Federal Identity, Credentialing, and Access Management

Trust Framework Provider Adoption Process (TFPAP)

For Levels of Assurance 1, 2, and Non-PKI 3

Version 1.0.1

Release Candidate

September 4, 2009

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	4/15/09	Initial Draft	Client
Draft	0.0.2	4/20/09	Revised per client inputs	Client
Draft	0.0.3	4/26/09	Revised per client inputs	Internal
Draft	0.0.4	4/27/09	Revised per internal discussion	Internal
Draft	0.0.5	4/30/09	Revisions per internal review	Client
Draft	0.0.6	5/3/09	Revisions per client inputs	Client
Draft	0.1.0	5/26/09	Revisions per client inputs	Internal
Draft	0.1.1	5/26/09	Revisions per internal review	Limited Distribution
Draft	0.1.2	6/1/09	Revisions per limited distribution feedback	Limited Distribution
Draft	0.1.3	6/5/09	Revisions per limited distribution feedback. Includes (a) addition of TFP organizational maturity assessment (Section 3.2), (b) additions to Trust Criteria, (c) reordering of trust criteria to better synchronize across assurance levels.	Limited Distribution
Draft	0.1.4	6/10/09	Revised per red line edits and comments (e.g., typos) received from limited distribution feedback.	Limited Distribution
Draft	0.1.5	6/18/09	Added Privacy discussion.	Limited Distribution
Draft	0.1.6	6/22/09	Revised per client inputs.	Limited Distribution
Draft	0.1.7	6/29/09	Revised per internal review.	Limited Distribution
Draft	0.1.8	7/6/09	Renamed from v1.0.0 Revised per external comments.	Limited Distribution
Draft	0.1.9	7/7/09	Revised per comments from CIO Council privacy WG.	Limited Distribution
Release Candidate	1.0.0	8/4/09	Revised per internal review.	General Distribution
Release Candidate	1.0.1	8/26/09	Revised per feedback. Corrected references to section 3.3. Added bold/italic notice as the last paragraph to Section 3.1. Deleted “on behalf of ICAM” in all TFP definitions/requirements. Added stipulation that full ICAMSC can designate another entity to vote on approval.	General Distribution

Editors

Dr. Peter Alterman	Judith Spencer	Chris Louden
Terry McBride	Dave Silver	Steve Lazerowich
David Wasley	Mary Ruddy	Brett McDowell
Toby Levin	Amber Smith	Dawn Wiggins
Debra Diener	Kellie Riley	Naomi Lefkowitz
James McCartney	Dr. Deborah Lafky	Niels Quist
Alan Lane	Debbie Bucci	

Executive Summary

It is in the government's best interest to leverage industry resources whenever possible. To support E-Government activities, Identity, Credential, and Access Management (ICAM) aims to leverage industry based credentials that citizens already have for other purposes. In order to ensure these credentials are trustworthy, the government requires a mechanism to assess these credentialing processes against federal requirements as codified by Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and General Services Administration (GSA). Industry-based frameworks to assess the trustworthiness of electronic credentials already exist and can be leveraged by the government. This approach enables a scalable model for extending identity assurance across a broad range of citizen and business needs. These *Trust Frameworks* include requirements for trust framework provider (TFP) auditing qualifications and processes, TFP organizational maturity, TFP member identity provider organizational maturity, TFP member identity provider credentials and their issuance, and TFP member identity provider privacy policies,

This document defines a process whereby the government can assess the efficacy of the Trust Frameworks for federal purposes so that an Agency online application or service can trust an electronic identity credential provided to it at a known level of assurance comparable to one of the four OMB Levels of Assurance. Trust Frameworks that are comparable to federal standards are *adopted* through this process, allowing federal relying parties to trust credential services that have been assessed under the framework. The adoption process is as follows:

1. **Assessment package submission** – the Applicant TFP provides evidence of comparability to federal standards for (a) TFP member identity providers' credentials for a specific level or levels of assurance, (b) TFP organizational maturity, (c) TFP auditor qualifications, (d) TFP auditing processes, and (e) privacy criteria for TFP member identity providers;
2. **Value determination** – Identity, Credential, and Access Management Sub Committee (ICAMSC) determination whether an Applicant's trust framework is worth assessing;
3. **Comparability assessment** – if value determination indicates applicant is worth assessing, assessment as to whether the Applicant's trust framework criteria for its member Identity Providers are comparable to one or more specific levels of assurance, that its auditor qualifications, auditing processes, and ongoing recertification processes are sufficient, and that its privacy criteria for member Identity Providers are comparable to ICAM requirements; and
4. **Adoption decision** – after reading the Assessment Report, the ICAMSC (or designated other) votes on whether to adopt the Applicant and its trust framework.

This trust framework covers remote electronic authentication of human users to IT systems over a network. It does not address the authentication of a person who is physically present. At OMB Levels of Assurance 3 and 4, the ICAMSC relies on the proven criteria and methodology of the FPKI Policy Authority. At OMB Levels of Assurance 1, 2, and non-PKI 3 (as defined in NIST Special Publication 800-63), each Identity Provider and TFP must demonstrate trust comparable to each of five categories (registration and issuance, tokens, token and credential management, authentication process, and assertions) for each Level of Assurance it wishes its credentials trusted by government applications. TFPs demonstrate comparability to the ICAMSC. Identity Providers demonstrate comparability to a TFP.

Subsequent to adoption, a TFP is subject to periodic comparability audits, and possibly discontinuance (i.e., no longer acceptable to the Federal government).

The ICAM Program will evolve over time. As the needs of the Program change or become clearer, it is likely that the trust framework adoption process will evolve. Draft revisions of this document will be made available to applicable Federal government agencies and organizations, including TFPs, for comment. Those comments will be provided to the ICAMSC for consideration and possible inclusion before final revision.

Table of Contents

Figures

1. BACKGROUND

The General Services Administration (GSA) Office of Governmentwide Policy (OGP) is responsible for government-wide coordination and oversight of Federal Identity, Credential, and Access Management (ICAM), comprised of Federal Public Key Infrastructure (FPKI), Federal Identity Credentialing (HSPD-12) [1] and E-Authentication activities. These activities are aimed at improving Electronic government services internally, with other government partners, with business partners, and with the American public.

On October 1, 2008, the GSA began to transition from the current E-Authentication Program Management Office hosted by the Federal Acquisition Service to an interagency governance model managed by the OGP. In so doing, E-Authentication became an integral part of the ICAM Program. One outcome of this move is a transition away from a Federation model to an open model that promotes multiple solutions to comply with Office of Management and Budget (OMB) M-04-04 [2] and that encourages agency innovation. GSA's long-range vision for Identity Management in government is a broad spectrum of solutions embracing open private sector solutions and high assurance, cybersecurity initiatives such as HSPD-12.

The Information Security and Identity Management Committee (ISIMC) is the Federal CIO Council's (FCIOC) locus of responsibility for cybersecurity and identity management. Comprised of senior agency officials, this committee has been assigned executive decision making authority and oversight for the ICAM roadmap and architecture development.

The high-level strategic goals and objectives for ICAM include:

1. Government-wide implementation of OMB M-04-04;
2. Physical Access Control;
3. Logical Access Control;
4. Consolidation of credentialing and authentication capabilities to comply with OMB M-06-22 [3] ; and
5. Developing clearly-defined processes and capabilities for enabling trust across the Federal government and between the Federal government and its external constituencies.

The outcomes of a successful ICAM include:

1. Realizing cost-savings by eliminating agency legacy credential systems through use of standards-based authentication utilities;
2. Exploiting economies of scale by leveraging Federal buying power for both credentialing and credential validation functions;
3. Providing the capability to re-use credentials across applications, eliminating the need to create and maintain a credential system for each application; and
4. Improving the security and privacy posture of the Federal government.

It is in the government's best interest to leverage industry resources whenever possible. To support E-Government activities, ICAM aims to leverage industry-based credentials that citizens already have for other purposes. In order to ensure these credentials are trustworthy, the government requires processes to assess these credentialing processes against federal requirements as codified by OMB, National Institute of Standards and Technology (NIST), and GSA. Industry-based frameworks to assess the trustworthiness of electronic credentials already exist and can be leveraged by the government. This approach enables a scalable model for extending identity assurance across a broad range of citizen and business needs. These

Trust Frameworks include requirements for the credentials and their issuance, as well as for auditing qualifications and processes.

This document defines a process whereby the government can assess the efficacy of the Trust Frameworks for Federal purposes so that an Agency online application or service can trust an electronic identity credential provided to it at a known level of assurance (LOA) comparable to one of the four OMB Levels of Assurance. Trust Frameworks that are comparable to federal standards are *adopted* through this process, allowing federal Relying Parties (RPs) to trust credential services that have been assessed under the trust framework.

2. INTRODUCTION

Critical to the success of the ICAM Program is the assessment and adoption of trust framework providers (TFPs) that best serve the interests of the Federal government. A TFP is an organization that defines or adopts an on-line identity trust model and then certifies[1] identity providers compliant with that model. Adoption means that any identity provider certified by that TFP is qualified to provide identity assertions to Federal agencies. The ICAM Sub Committee (ICAMSC) must determine that the TFP's trust model and processes are comparable to one or more of the trust models defined herein. This model scales readily.

The following adoption process, based on guidance from OMB and NIST, and review from private sector partners, provides a consistent, standard, structured means of identifying, vetting, and approving TFPs. In addition, this structured process provides assurance to all ICAM RPs of the validity, and thus dependability, of identity credentials and tokens. This confidence is essential to government-wide acceptance and use of non-local credentials.

Specifically, the ICAM model is based on comparing the policies and practices of non-Federal government TFPs to the risks and trust assurance outcomes of OMB M-04-04 and NIST Special Publication (SP) 800-63 [4]. There are five (5) trust criteria categories:

1. **Registration and Issuance** – how well does the credential service provider (Identity Provider) register and proof the identity of the credential applicant, and issue the credential to the approved applicant?
2. **Tokens** – What is the Identity Provider's token technology and how well does the technology intrinsically resist fraud, tampering, hacking, and other such attacks?
3. **Token and Credential Management** – how well does the Identity Provider manage and protect tokens and credentials over their full life cycle?
4. **Authentication Process –** how well does the Identity Provider secure its authentication protocol?
5. **Assertions –** how well does the Identity Provider secure Assertions, if used, and how much information is provided in the Assertion?

This trust framework covers remote electronic authentication of human users to IT systems over a network. It does not address the authentication of a person who is physically present.

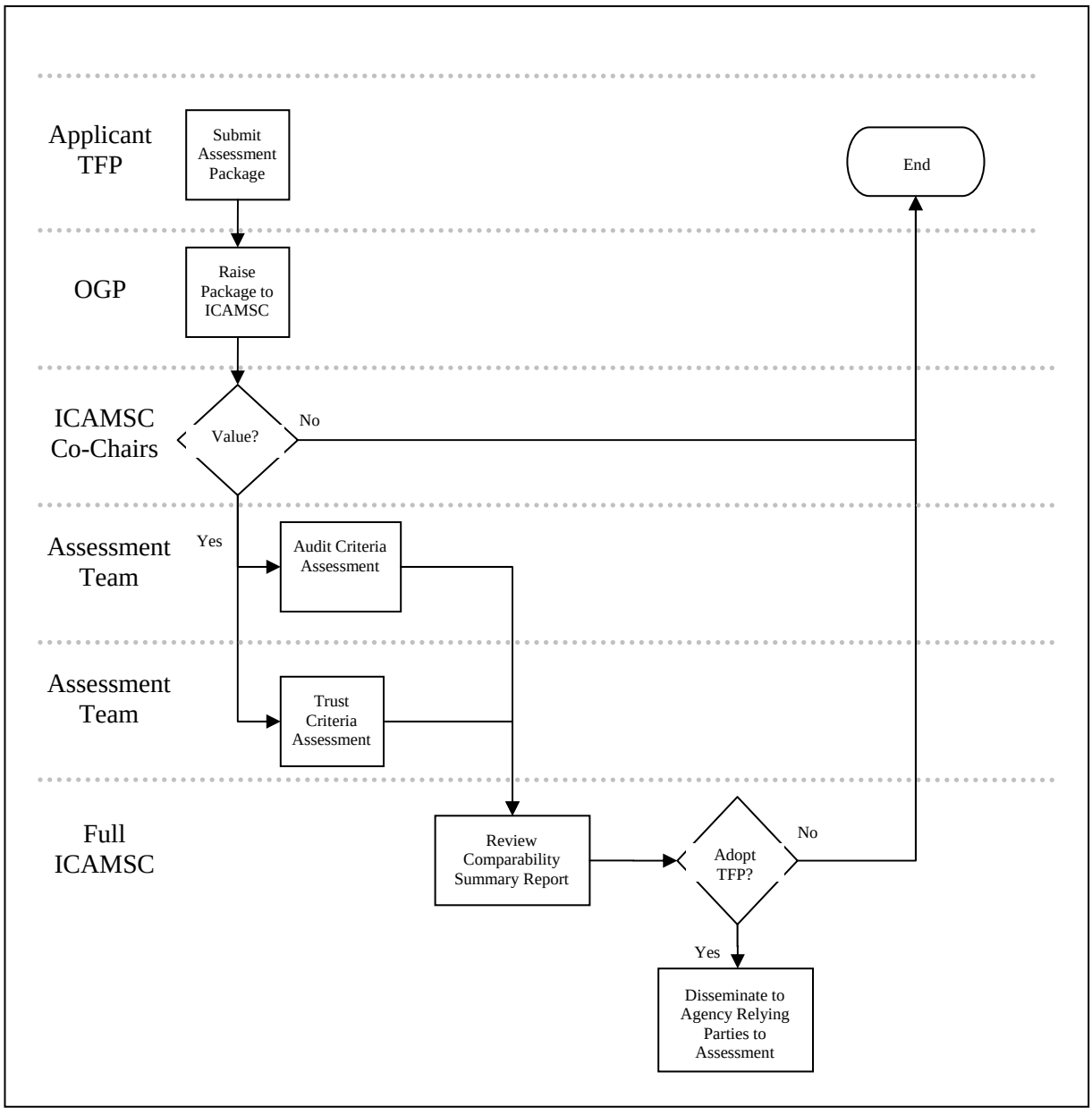
[1] TFP certification of an identity provider is the determination that the identity provider's policies and practices are comparable to ICAM trust requirements.

At OMB LOA 3 and 4, the ICAM relies on the proven criteria and methodology of the FPKI Policy Authority (FPKIPA). At OMB LOA 1, 2, and non-PKI 3 (as defined in NIST SP 800-63), ***each Identity Provider and TFP must demonstrate comparable trust in each of the above categories for each LOA it wishes its credentials to be trusted by government applications (including physical access control systems). TFPs demonstrate comparability to the ICAMSC. Identity Providers demonstrate comparability to a TFP.***

3. ADOPTION PROCESS

This section specifies the TFP adoption process. Figure 3-1 illustrates the high-level process flow.

Figure 3-1 High-Level TFP Adoption Process Flow



3.1 Assessment Package Submission

The process begins with an Applicant TFP (Applicant) submitting an Assessment Package to OGP, which then raises the submission to the ICAMSC[2]. The Assessment Package must include the framework's trust specifications with respect to applicable NIST SP 800-63 LOA trust criteria listed in Appendix A, the framework's privacy specifications with respect to Section 3.3 privacy criteria[3], the Applicant's audit and re-certification processes, the Applicant's auditor qualifications, and evidence of the Applicant's organizational maturity. The Assessment Package must build the case that the Applicant's trust model and practices are comparable at the desired LOA. Applicants are not required to submit their assertions in any particular format, nor are they required to comply strictly with any particular trust criterion. Instead, the Applicant must demonstrate that its trust specifications meet or exceed the trust criteria in NIST SP 800-63. Failure to comply with any particular requirement is not fatal, since alternative mitigation strategies[4] may satisfy trust criteria, especially at LOA 1 and LOA 2.

The Applicant's submission must directly and explicitly build the comparability case for all TFPAP criterions. It is unacceptable to merely present supporting documents, for example, and expect the Assessment Team to take on the burden of searching for comparability and building the case for the Applicant. Submissions that place the burden of building the case for comparability on the Assessment Team will be returned to the Applicant, which may cause delay in adoption.

3.2 Value Determination

The ICAMSC Co-Chairs determine whether adoption of the Applicant would be valuable to Federal Agencies. In doing so, the Co-Chairs consider whether the Applicant has (or is gaining) industry recognition, whether the Applicant has direct applicability to the Federal government, and other factors as appropriate. As part of the determination discussion, the ICAMSC Co-Chairs (or designated Team) assess the Applicant's organizational maturity, which may include, but is not limited to the following:

- Applicant legal status;
- Appropriate authorization to operate;
- Legal authority to commit the Applicant to conducting assessments and certifying Identify Providers;
- Financial capacity to manage the risks associated with conducting assessments and certifying Identify Providers;
- Understanding of, and compliance with any legal requirements incumbent on the Applicant in connection to conducting assessments and certifying Identify Providers;
- Scope and extent of implemented security controls (e.g., access control, confidentiality of Identity Provider information);
- Documentation of policies and procedures;
- Proof that Applicant practices are consistent with documented policies and procedures (e.g., via independent auditor reports, if required by LOA requirements).

---

[2] This buffers the process from changes in leadership at ICAMSC in the future. It also ensures an operational methodology to the overall adoption process.

[3] To that end, privacy experts from the CIO Council Privacy Committee will have the opportunity to participate in the TFP assessments.

[4] This is also known as "compensating controls".

The Assessment Team may request Applicant *bona fides* to assess Applicant organizational maturity, legitimacy, stability, and reputation. Additional effort is not expended on this Trust Framework unless it is determined to be in the best interest of the government.

3.3 Comparability Assessment

The ICAMSC directs OGP to establish one or more Assessment Teams to formally review the Applicant at the desired LOA(s). During an assessment, the Assessment Team communicates with the Applicant to ensure accuracy and to allow the Applicant to remedy identified deficiencies. There are two comparability assessments:

- **Trust Criteria Assessment** – Assessment Team determines whether criteria applied by the Applicant to its member identity providers are comparable to ICAM criteria. Trust criteria assessment includes:
    1. Technical and policy comparability based upon the Appendix A trust criteria;
    2. Privacy policy comparability using the following criteria:
        a. **Opt In** – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.
        b. **Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.
        c. **Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.
        d. **Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.
        e. **Non Compulsory** – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.
        f. **Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.
    3. Determination of whether the Applicant sufficiently reviews member identity provider *bona fides* to ensure member identity provider organizational maturity, legitimacy, stability, and reputation.
- **Audit Criteria Assessment** – where appropriate, Assessment Team reviews:
    1. Applicant auditor qualifications. At a minimum, the Applicant's auditors must:
        a. Demonstrate competence in the field of compliance audits;
        b. Be thoroughly familiar with all requirements that the Applicant imposes on member identity providers;
        c. Perform such audits as a regular ongoing business activity; and

   d. Be Certified Information System Auditors (CISA) and IT security specialist – or equivalent.
2. Applicant processes used to audit its member identity providers; and
3. Ongoing Applicant processes used to re-certify Applicant member identity providers.

An Assessment Team will typically consist of three (3) Assessors. Each Assessor will have demonstrated professional competency directly relevant to the assessment. To ensure consistency and fairness of the assessment process, assessments may be video or audio taped, detailed meeting minutes shall be taken, and/or an ombudsman may be present throughout the process[5].

The assessment process is flexible, and depends upon the needs of the Assessment Team. In general, the Team begins by reviewing the Applicant's submission. The Team may meet with the Applicant one or more times throughout the assessment process to ask questions or obtain clarifications. Such meetings become part of the assessment record. When the Team has sufficient information, it makes a final determination of comparability at the desired LOA(s). The Team may determine that there is no comparability at any LOA. The Team documents its findings, with all applicable supporting information, in a Summary Report specific to an Applicant. The Summary Report indicates:

1. The extent of the Applicant's comparability to the Federal government for each relevant Appendix A technical and policy trust criteria category;
2. The extent of the Applicant's comparability to the Federal government for each Section 3.3 privacy policy;
3. Sufficiency of the Applicant's review of the *bona fides* of its member identity providers; and
4. Sufficiency of the Applicant's auditor qualifications, auditing processes, and recertification processes.

3.4 ICAMSC Adoption Decision

The Full ICAMSC (or designated other) reviews the Summary Report for the Applicant, and votes on whether to adopt the Applicant. Upon adoption, the Applicant is added to the *Approved TFP List* maintained by OGP and posted on appropriate websites; agencies may be notified of the adoption, and the TFP can be used by the Federal government.

4. ONGOING ACTIVITIES

An adopted TFP is subject to the following:

- Determination as to whether the TFP should be discontinued (i.e., no longer acceptable to the Federal government), as requested by any ICAMSC member. Discontinuance may be for reasons including, but not limited to, no longer applicable to the Federal government, no longer comparable with applicable ICAMSC requirements; failure to abide by terms of original agreement; etc.
- Comparability audit (i.e., another comparability mapping), as requested by any ICAMSC member; and

[5] If the fairness of the process is questioned, the Ombudsman may be asked to "certify" in a report that the assessment was consistent and fair.

- Comparability audit due to some length of time since last audit (e.g., every three years) or a significant change to TFP operations or policies.

5. ADOPTION PROCESS MAINTENANCE

The ICAM Program will evolve over time. As the needs of the Program change or become clearer, it is likely that the trust framework adoption process will evolve. The ICAMSC oversees trust framework adoption process maintenance. Draft revisions of this document will be made available to applicable Federal government agencies and organizations, including TFPs, for comment. Those comments will be provided to the ICAMSC before the final revision is approved. Any ICAMSC member can request revision to this document, as circumstances warrant.

APPENDIX A – TRUST CRITERIA

The below sets of Trust Criteria for LOA 1 through 4 are taken verbatim from NIST SP 800-63 and appear in column 1. Column 2 provides clarification or explanation around the intent of the corresponding criteria in Column 1. For additional background and context per trust criterion, read the entire applicable section of NIST SP 800-63.

Many of these criteria apply at more than one LOA. For convenience of the reader, all criteria applicable to each LOA are included in the tables for that LOA. In some cases, the parameters of a common criterion (e.g., required password entropy) may be different between LOAs.

A-1 Assurance Level 1

Registration and Issuance

Assurance Level 1 R&I Trust Criteria	Comment
1. A trusted relationship always exists between the RA and Identity Provider.	Mechanisms and policies should be in place to ensure each party and its obligations are known to the other.
2. Sensitive data collected during the registration stage must be protected at all times (e.g. transmission and storage) to ensure its security and privacy.	Sufficiently protect all sensitive data including PII (as defined by the Federal Government; See Appendix C) obtained during registration.
3. Resist token issuance disclosure threat.	Issue token in a manner that protects confidentiality of information.
4. Resist token issuance tampering threat.	Establish a procedure that allows the Subscriber to authenticate the CSP as the source of any token and credential data that he or she may receive.
5. Resist unauthorized token issuance threat.	Establish procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure.
6. Some effort should be made to uniquely identify and track applications.	"Applications" means "requests for token". The intent is to ensure that the same party acts as Applicant throughout the registration, and token and credential issuance processes.

Tokens

Assurance Level 1 Tokens Trust Criteria	Comment
1. Resist token duplication threat.	Protect against a Subscriber's token being copied with or without his or her knowledge (e.g., use tokens that are hard to copy).
2. Resist social engineering threat.	Protect against an Attacker establishing a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret.
3. For memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, and out of band tokens, the probability that an Attacker can guess a valid authenticator, over the lifetime of the token, must be less than 2^{-10} (1 in 1024).	The maximum probability that, over the life of the password, an Attacker with no *a priori* knowledge of the password will succeed in an in-band password guessing attack. See NIST SP 800-63 Appendix A for complete discussion.

Token and Credential Management

Assurance Level 1 T&C Management Trust Criteria	Comment
1. Files of shared secrets used by Verifiers shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall not contain the plaintext passwords.	Sufficiently protect shared secrets such as passwords.
2. Long term token secrets should not be shared with other parties unless absolutely necessary.	Any secret (e.g., password, PIN, key) involved in authentication shall not be disclosed to third parties by verifier or CSP, unless absolutely necessary and appropriate (e.g., with Federal ICAM infrastructure elements).

Authentication Process

Assurance Level 1 Authentication Process Trust Criteria	Comment
1. Resist online guessing threat.	Protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. Resist replay threat.	Protect against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.
3. Successful authentication requires that the Claimant shall prove, through a secure authentication protocol, that he or she controls the token.	Ensure that the Claimant (person being authenticated) actually possesses the token.
4. Plaintext passwords or secrets shall not be transmitted across a network.	A network is an open communications medium, typically the Internet, used to transport messages between the Claimant and other parties.

Assertions

Assurance Level 1 Assertions Trust Criteria	Comment
1. Use an ICAM adopted authentication scheme.	Use of any ICAM adopted authentication scheme defined for this assurance level is acceptable.

A-2 Assurance Level 2

LOA 2 PKI is out of scope for this document, and is addressed in *Criteria and Methodology For Cross Certification With the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA)* [11][6]. For Assurance Level 2 non-PKI authentication (e.g., memorized secret token), the following applies:

Registration and Issuance

Assurance Level 2 R&I Trust Criteria	Comment
1. A trusted relationship always exists between the RA and Identity Provider.	Mechanisms and policies should be in place to ensure each party and its obligations are known to the other.
2. Sensitive data collected during the registration and identity proofing stage must be protected at all times (e.g. transmission and storage) to ensure its security and privacy.	Sufficiently protect all sensitive data including PII (as defined by the Federal Government; See Appendix C) obtained during registration and identity proofing.
3. Resist token issuance disclosure threat.	Issue token in a manner that protects confidentiality of information.
4. Resist token issuance tampering threat.	Establish a procedure that allows the Subscriber to authenticate the CSP as the source of any token and credential data that he or she may receive.
5. Resist unauthorized token issuance threat.	Establish procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure.
6. To ensure that the same party acts as Applicant throughout the process, the Applicant shall identify himself/herself in any new electronic transaction (beyond the first transaction or encounter) by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or physical address of record. The Applicant shall identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter.	Registration, identity proofing, and token and credential issuance represent different goals of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. (Two electronic transactions are considered to be separate if they are not part of the same protected session.) In these cases, the following methods shall be used to ensure that the same party acts as Applicant throughout the process.
7. Resist repudiation of registration threat.	Protect against a Subscriber denying registration, claiming that they did not register that token.
8. Applicant undergoes identity proofing by a trusted Registration Authority (RA).	Requires presentation of identifying materials or information.

[6] When PKI certificate-based authentication is to an Identity Provider (rather than directly to the RP), assertion processing is also required and must additionally follow assertion table trust criteria.

Assurance Level 2 R&I Trust Criteria	Comment
9. Either the RA or the Identity Provider shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including the evidence required below.	A record of the facts of registration and proofing.
10. The Identity Provider shall be prepared to provide records of identity proofing to Relying Parties as necessary.	In the event of detected or suspected identity fraud the Identity provider may be required to provide the detailed records of registration and credential issuance as part of an investigation.
11. The identity proofing and registration process shall be performed according to a written policy or *practice statement* that specifies the particular steps taken to verify identities.	The practice statement should address primary objectives of registration and identity proofing.
12. If the RA and Identity Provider are remotely located, and communicate over a network, the entire registration transaction between the RA and Identity Provider shall be cryptographically authenticated using an authentication protocol that meets Level 2 requirements, and any secrets transmitted shall be encrypted using an Approved encryption method.	See Appendix C for definition of "Approved".
13. The Identity Provider shall be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. The Identity Provider shall be capable of conveying this information to Verifiers and Relying Parties.	Ensure a person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person.
14. The name associated with the Subscriber may be pseudonymous but the RA or Identity Provider shall know the actual identity of the Subscriber. In addition, pseudonymous Level 2 credentials must be distinguishable from Level 2 credentials that contain meaningful names.	Associate a person's pseudonym to the person's real name. Support a mechanism to specify whether the name in the credential is real or pseudonym.
15. The results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality and integrity.	Sufficiently protect all identity proofing information and ensure it comes from known, trusted sources.
16. Applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other individual identifying information.	
17. For In-Person Proofing – Possession of a valid current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality (e.g. driver's license or Passport). Inspect photo-ID, compare picture to Applicant, record ID number, address and DoB. If ID appears valid and photo matches Applicant then: a. If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or; b. If ID does not confirm address of record, issues credentials in a manner that confirms address of record.	If ID does not confirm address of record, then the issuance process should include a mechanism to confirm the address of record.

Assurance Level 2 R&I Trust Criteria	Comment
18. For Remote Proofing – Possession of a valid Government ID (e.g. a driver's license or Passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Inspect both ID number and account number supplied by Applicant (e.g. for correct number of digits). Verifies information provided by Applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Address confirmation and notification: a. Sends notice to an address of record confirmed in the records check or; b. Issues credentials in a manner that confirms the address of record supplied by the Applicant; or c. Issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or e-mail at number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.	
19. If the exact number of tokens to be issued is not agreed upon early in the registration process, then the tokens should be distinguishable so that Verifiers will be able to detect whether any suspicious activity occurs during the first few uses of a newly issued token.	A common reason for breaking up the registration process as described above is to allow the subscriber to register or download software tokens in two or more different computing environments. This is permissible as long as the tokens individually meet the appropriate assurance level.
20. Federally regulated financial institutions, brokerages and dealers may issue credentials to their customers via the mechanisms normally used for on-line banking or brokerage credentials, and may use on-line banking or brokerage credentials and tokens as Level 2 E-authentication credentials and tokens, provided they meet the provisions Level 2.	Federal law, including the Bank Secrecy Act and the USA Patriot Act, impose a duty on financial institutions to "know their customers" and report suspicious transactions to help prevent money laundering and terrorist financing. Many financial institutions are regulated by Federal Agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC). These regulators normally require the intuitions to implement a Customer Identification Program. These provisions apply to Federally regulated financial institutions, brokerages and dealers subject to such Federal regulation, that implement such a Customer Identification Program.

Tokens

Assurance Level 2 Tokens Trust Criteria	Comment
1. Resist token theft threat.	Protect a token with a physical manifestation (e.g., one time password device, hardware cryptographic device) from being stolen by an Attacker.
2. Resist token duplication threat.	Protect against a Subscriber's token being copied with or without his or her knowledge (e.g., use tokens that are hard to copy).
3. Resist social engineering threat.	Protect against an Attacker establishing a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret.
4. For memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, and out of band tokens, the probability that an Attacker can guess a valid authenticator, over the lifetime of the token, must be less than 2^{-14} (1 in 16,384).	The maximum probability that, over the life of the password, an Attacker with no *a priori* knowledge of the password will succeed in an in-band password guessing attack. See NIST SP 800-63 Appendix A for complete discussion.
5. When a multi-factor token or a multi-token authentication scheme is being used, the security properties of each factor or of each token are considered additive in nature. If one factor of a multi-factor scheme or one token of a multi-token scheme has the desired properties for a given assurance level, it is considered sufficient.	Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained.
6. For single token schemes that use one token to gain access to a second token, the compound solution is only as strong as the token with the lowest assurance level.	The solution is only as strong as its weakest link.
7. For memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, and out of band tokens, authenticators must have greater than 10 bits of min-entropy.	See NIST SP 800-63 Appendix A for complete discussion. Min-entropy is a measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity.
8. For out of band tokens, the authenticator must have a limited lifetime, on the order of minutes and can only be used once.	
9. Single factor one time password devices must use Approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password. The cryptographic module performing this operation shall be validated at FIPS 140-2 Level 1 or higher. The nonce may be a date and time, or a counter generated on the device. The one-time password must have a limited lifetime, on the order of minutes.	See Appendix C for definition of "Approved". See Appendix B for reference to FIPS 140-2 document.
10. For single factor cryptographic devices, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.	See Appendix B for reference to FIPS 140-2 document.

Token and Credential Management

Assurance Level 2 T&C Management Trust Criteria	Comment
1. Files of shared secrets used by Identity Providers at Level 2 shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall not contain the plaintext passwords or secrets; two alternative methods may be used to protect the shared secret: a. Passwords may be concatenated to a variable salt (variable across a group of passwords that are stored together) and then hashed with an Approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file. The variable salt may be composed using a global salt (common to a group of passwords) and the username (unique per password) or some other technique to ensure uniqueness of the salt within the group of passwords. b. Shared secrets may be stored in encrypted form using Approved encryption algorithms and modes, and the needed secret decrypted only when immediately required for authentication. In addition, any method allowed to protect shared secrets at Level 3 or 4 may be used at Level 2.	Sufficiently protect shared secrets such as passwords. See Appendix C for definition of “Approved”.

Assurance Level 2 T&C Management Trust Criteria	Comment
2. Long term shared authentication secrets, if used, shall never be revealed to any party except the Subscriber and Identity Provider (including Verifiers operated as a part of the Identity Provider); however, session (temporary) shared secrets may be provided by the Identity Provider to independent Verifiers. Cryptographic protections are required for all messages between the Identity Provider and Verifier which contain private credentials or assert the validity of weakly bound or potentially revoked credentials. Private credentials shall only be sent through a protected channel to an authenticated party to ensure confidentiality and tamper protection. The Identity Provider may send the Verifier a message, which either asserts that a weakly bound credential is valid, or that a strongly bound credential has not been subsequently revoked. In this case, the message shall be logically bound to the credential, and the message, the logical binding, and the credential shall all be transmitted within a single integrity protected session between the Verifier and the authenticated Identity Provider. If revocation is an issue, the integrity protected messages shall either be time stamped, or the session keys shall expire with an expiration time no longer than that of the revocation list. Alternatively, the time stamped message, binding, and credential may all be signed by the Identity Provider, although, in this case, the three in combination would comprise a strongly bound credential with no need for revocation.	Sufficiently protect long term shared authentication secrets.
3. The Identity Provider shall establish suitable policies for renewal and re-issuance of tokens and credentials. Proof-of-possession of the unexpired current token shall be demonstrated by the Claimant prior to the Identity Provider allowing renewal and re-issuance. Passwords shall not be renewed; they shall be re-issued. After expiry of current token, renewal and re-issuance shall not be allowed. All interactions shall occur over a protected channel such as SSL/TLS. Secondary credentials must never be renewed or re-issued.	

Assurance Level 2 T&C Management Trust Criteria	Comment
4. Identity Providers shall revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised to ensure that a Claimant using the token cannot successfully be authenticated. If the Identity Provider issues credentials that expire automatically within 72 hours (e.g. issues fresh certificates with a 24 hour validity period each day) then the Identity Provider is not required to provide an explicit mechanism to revoke the credentials. Identity Providers that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours. CAs cross-certified with the Federal Bridge CA at the Citizen and Commerce Class Basic, Medium and High or Common Certificate Policy levels are considered to meet credential status and revocation provisions of this level. Secondary credentials must have a lifetime less than 12 hours.	For PKI credentials, Federal ICAM relies on the proven criteria and methodology of the FPKIPA.
5. A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the Identity Provider or its representative. The record retention period of data for Level 2 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. Identity Providers operated by or on behalf of executive branch agencies shall also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.	
6. Tokens can be renewed using out of band delivery mechanisms. If the Subscriber uses an out of band token delivery approach, re-registration of the delivery mechanism can be equated to token renewal or re-issuance. In such a case, the subscriber must use an alternate, yet already registered delivery mechanism to deliver the token and then gain access to the Identity Provider such that the registration data can be updated by the Subscriber or, if no alternate out of band channel was registered with the original out of band channel the subscriber must re-establish their identity with the Identity Provider in order to update their registration data.	
7. The Identity Provider should establish policies for token collection to avoid the possibility of unauthorized use of the token after it is considered out of use.	The Identity Provider may destroy such collected tokens, or zeroize them to ensure that there are no remnants of information that can be used by an Attacker to derive the token value.

Authentication Process

Assurance Level 2 Authentication Process Trust Criteria	Comment
1. Resist online guessing threat.	Protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. Resist replay threat.	Protect against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.
3. Successful authentication requires that the Claimant shall prove, through a secure authentication protocol, that he or she controls the token.	Ensure that the Claimant (person being authenticated) actually possesses the token.
4. Plaintext passwords or secrets shall not be transmitted across a network.	A network is an open communications medium, typically the Internet, used to transport messages between the Claimant and other parties.
5. Resist session hijacking threat.	Protect against an Attacker being able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the Subscriber.
6. Resist eavesdropping threat. Approved cryptography is required to resist eavesdropping.	Protect against an attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant. See Appendix C for definition of “Approved”.
7. Weakly resist man-in-the-middle threat.	Protect against an attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. A protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.
8. The authentication process shall provide sufficient information to the Verifier to uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time of registration, and (ii) verified by the RA in the issuance of the token and credential.	Ensure the authentication process can uniquely identify each Subscriber and the associated tokens and credentials issued to that Subscriber.

Assurance Level 2 Authentication Process Trust Criteria	Comment
9. Session data transmitted between the Claimant and the Relying Party following a successful Level 2 authentication must be protected as described in the NIST FISMA guidelines. Specifically, all session data exchanged between information systems that are categorized as FIPS 199 "Moderate" or "High" for confidentiality and integrity, shall be protected in accordance with NIST SP 800-53 Control SC-8 (which requires transmission confidentiality) and SC-9 (which requires transmission integrity).	Protect data exchanged between the end user and the Relying Party. See Appendix B for reference to FIPS 199 and NIST SP 800-53 documents.

Assertions

Assurance Level 2 Assertions Trust Criteria	Comment
1. Use an ICAM adopted authentication scheme.	Use of any ICAM adopted authentication scheme defined for this assurance level is acceptable.

A-3 Assurance Level 3

LOA 3 PKI is out of scope for this document, and is addressed in *Criteria and Methodology For Cross Certification With the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA)* [11][7]. For Assurance Level 3 non-PKI authentication (e.g., One Time Password device), the following applies:

Registration and Issuance

Assurance Level 3 R&I Trust Criteria	Comment
1. A trusted relationship always exists between the RA and Identity Provider.	Mechanisms and policies should be in place to ensure each party and its obligations are known to the other.
2. The sensitive data collected during the registration and identity proofing stage must be protected at all times (e.g. transmission and storage) to ensure its security and privacy.	Sufficiently protect all sensitive data including PII (as defined by the Federal Government; See Appendix C) obtained during registration and identity proofing.
3. Resist token issuance disclosure threat.	Issue token in a manner that protects confidentiality of information.
4. Resist token issuance tampering threat.	Establish a procedure that allows the Subscriber to authenticate the CSP as the source of any token and credential data that he or she may receive.
5. Resist unauthorized token issuance threat.	Establish procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure.
6. To ensure that the same party acts as Applicant throughout the process, the Applicant shall identify himself/herself in each new electronic transaction by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's physical address of record. The Applicant shall identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter. Temporary secrets shall not be reused.	Registration, identity proofing, and token and credential issuance represent different goals of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. (Two electronic transactions are considered to be separate if they are not part of the same protected session.) In these cases, the following methods shall be used to ensure that the same party acts as Applicant throughout the process.
7. Resist repudiation of registration threat.	A Subscriber denies registration, claiming that they did not register that token.
8. Applicant undergoes identity proofing by a trusted Registration Authority (RA).	Requires presentation and verification of identifying materials or information.

[7] When PKI certificate-based authentication is to an Identity Provider (rather than directly to the RP), assertion processing is also required and must additionally follow assertion table trust criteria.

Assurance Level 3 R&I Trust Criteria	Comment
9. Either the RA or the Identity Provider shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including the evidence required in the sections below.	A record of the facts of registration and proofing.
10. The Identity Provider shall be prepared to provide records of identity proofing to Relying Parties as necessary	The record of the facts of registration and proofing.
11. The identity proofing and registration process shall be performed according to a written policy or *practice statement* that specifies the particular steps taken to verify identities.	The practice statement should address primary objectives of registration and identity proofing.
12. If the RA and Identity Provider are remotely located, and communicate over a network, the entire registration transaction between the RA and Identity Provider shall be cryptographically authenticated using an authentication protocol that meets Level 3 requirements, and any secrets transmitted shall be encrypted using an Approved encryption method.	See Appendix C for definition of "Approved".
13. The Identity Provider shall be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. The Identity Provider shall be capable of conveying this information to Verifiers and Relying Parties.	Ensure a person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person.
14. The name associated with the Subscriber shall be meaningful.	Verified real names, not pseudonyms.
15. The results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality and integrity.	Sufficiently protect all identity proofing information and ensure it comes from known, trusted sources.
16. Applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other individual identifying information.	
17. For In-Person Proofing – Possession of verified current primary Government Picture ID that contains Applicant's picture and either address of record or nationality (e.g. driver's license or passport). Inspects Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compares picture to Applicant, record ID number, address and DoB. If ID is valid and photo matches Applicant then: a. If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b. If ID does not confirm address of record, issues credentials in a manner that confirms address of record.	

Assurance Level 3 R&I Trust Criteria	Comment
18. For Remote Proofing – Possession of a valid Government ID (e.g. a driver's license or Passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers. Verify information provided by Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a. Issues credentials in a manner that confirms the address of record supplied by the Applicant; or b. Issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records, while recording the Applicant's voice or using equivalent alternative means to establish non-repudiation.	
19. If the exact number of tokens to be issued is not agreed upon early in the registration process, then the tokens should be distinguishable so that Verifiers will be able to detect whether any suspicious activity occurs during the first few uses of a newly issued token.	A common reason for breaking up the registration process as described above is to allow the subscriber to register or download software tokens in two or more different computing environments. This is permissible as long as the tokens individually meet the appropriate assurance level.
20. Federally regulated financial institutions, brokerages and dealers may issue credentials to their customers via the mechanisms normally used for on-line banking or brokerage credentials, and may use on-line banking or brokerage credentials and tokens as Level 3 E-Authentication credentials and tokens, provided: a. The customers have been customers in good standing for a period of at least 1 year prior to the issuance of E-auth credentials, and b. The customers have appeared in-person before a representative of the financial institution, and the representative has inspected a Government issued primary Photo-ID and compared the picture to the customer. c. The credentials and tokens meet all additional provisions of Level 3 as appropriate.	Federal law, including the Bank Secrecy Act and the USA Patriot Act, impose a duty on financial institutions to "know their customers" and report suspicious transactions to help prevent money laundering and terrorist financing. Many financial institutions are regulated by Federal Agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC). These regulators normally require the intuitions to implement a Customer Identification Program. These provisions apply to Federally regulated financial institutions, brokerages and dealers subject to such Federal regulation, that implement such a Customer Identification Program.

Assurance Level 3 R&I Trust Criteria	Comment
21. PKI credentials shall be issued by a CA cross-certified with the FBCA under FBCA CP, Common CP, or C4 CP, or a policy mapped to one of those policies.	For PKI credentials, Federal ICAM relies on the proven criteria and methodology of the FPKIPA.

Tokens

Assurance Level 3 Tokens Trust Criteria	Comment
1. Resist token theft threat.	Protect a token with a physical manifestation (e.g., one time password device, hardware cryptographic device) from being stolen by an Attacker.
2. Resist token duplication threat.	Protect against a Subscriber's token being copied with or without his or her knowledge (e.g., use tokens that are hard to copy).
3. Resist social engineering threat.	Protect against an Attacker establishing a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret.
4. When a multi-factor token or a multi-token authentication scheme is being used, the security properties of each factor or of each token are considered additive in nature. If one factor of a multi-factor scheme or one token of a multi-token scheme has the desired properties for a given assurance level, it is considered sufficient.	Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained.
5. For single token schemes that use one token to gain access to a second token, the compound solution is only as strong as the token with the lowest assurance level.	The solution is only as strong as its weakest link.

Token and Credential Management

Assurance Level 3 T&C Management Trust Criteria	Comment
1. Files of long-term shared secrets used by Identity Providers or Verifiers at Level 3 shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall be encrypted so that: a. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation. b. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module.	See Appendix B for reference to FIPS 140-2 document.

Assurance Level 3 T&C Management Trust Criteria	Comment
2. Identity Providers shall provide a secure mechanism to allow Verifiers or Relying Parties to ensure that the credentials are valid. Such mechanisms may include on-line validation servers or the involvement of Identity Provider servers that have access to status records in authentication transactions. Temporary session authentication keys may be generated from long-term shared secret keys by Identity Providers and distributed to third party Verifiers, as a part of the verification services offered by the Identity Provider, but long-term shared secrets shall not be shared with any third parties, including third party Verifiers. Approved cryptographic algorithms are used for all operations.	See Appendix C for definition of "Approved".
3. Renewal and re-issuance shall only occur prior to expiration of the current credential. Claimants shall authenticate to the Identity Provider using the existing token and credential in order to renew or re-issue the credential. All interactions shall occur over a protected channel such as SSL/TLS.	
4. Identity Providers shall have a procedure to revoke credentials and tokens within 24 hours. Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid. Shared secret based authentication systems may simply remove revoked Subscribers from the verification database. Secondary credentials must have a lifetime less than 2 hours.	
5. A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the Identity Provider or its representative. The record retention period of data for Level 3 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. Identity Providers operated by or on behalf of executive branch agencies shall also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.	

Assurance Level 3 T&C Management Trust Criteria	Comment
6. Tokens can be renewed using out of band delivery mechanisms. If the Subscriber uses an out of band token delivery approach, re-registration of the delivery mechanism can be equated to token renewal or re-issuance. In such a case, the subscriber must use an alternate, yet already registered delivery mechanism to deliver the token and then gain access to the Identity Provider such that the registration data can be updated by the Subscriber or, if no alternate out of band channel was registered with the original out of band channel the subscriber must re-establish their identity with the Identity Provider in order to update their registration data.	
7. The Identity Provider should establish policies for token collection to avoid the possibility of unauthorized use of the token after it is considered out of use.	The Identity Provider may destroy such collected tokens, or zeroize them to ensure that there are no remnants of information that can be used by an Attacker to derive the token value.
8. Token and credential verification services categorized as FIPS 199 "Moderate" or "High" for availability shall be protected in accordance with the Contingency Planning (CP) controls specified in NIST SP 800-53 to provide an adequate level of availability needed for the service.	See Appendix B for reference to FIPS 199 and NIST SP 800-53 documents.

Authentication Process

Assurance Level 3 Authentication Process Trust Criteria	Comment
1. Resist online guessing threat.	Protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. Resist replay threat.	Protect against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.
3. Authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Authentication requires that the Claimant prove through a secure authentication protocol that he or she controls the token.	Ensure that the Claimant (person being authenticated) actually possesses the token.
4. Plaintext passwords or secrets shall not be transmitted across a network.	A network is an open communications medium, typically the Internet, used to transport messages between the Claimant and other parties.
5. Resist session hijacking threat.	Protect against an Attacker being able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the Subscriber.

Assurance Level 3 Authentication Process Trust Criteria	Comment
6. Resist eavesdropping threat.	Protect against an attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant. See Appendix C for definition of "Approved".
7. Weakly resist man-in-the-middle threat.	Protect against an attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. A protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.
8. The authentication process shall provide sufficient information to the Verifier to uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time of registration, and (ii) verified by the RA in the issuance of the token and credential.	Ensure the authentication process can uniquely identify each Subscriber and the associated tokens and credentials issued to that Subscriber.
9. Approved cryptographic techniques shall be used for all operations including the transfer of session data.	Protect data exchanged between the end user and the Relying Party. See Appendix C for definition of "Approved".
10. Resist phishing/pharming threat.	Protect against a phishing attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier, and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier; and against a pharming attach where an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/Relying Party, and revealing sensitive information, downloading harmful software or contributing to a fraudulent act.

Assertions

Assurance Level 3 Assertions Trust Criteria	Comment
1. Use an ICAM adopted authentication scheme.	Use of any ICAM adopted authentication scheme defined for this assurance level is acceptable.

A-4 Assurance Level 4

LOA 4 PKI is out of scope for this document, and is addressed in *Criteria and Methodology For Cross Certification With the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA)* [11].

APPENDIX B – REFERENCE DOCUMENTATION

[1] HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[2] OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] OMB M-06-22: Cost Savings Achieved Through E-Government and Line of Business Initiatives
http://www.whitehouse.gov/omb/memoranda/fy2006/m06-22.pdf

[4] NIST Special Publication 800-63: Electronic Authentication Guideline
http://csrc.nist.gov/publications/PubsSPs.html

[5] NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/PubsSPs.html

[6] Federal Information Processing Standard 140-2: Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/PubsFIPS.html

[7] Federal Information Processing Standard 199: Standards for Security Categorization of Federal Information and Information Systems
http://csrc.nist.gov/publications/PubsFIPS.html

[8] X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[9] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

[10] Citizen and Commerce Class Common Certificate Policy
http://www.cio.gov/fpkipa/documents/citizen_commerce_cp.pdf

[11] Criteria and Methodology For Cross Certification With the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA)
http://www.cio.gov/fpkia/documents/crosscert_method_criteria.pdf

APPENDIX C - DEFINITIONS

Term	Definition
Adopted Authentication Scheme (Adopted Scheme)	An open identity management standard that the ICAM assesses, approves, and scopes for government-wide use. An adopted scheme meets all applicable ICAM requirements, as well as other Federal statutes, regulations, and policies. In addition, the structured adoption process provides assurance to all ICAM participants that underlying identity assurance technologies are appropriate, robust, reliable, and secure.
Adoption	Acceptance of a 3rd party Trust Framework by the Federal government after rigorous review and determination of comparability at a specified Level of Assurance.
Approved Encryption Method	FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation
Assertion	A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes.
Assertion Reference	Identifies the Verifier and includes a pointer to the full assertion held by the Verifier.
Audit Criteria	TFP auditor qualifications, TFP identity provider audit processes, and ongoing TFP identity provider re-certification processes.
Authentication	The process of establishing confidence in the identity of users or information systems.
Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.
Bearer Assertion	An assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion. The Relying Party has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the Relying Party.
Biometric	Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.
Bona Fides	Evidence that provides insight into an organization's maturity, legitimacy, stability, and reputation.
Certification (Certify)	TFP certification of an identity provider is the determination that the identity provider's policies and practices are comparable to ICAM trust requirements.
Claimant	A party whose identity is to be verified using an authentication protocol.
Comparability	Equivalence of Trust Framework Provider criteria to ICAM trust criteria as determined by ICAM designated Assessment Teams.
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
Cross-certified	A certificate used to establish a trust relationship between two Certification Authorities.

Term	Definition
Cryptographic	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.
Direct Assertion Model	The Claimant uses his or her E-authentication token to authenticate to the Verifier. Following successful authentication of the Claimant, the Verifier creates an assertion, and sends it to the Subscriber to be forwarded to the Relying Party. The assertion is used by the Claimant/Subscriber to authenticate to the Relying Party.
E-Authentication Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Entropy	A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. See NIST SP 800-63 for additional information.
Full Legal Name	A person's name that is usually the name given at birth and recorded on the birth certificate but that may be a different name that is used by a person consistently and independently or that has been declared the person's name by a court. That is, the name one has for official purposes; not a nickname or pseudonym.
Holder-of-key Assertion	A holder-of-key assertion contains a reference to a symmetric key or a public key (corresponding to a private key) possessed by the Subscriber. The Relying Party may require the Subscriber to prove possession of the secret that is referenced in the assertion. In proving possession of the Subscriber's secret, the Subscriber also proves that he or she is the rightful owner of the assertion. It is therefore difficult for an Attacker to use a holder-of-key assertion issued to another Subscriber, since the former cannot prove possession of the secret referenced within the assertion
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.
Identity Provider	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The Identity Provider may encompass Registration Authorities and verifiers that it operates. An Identity Provider may be an independent third party, or may issue credentials for its own use.
Indirect Assertion Model	In the indirect model, the Claimant uses his or her token to authenticate to the Verifier. Following successful authentication, the Verifier creates an assertion as well as an assertion reference (which identifies the Verifier and includes a pointer to the full assertion held by the Verifier). The assertion reference is sent to the Subscriber to be forwarded to the Relying Party. In this model, the assertion reference is used by the Claimant/Subscriber to authenticate to the Relying Party. The Relying Party then uses the assertion reference to explicitly request the assertion from the Verifier.
Integrity	The property that data has not been altered by an unauthorized entity.
Issuance	Delivery of token or credential to the subscriber of an Identity Provider.
Level of Assurance (LOA)	In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Term	Definition
Min-Entropy	A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). See NIST SP 800-63 for additional information.
Multi-factor Authentication	Use of two or more of he following: 1. *Something you know* (for example, a password) 2. *Something you have* (for example, an ID badge or a cryptographic key) 3. *Something you are* (for example, a thumb print or other biometric data) Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors.
Multi-token Authentication	Two or more tokens are required to verify the identity of the Claimant.
Network	An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties.
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Out of Band	Communications which occur outside of a previously established communication method or channel.
Personal Identifying Information	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Possession and Control of a Token	The ability to activate and use the token in an authentication protocol.
Proof of Possession Protocol	A protocol where a Claimant proves to a Verifier that he/she possesses and controls a token (e.g., a key or password)
Pseudonym	A Subscriber name that has been chosen by the Subscriber that is not verified as meaningful by identity proofing.
Registration	The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.

Term	Definition
Registration Authority	A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying Party (RP)	An entity that relies upon the Subscriber's credentials or Verifier's assertion of an identity, typically to process a transaction or grant access to information or a system.
Salt	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.
Strong Man in the Middle Resistance	A protocol is said to be strongly resistant to man-in-the-middle attack if it does not allow the Claimant to reveal, to an attacker masquerading as the Verifier, information (token secrets, authenticators) that can be used by the latter to masquerade as the true Claimant to the real Verifier.
Strongly Bound Credentials	The association between the identity and the token within strongly bound credentials cannot be easily undone. For example, a digital signature binds the identity to the public key in a public key certificate; tampering of this signature can be easily detected through signature validation.
Subscriber	A party who has received a credential or token from a CSP.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant’s identity.
Token Authenticator	The value that is provided to the protocol stack to prove that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependant upon the token authenticator, but they may or may not explicitly contain it.
Trust Criteria	Set of benchmarks used to measure an identity provider’s technical and operational controls with respect to registration and issuance, tokens, token and credential management, the authentication process, and assertions.
Trust Framework	Trust Framework Provider processes and controls for determining an identity provider’s compliance to OMB M-04-04 Levels of Assurance.
Trust Framework Provider (TFP)	A TFP is an organization that defines or adopts an on-line identity trust model and then, certifies identity providers that are in compliance with that model.
Verifier	An entity that verifies the Claimant’s identity by verifying the Claimant’s possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.

Term	Definition
Weak Man in the Middle Resistance	A protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.
Weakly Bound Credentials	The association between the identity and the token within a weakly bound credential can be readily undone and a new association can be readily created. For example, a password file is a weakly bound credential since anyone who has "write" access to the password file can potentially update the associations contained within the file.

APPENDIX D - ACRONYMS

Acronym	Definition
CA	Certification Authority
CIO	Chief Information Officers
CISA	Certified Information System Auditor
CP	Certificate Policy
CSP	Credential Service Provider
DoB	Date of Birth
FBCA	Federal Bridge Certification Authority
FCIOC	Federal Chief Information Officers Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal Public Key Infrastructure Policy Authority
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ICAMSC	Identity, Credential, and Access Management Sub Committee
ID	Identifier
ISIMC	Information Security and Identity Management Committee
IT	Information Technology
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
SC	System and Communications Protection
SP	Special Publication
TFP	Trust Framework Provider
TFPAP	Trust Framework Adoption Process