such as a browser, the actual assertion should be encrypted; if the assertion passed directly between the service provider and the relying party, the actual assertion should either be encrypted or be sent over an authenticated protected channel.
* All encryption algorithms should be currently approved by NIST for use by Federal agencies.
 |
| <enter response here> |
| **8.7 Describe how the assertion implements the holder of key process (FAL3 only)** |
| **Target*** The assertion should specify that the relying party should require that the subscriber perform a holder-of-key verification.
* The assertion should contain a reference to the key that is to be used to perform holder-of-key verification.
* The assertion should not contain the symmetric key or private key that can be used to perform the holder-of-key verification.
 |
| <enter response here> |

# Credential Validation

Complete the tables by describing the processes used to support credential validation. If more than one process is supported, describe differences or create a new row for each distinct process. If described in a different table, referencing that table is sufficient; the process does not need to be described twice. Please refer to [Table 2](#bookmark=id.1pxezwc) for applicability.

Table 9: Credential Validation

|  |
| --- |
| **9.1 Describe service availability** |
| **Target*** To prevent denial of service to relying parties, the credential validation service should maintain a high level of service availability.
* Describe any scheduled maintenance windows when the service may regularly be unavailable.
* Describe any rate limits for use of the validation service.
 |
| <enter response here> |
| **9.2 Provide detailed information on how the private signing key used to digitally sign assertions is protected** |
| **Target*** Key should be generated and stored appropriately.
* Key size should have equivalent (or higher) entropy to RSA-2048.
* Generation and activation of key should be under multiparty control.
* If the key is backed up, all backups should also be stored and protected to the same level as the original.
* If the key is transferred between cryptographic modules, it should be encrypted in transit.
* How often is the signing system re-keyed?
 |
| <enter response here> |
| **9.3 Describe the process to register relying parties to the validation service** |
| **Target*** Delivery of the public key associated with the private signing key should use a secure out-of-band method.
* Describe the process for establishing trust between the relying party and the validation service.
* If key information needs to be transferred, then protocols requiring the transfer of keying information should use a secure method during the registration process to exchange keying information needed to operate the federated relationship, including any shared secrets or public keys.
* The trust agreement between the credential service provider and the relying party should establish the minimum and maximum IAL and AAL values for each connection.
 |
| <enter response here> |
| **9.4 Describe processes and procedures in place to address disaster recovery and business continuity** |
| **Target*** Provider should maintain a disaster recovery plan.
* Provider should have mechanisms in place to replace the signing key in the event of compromise or suspected compromise of the private signing key, and to provide relying parties with updated key information.
* Provider should have mechanisms in place to notify relying parties of signing key compromise or other incidents.
 |
| <enter response here> |
| **9.5 Describe your incident response plan for data breaches, including detection, reporting and investigation** |
| **Target*** Provider should maintain a incident response plan.
* Provider should have mechanisms in place to detect unauthorized access.
* Provider should have mechanisms in place to notify users and relying party customers.
 |
| <enter response here> |

# Additional Information

This section can be used to provide any additional information an agency should be aware of while evaluating this Credential Service Provider offering. A few topics are included in the following table, but additional lines can be added to ensure the offered capabilities are fully covered.

Table 10: Additional Information

|  |
| --- |
|  |
| **10.1 Describe what customizations are available for the user interface look and feel of the workflow to meet agency branding requirements** |
| <enter response here> |
| **10.2 Provide detailed information about procedures to work with an agency to continuously improve the identity proofing process and outcomes** |
| <enter response here> |
| **10.3 Describe the system maintenance process and whether the schedule can be tailored to meet agency requirements** |
| <enter response here> |
| **10.4 Describe processes used to train and evaluate performance, include:*** **risk model**
* **processes**
* **tools**
* **test data used to ensure coverage of broad demographics indicative of the target population**
 |
| <enter response here> |
| **10.5 Describe how users manage their consent to release attributes, revoke that consent and manage their account** |
| <enter response here> |
| **10.6 Provide the link to how users are informed about how their personal Information may be used** |
| <enter response here> |
| **10.7 Describe what information is available to customers to enable an appropriate privacy risk assessment** |
| <enter response here> |
| **10.8 Describe any service level metrics that are available to customers, such as:** * **operational capacity**
* **recovery capabilities**
* **contingency capability to provide services in the case of natural disaster affecting a wide geographic region**
* **failure rates, etc.**
 |
| <enter response here> |
| **10.9 If applicable, describe any mobile documents, that are accepted as identity documents, or how these may be added in the future.** |
| <enter response here> |
| **10.10 If applicable, describe any mobile documents that are accepted as authenticators, how your solution interfaces/integrates with the relying party, or how these may be added in the future.** |
| <enter response here> |

# Appendix A: NIST SP 800-63B Authenticator Types

The following table is based on 800-63B-4 Table 1: AAL Summary of Requirements. This is for information only to assist in categorizing how a supported authenticator meets the different AAL categories. Note if there is more than 1 x in a row, all authenticators in that row must be used in combination to meet the specified AAL.

Table 11: NIST SP 800-63B Authenticator Types

| x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **AAL** | **Single Factor Authenticators** | **Multi-Factor Authenticators** |
| **Biometric** | **Memorized Secret** | **Look-up Secret**  | **Out-of-band Device**  | **One-Time Password Software**  | **One-Time Password Device** | **Cryptographic Software**  | **Cryptographic Device**  | **Biometric Activated One-Time Password Software**  | **Memorized Secret Activated One-Time Password Software**  | **Biometric Activated One-Time Password Device**  | **Memorized Secret Activated One-Time Password Device** | **Biometric Activated Cryptographic Software** | **Memorized Secret Activated Cryptographic Software** | **Biometric Activated Cryptographic Device**  | **Memorized Secret Activated Cryptographic Device** |
| **AAL1.01** |  | **x** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **AAL1.02** |  |  | **x** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **AAL1.03** |  |  |  | **x** |  |  |  |  |  |  |  |  |  |  |  |  |
| **AAL1.04** |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |  |  |
| **AAL1.05** |  |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |  |
| **AAL1.06** |  |  |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |
| **AAL1.07** |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |  |  |
| **AAL1.08** |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |  |
| **AAL1.09** |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |
| **AAL1.10** |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |
| **AAL1.11** |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |
| **AAL1.12** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |
| **AAL2.01** |  |  |  |  |  |  |  |  | **x** |  |  |  |  |  |  |  |
| **AAL2.02** |  |  |  |  |  |  |  |  |  | **x** |  |  |  |  |  |  |
| **AAL2.03** |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |  |  |
| **AAL2.04** |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |  |
| **AAL2.05** |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |  |
| **AAL2.06** |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |  |
| **AAL2.07** |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |
| **AAL2.08** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |
| **AAL2.09** |  | **x** | **x** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **AAL2.10** |  | **x** |  | **x** |  |  |  |  |  |  |  |  |  |  |  |  |
| **AAL2.11** |  | **x** |  |  |  | **x** |  |  |  |  |  |  |  |  |  |  |
| **AAL2.12** |  | **x** |  |  |  |  | **x** |  |  |  |  |  |  |  |  |  |
| **AAL2.13** |  | **x** |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |
| **AAL3.01** |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |  |
| **AAL3.02** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** |
| **AAL3.03** | **x** |  |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |
| **AAL3.04** |  | **x** |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |
| **AAL3.05** |  |  |  |  |  | **x** |  |  |  |  |  |  | **x** |  |  |  |
| **AAL3.06** |  |  |  |  |  | **x** |  |  |  |  |  |  |  | **x** |  |  |
| **AAL3.07** |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  | **x** |  |
| **AAL3.08** |  |  |  |  |  | **x** |  |  |  |  |  |  |  |  |  | **x** |
| **AAL3.09** |  | **x** |  |  |  | **x** | **x** |  |  |  |  |  |  |  |  |  |

# Appendix B: Source Documents

Targets sourced from:

[NIST SP 800-63](https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines)

[NIST SP 800-63-4](https://csrc.nist.gov/pubs/sp/800/63/4/ipd)

[Conformance Criteria for NIST SP 800-63](https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines)