ICAM
Identity, Credential,
& Access Management

Federal Identity, Credential, and Access Management
Trust Framework Solutions

Trust Framework Provider Adoption Process (TFPAP)

For

All Levels of Assurance

Version 2.0
02/07/2014

Questions?
Contact the FICAM TFS Program Manager at TFS.EAO@gsa.gov

Document History

Status	Release	Date	Comment	Audience
DRAFT	1.1.0	3/18/13	Updated to reflect the recognition of the Federal PKI Policy Authority (FPKIPA) as a TFS-approved Trust Framework Provider for non-Federally issued PKI based credentials.	TFET
FINAL	1.1.0	3/28/13	Approved for public release	Public
DRAFT	2.0	11/11/13	Draft version released for public comment	Public
DRAFT	2.0	1/24/14	Updated to reflect external stakeholder feedback.	TFS Program Manager
FINAL	2.0	02/07/14	Approved for public release	Public

This document supersedes all prior versions of the FICAM Trust Framework Provider Adoption Process (TFPAP)

Table of Contents

List of Figures

1. PURPOSE

This document is the *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance* and defines a process whereby the U.S. Federal Government can assess the efficacy of external Trust Frameworks for Federal purposes so that an agency's 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 Office of Management and Budget (OMB) Levels of Assurance.

Trust Frameworks that are comparable to U.S. federal standards are *adopted* through this process, allowing U.S. Federal Government Relying Parties (RPs) to trust credentials that have been assessed under the adopted trust framework.

1.1 Audience

This guideline is intended for:

- **Trust Framework Providers (TFPs)**, who are seeking to map their security and privacy guidelines to U.S. Federal Government security and privacy requirements
- **Security and Privacy Practitioners**, who recommend, design, build or provide solutions that meet U.S. Federal Government requirements
- **Token Managers (TMs), Identity Managers (IMs) and Credential Service Providers (CSPs)**, who are seeking to offer their services for use by the U.S. Federal Government.

1.2 Usage

1. Read the *Trust Framework Solutions Overview* to understand the background, authorities and components of the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS) Program.
2. Read the *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance* to understand the role of the TFP.
3. Read the *Identity Scheme and Protocol Profile Adoption Process* to understand how protocol profiles are created, adopted and used by the government to ensure that the RP application and the CSP communicate in a confident, secure, interoperable and reliable manner.
4. Read the *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* to understand the requirements for offering services to the U.S. Federal Government.

2. BACKGROUND

The FICAM TFS is the federated identity framework for the U.S. Federal Government. It includes guidance, processes and supporting infrastructure to enable secure and streamlined citizen and business facing online service delivery.

The *Trust Framework Solutions Overview* document provides a holistic overview of the components of the TFS which consists of:

- *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance*
- *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services*
- *Identity Scheme and Protocol Profile Adoption Process*
- *Relying Party Guidance for Accepting Externally Issued Credentials*
- E-Government Trust Services Certificate Authority (EGTS CA)
- E-Government Trust Services Metadata Services (EGTS Metadata Services)

This document provides the process by which the security and privacy practices of external (to the U.S. Federal Government) identity service providers can be mapped to those of the U.S. Federal Government for the purposes of conducting citizen-to-government, business-to-government and non-federal and foreign government-to-Federal Government digital interactions.

It covers remote electronic authentication of human users to Information Technology (IT) systems over a network. It does not address the authentication of a person who is physically present.

The TFS TFPAP is inclusive of externally issued Public Key Infrastructure (PKI) and non-PKI credentials at All OMB Levels of Assurance.

2.1 Federation and Trust Frameworks

There is a business need to provide online services seamlessly across organizational and jurisdictional boundaries that include a combination of public and private service providers. Fulfilling this need requires a level of trust between many organizations having diverse mandates and acting under different authorities. Within this context, there is a need to have well-defined arrangements that ensure the confidence in each other's services, including their underlying business and technical processes. Arrangements that ensure confidence can be referred to as trust relationships. The overall approach of governing these trust relationships can be referred to as federation.

A federation is comprised of a multi-party arrangement in which there is agreement on the adherence to standards and practices that ensure confidence, enable interoperability, realize efficiencies and reduce risk. Many federations today are informal in nature and are based upon shared practices and shared objectives that have been developed over time. However, as federations become more formalized, frameworks that provide common understandings, contractual agreements, service agreements, legal obligations, and dispute resolution mechanisms replace the informal agreements.

These formal arrangements, which exist in the industry, are becoming known as *Trust Frameworks*. Leveraging them enables a scalable model for extending identity assurance across a broad range of citizen and business needs.

Trust Frameworks[1] are the governance structure for a specific identity system consisting of:

- *The Technical and Operational Specifications that have been developed to:*
    - Define requirements for the proper operation of the identity system (i.e., so that it works),
    - Define the roles and operational responsibilities of participants, and
    - Provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that it is trustworthy); and
- *The Legal Rules that govern the identity system in order to*
    - Regulate the content of the Technical and Operational Specifications,
    - Make the Technical and Operational Specifications legally binding on and enforceable against the participants, and
    - Define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

[1] As defined by the American Bar Association's Federated Identity Management Legal Task Force.

2.2 Trust Framework Adoption

Critical to the success of the FICAM TFS is the assessment and adoption of TFPs that best serve the interests of the Federal Government. A TFP is an organization that defines a Trust Framework and then certifies[2] CSPs compliant with that Trust Framework. Adoption means that any identity service certified by that TFP is qualified to provide identity assertions to federal agencies. The FICAM TFS 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 TFPAP, based on guidance from OMB and National Institute of Standards and Technology (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 Federal Government RPs of the validity, and thus dependability, of identity credentials, tokens and other services. This confidence is essential to government-wide acceptance and use of non-local identity services.

The adoption of a Trust Framework by the FICAM TFS Program is limited to the *Technical and Operating Specification* component of that Trust Framework, and does not encompass its *Legal Rules* component. In all cases, it is expected that the *Legal Rules* component will be addressed directly by an agency's acquisition and contracting processes, or by the acquisition and contracting processes of Shared Service Provider(s) acting on behalf of an agency.

3. IMPLEMENTATION

3.1 Security, Privacy and Interoperability Practices

The TFPAP model is based on comparing the policies and practices of non-Federal Government TFPs to the risks and assurance outcomes of OMB Policy Memorandum M-04-04, NIST Special Publication (SP) 800-63 [4], the Fair Information Practice Principles (FIPPs) and other relevant Government guidance.

There are seven (7) trust criteria categories:

1. **Registration and Issuance** – How well does the CSP register and proof the identity of the credential applicant, and issue the credential to the approved applicant?
2. **Tokens** – What is the CSP'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 CSP manage and protect tokens and credentials over their full life cycle?
4. **Authentication Process –** How well does the CSP secure its authentication protocol?
5. **Assertions –** How well does the CSP secure Assertions, if used, and how much information is provided in the Assertion?
6. **Ongoing Verification –** What compensating controls does the CSP implement that provides an ongoing identity verification capability? [OPTIONAL]
7. **Privacy –** How well does the privacy policies of the CSP adhere to the Fair Information Practice Principles?

[2] TFP certification of a CSP is the determination that the CSP's policies and practices are comparable to FICAM trust requirements.

3.2 Guidance on Privacy Trust Criteria

This section should be used by Assessors and Auditors when determining whether an Applicant CSP shall be approved by the TFP, and during re-assessment audits required by TFPs for renewal of a CSP's certification. If Assessors and Auditors find any material deficiencies in the implementation of the TFPAP Privacy Criteria, they should specify them in their written report to the TFP, and should also state what remediation has been implemented to address the deficiency. Assessors and Auditors should revisit the CSP within 6 months to evaluate whether the material deficiency has been fully addressed, and should provide the TFP with a written report describing the manner in which the deficiency has been addressed.

To optimize the assessment process, it is recommended that Assessors and Auditors have accreditation with the International Association of Privacy Practitioners (IAPP) (e.g., CIPP, CIPP/G, CIPP/IT, CIPM), and strongly recommended that Assessors and Auditors have a working knowledge of privacy concepts including the Fair Information Practice Principles (FIPPs) upon which the TFPAP Privacy Criteria are based.

3.2.1 Adequate Notice

Adequate Notice – CSP 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 Personally Identifiable Information (PII) to any party. Adequate Notice should be incorporated into the Opt In process.

1. Is the notice written in plain language so that it is easily understood by the average user?
2. Does the notice convey what information is being transmitted, the user's options, and the outcome of not transmitting the information?
3. Is the user information being transmitted the same information that is described in the notice? Is that the only information being transmitted?
4. Is the notice incorporated into the "opt in" mechanism?
5. If so, is the notice clear, concise, unavoidable, and in real-time?
6. Is the notice merely a linked general privacy policy or terms of service?

Supplemental Explanation: Adequate notice is a practical message that is designed to help the average user understand how to engage in the authentication transaction, including, what information is being transmitted about the user, what options the user has with respect to the transmission of the information, and the consequences of refusing any transmission. For example, if the information to be transmitted is required by the RP for the authentication, the notice should make clear that the transmission is required and refusal will cancel the transaction and return the user to the RP's website for further assistance. If the information to be transmitted is not required for authentication, but, for example, will be collected by the RP in order to provide the service requested by the user more conveniently, the notice should make this distinction clear and indicate that if the user refuses the transmission, the user will be able to provide the information directly on the RP's website. Assessors and Auditors should look for a notice that is generated at the time of the authentication transaction. The notice should be in visual proximity (i.e. unavoidable) to the action being requested, and the page should be designed in such a way that any other elements on the page do not distract the user from the notice. The content of the notice should be tailored to the specific transaction. The notice may
be divided into multiple or "layered" notices if such division makes the content more understandable or enables users to make more meaningful decisions. For these reasons, the notice should be incorporated

into the “opt in” mechanism as set forth below. In sum, an Adequate Notice is never just a link somewhere on a page that leads to a complex, legalistic privacy policy or general terms and conditions.

3.2.2 Opt In

Opt In – CSP 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. . If a CSP is aware that certain requested attributes are not required for authentication, the Credential Service Provider should allow End Users to opt out of the non-required individual attributes for each transaction..

Suggested Assessment Questions:

1. Is each attribute, or piece of user information to be transmitted, displayed to the user before each transmission?
2. Is there a mechanism for obtaining explicit user confirmation of the information transmission?
3. Is the mechanism specific to the authentication transaction?
4. Is the mechanism intuitive and easy to use?
5. Does the user have the ability to expressly permit or deny the transmission of specific pieces of user information, to the extent not required by the authentication transaction?

Supplemental Explanation: The goal is for the user is to understand the opt-in process, and to have a meaningful opportunity to agree. There are various ways to implement this goal. Users need to be able to see each piece of information, or attribute that is to be transmitted prior to it being transmitted. The confirmation mechanism must enable the user to make an explicit affirmation to permit the transmission of user information in accordance with the notice as described above. Confirmation mechanisms should be designed so that they are intuitive and easy to use. They need to be specific to the transaction. To the extent the information to be transmitted is not required for authentication (i.e., the RP would like to have the information to pre-populate transaction fields or for other reasons, but the information is not necessary to accomplish the authentication of the user), users should have the ability to expressly permit or deny the transmission of specific pieces of such user information, for example, through radio buttons or similar mechanisms. As described above, the design of the notice and the confirmation mechanism should be considered as an integrated concept. Mechanisms that allow users to affirmatively waive notices and opt-in consents for each transmission such as a “don’t show me this message again” option are acceptable. Mechanisms such as a simple “agree” button on ‘general terms of service’ or pre-checked consents are strongly discouraged because they are unlikely to meet the essential objective of meaningful understanding.

Generally, it is less meaningful to obtain opt-in at the time the credential is issued rather than at the time of the transaction. In certain circumstances, the Trust Framework Evaluation Team (TFET) may approve TFPs that accept this practice. Assessors should be made aware of agreements made between the TFP and TFET that affirmatively accept this practice and any constraints established for this practice.

3.2.3 Minimalism

Minimalism – CSP must transmit only those attributes that were explicitly requested by the RP application or required by the federal profile.

Suggested Assessment Questions:

1. Is there written documentation describing the user information requested by the RP?
2. Does the written documentation distinguish between information that the RP needs to conduct the authentication transaction and any other information that the RP would like to collect (e.g. to increase efficiency or convenience in providing the service requested by the user)?
3. Does the CSP actually only transmit those attributes that were explicitly requested by the RP or required by the federal profile?
4. In the absence of any written documentation, does the CSP only send attributes required by the federal profile?

Supplemental Explanation: Assessors and Auditors need to ensure that CSP are only sending the information that is explicitly requested by the RP or that is required by the federal profile. Written documentation is important in ensuring that the Adequate Notice and Opt-in principles are appropriately executed in terms of distinguishing between information that the RP needs to conduct the authentication transaction and information that the RP would like to collect. In the absence of any such written documentation from the RP, only the information required by the federal profile may be sent.

3.2.4 Activity Tracking

> **Activity Tracking** – Commercial CSP must not disclose information on End User activities with the government to any party, nor use the information for any purpose other than federated authentication or to comply with law or legal process.

Suggested Assessment Questions:

1. Is there a written policy on how the CSP will comply with this principle?
2. Does the CSP have any technical means for ensuring compliance with its written policy?
3. What other means does the CSP employ to ensure compliance? Employee training?
4. Does the CSP have procedures to measure the effectiveness of its methods?
5. Does the CSP make its compliance with this principle clear to users?

Supplemental Explanation: The purpose of this principle is to ensure that the CSP does not use or disclose any information about the user and his or her interactions with the government, which the CSP learns as a result of providing the authentication service for any purpose other than to provide the authentication service or to comply with law or legal process. Assessors and Auditors should check for a written policy that demonstrates how the CSP will comply with this principle. Assessors and Auditors should also evaluate the effectiveness of the means, technical or otherwise, which the CSP uses to achieve compliance. Finally, Assessors and Auditors should check whether the CSP provides an explanation of this principle to users. This explanation may be located in a general privacy policy about the collection and use of personal information.

3.2.5 Termination

> **Termination** – In the event a CSP ceases to provide this service, or the user ceases to use the CSP, the Provider shall continue to protect or destroy any sensitive data including PII.

Suggested Assessment Questions:

1. Is there a written policy or plan demonstrating how the CSP will manage sensitive data in the event of a bankruptcy, sale, or voluntary discontinuation of the provision of identity services?
2. What commitments does the policy or plan contain with respect to the destruction or transfer of the data?
3. Does the policy or plan provide for notice to the users in the event of transfer of their sensitive data?
4. Is there a clear process for the user to expressly indicate that they are ceasing to use the CSP or a policy to manage inactive accounts?
5. In the event that a user ceases to use the CSP, does the policy or plan contain commitments with respect to the protection or destruction of the user's sensitive data including PII?

Supplemental Explanation: Assessors and Auditors should evaluate whether the written policy or plan expressly provides for destruction of the data, as appropriate, or a commitment that the CSP, to the best of its abilities, will require that any recipient of the data protect the data in kind. Ideally, CSPs shall give users notice when their sensitive data will be transferred to another entity.

3.3 PKI Authentication and Federation

PKI Credentials in a federation can be used in three use cases:

1. Presented directly to the RP and validated by the RP (Not a federation use case per se, but provided for the sake of completeness)
2. Presented to a CSP, which validates the credential and generates a bearer assertion to the RP
3. Presented to a CSP, which validates the credential and generates a holder-of-key assertion to the RP

In the first case, the TFPAP recognizes the Federal PKI Policy Authority (FPKIPA) as a TFPAP-adopted TFP[3] and will rely on its proven criteria and methodology for non-Federally issued PKI credentials[4] (i.e., if a Certificate Authority [CA] has been cross-certified with the Federal PKI Bridge, it is considered FICAM TFS Approved). It is important to note that in this case, sufficient data may not be present in the PKI credential to allow the subject to be enrolled into an RP application and that alternate means of conveying verified attributes from the CSP to the RP (e.g., Backend Attribute Exchange compliant attribute queries) may need to be implemented.

In the second case, the PKI credential is simply a token like any other, and the TFP in its evaluation of the CSP must demonstrate trust comparable to each of the six categories (registration and issuance, tokens, token and credential management, authentication process, assertions, and privacy) for each Level of Assurance it wishes its credentials trusted by government applications (including physical access control systems).

[3] The FICAM TFS recognizes the FPKIPA Memorandum of Understanding (MOU) as an ATOS equivalent and serves as the precedent for the ATOS approach.

[4] The TFS TFPAP currently only recognizes CAs that are approved under FPKIPA processes for direct authentication.

Lastly the case of a PKI credential that is presented to a CSP resulting in the generation of an authentication assertion is supported with the following caveat:

- In order for the RP to consider the assertion to be a Level 4 assertion of identity, the interaction between the CSP and the RP must comply with the holder-of-key provisions as documented in the *FICAM SAML 2.0 Web Browser SSO Profile*.
- Only FPKIPA-approved PKI credentials recognized at LOA 4 are supported for holder-of-key usage at Level 4.

3.4 Component Identity Services

The traditional e-authentication model of a CSP bundles the functions of a TM which specializes in authentication, IM which specializes in identity proofing and attribute management, and a secure binding function that combines the two to produce a credential.

Over the last number of years, an industry trend has emerged whereby these functions have been separated into components that can be offered by separate service providers. This trend has been driven by the fact that:

- Vendors have focused their offerings according to their core strengths, which leads to improved quality of service for agency RPs.
- Some identity solution architectures require or desire the use of separated services, which offers agency RPs a greater quantity of service choice and increased flexibility in selecting only those services that are needed from an external provider.

The update to SP 800-63 in December 2011 included an explicit statement regarding separation of token authentication and IMs, as follows: “Current government systems do not separate the functions of authentication and attribute providers. In some applications, these functions are provided by different parties. While a combined authentication and attribute provider model is used in this document, it does not preclude agencies from separating these functions.”

The TFPAP recognizes that credentialing functions may be conducted by separate and independent entities that have relationships based on contracts as well as laws and regulations, especially in the private sector. As such, it supports a flexible conceptual model that brings together TMs, IMs and CSPs.

This conceptual model is supported by the following terminology from NIST SP 800-63:

- **Token**: Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity. Tokens are possessed by a Claimant and controlled through one or more of the traditional authentication factors (something you know, have, or are).
- **Identity**: A set of attributes that uniquely describe a person within a given context.
- **Credential**: An object or data structure that authoritatively binds an identity to a token possessed and controlled by a Subscriber.
- **CSP**: A trusted identity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. A CSP may be an independent third party, or may issue credentials for its own use.
- **Registration Authority (RA)**: A trusted entity that establishes and vouches for the identity or attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP

In NIST SP 800-63, the RA is responsible for identity proofing and the CSP maintains the link between the identity proofing and the token management. SP 800-63 explains the relationship between the RA and the CSP as such: "There is always a relationship between the RA and CSP. In the simplest and perhaps the most common case, the RA and CSP are separate functions of the same entity. However, an RA might be part of a company or organization that registers Subscribers with an independent CSP, or several different CSPs."

The explanation of RA and CSP in SP 800-63 stated above clearly establishes that they can be separate entities and results in the de-coupled component service model provided in Figure 1 below:

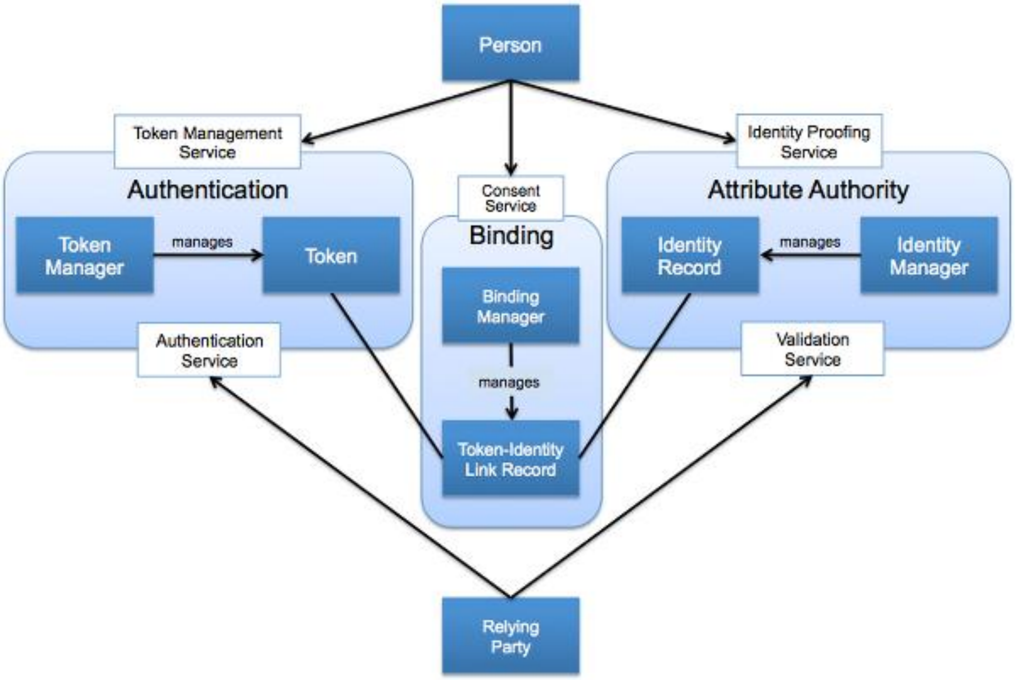

Figure 1: Component Services Model[5]

In this fully decoupled model, the authentication, attribute provider and the secure binding functions are separate.

Given that the TFS Program is focused on leveraging commercial solutions, the TFPAP recognizes Trust Frameworks that choose to "un-bundle" the functions into component services as part of their trust criteria evaluation.

With this context, the TFPAP utilizes the following terminology for token and identity assurance levels, while continuing to utilize the existing LOA terminology for credential assurance:

[5] The model is based on assurance and identity concepts that have been discussed in multiple jurisdictions and communities. In particular, the FICAM TFS Program would like to acknowledge the contributions of the Treasury Board Secretariat of Canada (Canada TBS) and the Kantara Identity Assurance Work Group (IAWG).

- **Level of Assurance (LOA)**: Per OMB M-04-04, 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.
- **Token Assurance Level (TAL)**: The degree of confidence that that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., token, identifier) and that the token has not been compromised (e.g., tampered with, corrupted, modified).
- **Identity Assurance Level (IAL)**: The degree of confidence that an individual, organization or device is who or what it claims to be.

In addition, the TFPAP provides the following clarification for assurance levels:

Level	Identity Assurance	Token Assurance	OMB M-04-04 Assurance
4	Very high confidence that an individual is who he or she claims to be.	Very high confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Very high confidence in the asserted identity's validity
3	High confidence that an individual is who he or she claims to be.	High confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	High confidence in the asserted identity's validity
2	Some confidence that an individual is who he or she claims to be.	Some confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Some confidence in the asserted identity's validity
1	Little or no confidence that an individual is who he or she claims to be.	Little or no confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Little or no confidence in the asserted identity's validity

The value of the component service model lies in the flexibility possible in combining the various functions as part of an industry service offering.

Within the framework of the FICAM TFS Program, the following three combinations are recognized:

1. A **CSP**, which offers:

   - Token Management Services
   - Authentication Services
   - Identity Proofing Services
   - Attribute Validation Services

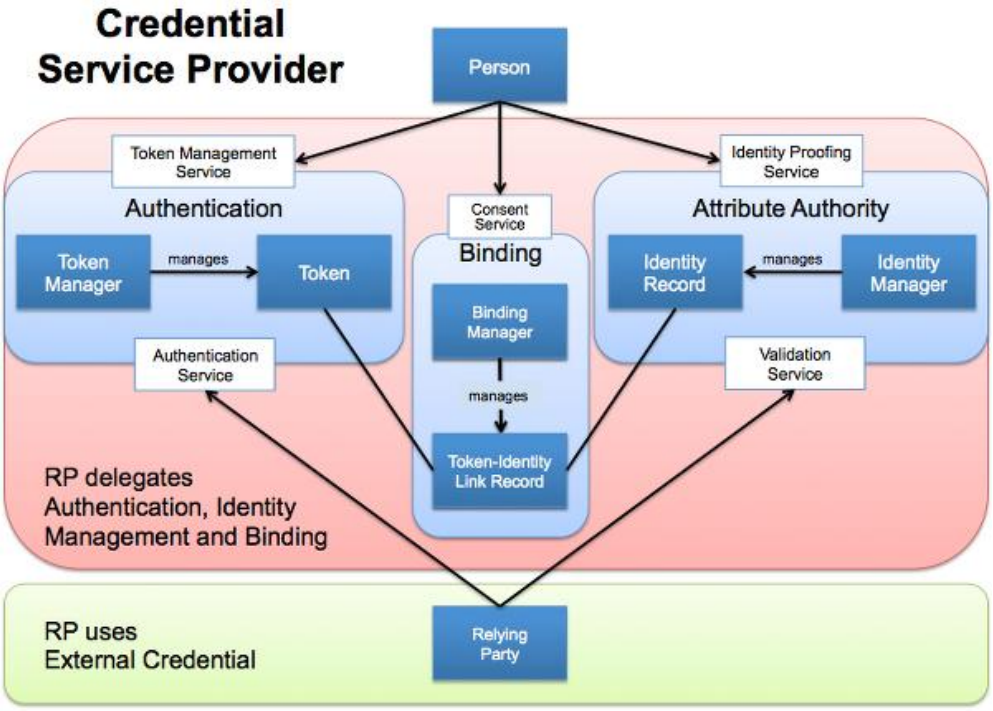

Figure 2: Credential Service Provider Services

2. A **TM**, which offers:

- Token Management Services
- Authentication Services

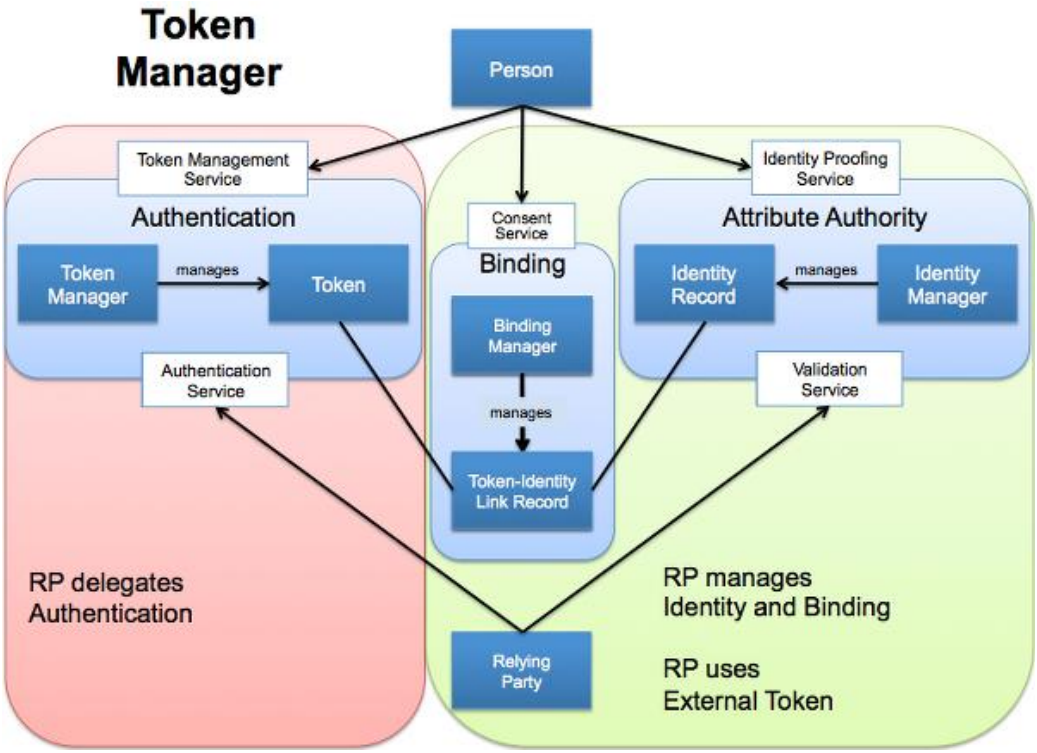

Figure 3: Token Manager Services

3. An **IM**, which offers:

- Identity Proofing Services
- Attribute Validation Services

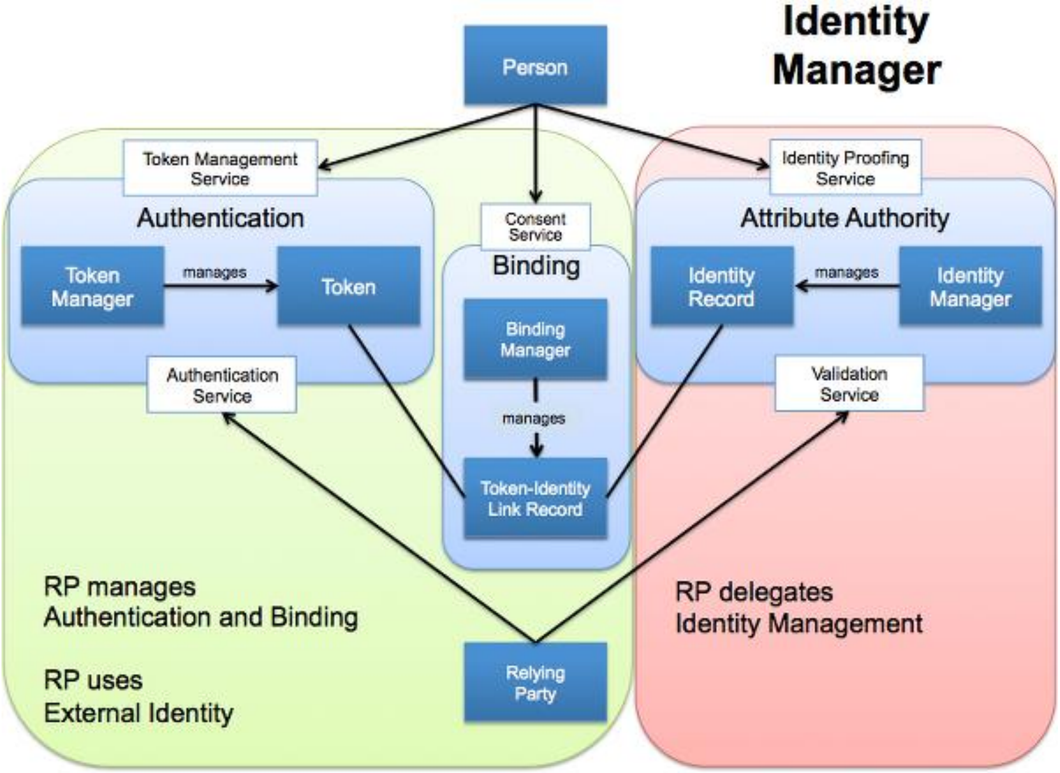

Figure 4: Identity Manager Services

In the current iteration of this guidance, the TFPAP does not provide explicit trust criteria to accommodate un-bundling but may, on a case-by-case basis, leverage the approaches of the TFPs with the following caveats:

- The TFPAP recommends the adoption of the above standard terminology by TFPs;
- The TFP in its evaluation of an entity (TM, IM or a full-service CSP) **MUST explicitly articulate the trust criteria (**Registration and Issuance, Tokens, Token and Credential Management, Authentication Process, Assertions and Privacy) **that ARE addressed and those that ARE NOT addressed for that entity**; and
- The TFPAP currently does NOT support combining the functions across Trust Frameworks (i.e., A TM approved under Trust Framework A and an IM approved under Trust Framework B cannot be combined to create a CSP). This will ensure that a single TFP will be accountable for all trust criteria for its Trust Framework

It is expected that as further practical experience becomes available, the TFPAP will be updated to reflect best practices in this area.

3.5 TFP Governance

The FICAM TFS Program will meet at least quarterly with all adopted TFPs to review ongoing activity and to discuss issues of mutual interest.

Adopted TFPs are subject to the following by the FICAM TFS program:

- Determination as to whether the TFP should be discontinued (i.e., no longer acceptable to the Federal Government). Discontinuance may be for reasons including, but not limited to, no longer applicable to the Federal Government, no longer comparable with applicable U.S. Federal Government requirements, failure to abide by terms of original agreement, etc;.
- Comparability audit (i.e., another comparability mapping), as requested by FICAM TFS;
- 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;
- Requests by FICAM TFS for detailed information regarding assessments of Identity Services that seek to offer their services to the U.S. Federal Government;
- Informing FICAM TFS of significant changes in TFP-approved entity (i.e., CSP) and identity service operations or policies that impact ongoing TFP approval or renewal (e.g., if a CSP changes privacy and security policies as a result of a merger or split, the TFP needs to notify the FICAM TFS and can be reassessed for continued approval); and
- TFS Program updates to the TFPAP must be approved for use by an adopted TFP within 6 months of the final version of the updated TFPAP. The TFP is required to notify the TFS Program at adoption.

3.6 FICAM TFS Program Relationship to TFP Approved Entities

TFPs demonstrate comparability to the TFPAP Requirements for Security and Privacy. Identity Services demonstrate comparability to a TFP's Trust Framework.

Entities qualified by a TFP as having met the TFPAP requirements for security and privacy have the option of applying to the FICAM TFS Program to be approved to offer their services to the U.S. Federal Government.

Information on the FICAM TFS application and approval process can be found in the FICAM TFS *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* Guidance.

3.7 FICAM TFS Assurance Level Needs and Supporting Processes

The FICAM TFS Program is focused on enabling and supporting the security and privacy requirements of Government to Citizen and Government to Business online services. The assurance needs of such services range from Level 1 to Level 4.

3.7.1 Assurance Level 1

As described in OMB-04-04, at Level 1 there exists little to no confidence in an asserted identity. Given the lack of identity assurance at Level 1, **the FICAM TFS Program DOES NOT RECOMMEND the use of Level 1 Identity Services in e-authentication transactions that require assurances of identity.**

The value of a Level 1 identity service, which can only be used for very low risk/value transactions, lies in:

- Decreasing the burden to individuals in having to manage multiple identity credentials
- The ability to explore and validate new protocols and approaches in an environment that has minimal security and privacy risk
- Reducing, to some degree, the infrastructure and operational costs to Government in managing Level 1 credentials or services
- Ensuring that there exists a pool of identity services operating in a manner that protects the information that an applicant/individual has entrusted to it.

As such, the use of a Level 1 credential or service offering by an agency should be based on a case-by-case Agency risk analysis of the credential or service offering that includes an evaluation of its security and privacy characteristics.

As a service to Agencies, the FICAM TFS Program will maintain a listing of identity services on the IDManagement.gov website that have **self-asserted, to an adopted TFP, a minimum set of security and privacy criteria** as documented in Appendix A, Section A-1

3.7.2 Assurance Levels 2-4

The majority of high value citizen facing services require assurances of identity that range from level 2 to level 4**.** The criteria and the processes provided in this document will be used to assess and verify if the commercial services can meet the security, privacy and interoperability requirements at each assurance level.

The IDManagement.gov website will provide the authoritative listing of which TMs, IMs, and CSPs have been approved by the FICAM TFS Program.

4. TFP ADOPTION PROCESS

4.1 Assessment Package Submission

The process begins with an Applicant TFP (Applicant) submitting an Assessment Package to the FICAM TFS Program Manager, who then consults with relevant government agencies and organizations regarding the submission.

The Assessment Package must include:

- The framework's trust specifications with respect to applicable trust criteria listed in Appendix A;
- 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[6] may satisfy trust criteria.

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.

4.2 Value Determination

The FICAM TFS Program Manager, after consultation with relevant government agencies and organizations, determines whether adoption of the Applicant would be valuable to federal agencies. In doing so, the FICAM TFS Program considers 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 FICAM TFS Program (or designated Team) assesses 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 identity services;
- Financial capacity to manage the risks associated with conducting assessments and certifying identity services;
- Understanding of, and compliance with any legal requirements incumbent on the Applicant in connection to conducting assessments and certifying identity services;
- Scope and extent of implemented security controls (e.g., access control, confidentiality of CSP information);
- Documentation of policies and procedures; and
- Proof that Applicant practices are consistent with documented policies and procedures (e.g., via independent auditor reports, if required by LOA requirements).

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.

4.3 Comparability Assessment

The FICAM TFS Program Manager establishes 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 CSPs are comparable to Identity, Credential, and Access Management (ICAM) criteria. Trust criteria assessment includes:
    1. Technical policy and privacy policy comparability based upon Appendix A trust criteria;

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

    2. Determination of whether the Applicant sufficiently reviews member CSP *bona fides* to ensure member CSP 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 CSPs;
        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 CSPs; and
    3. Ongoing Applicant processes used to re-certify Applicant member CSPs.

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.[7]

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 FICAM TFS requirements 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 CSPs; and
4. Sufficiency of the Applicant's auditor qualifications, auditing processes, and recertification processes.

4.4 TFP Adoption Decision

The FICAM TFS Program reviews the Summary Report for the Applicant, and after consultation with relevant government agencies and organizations, decides on whether to adopt the Applicant. Upon adoption, the Applicant is added to the *Approved TFP List* maintained by the FICAM TFS Program and posted on appropriate websites; agencies may be notified of the adoption, and the TFP can be used by the Federal Government.

4.5 TFP Adoption Process Maintenance

The TFPAP 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 FICAM TFS Program oversees trust framework

[7] 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.

adoption process maintenance. The process of drafting revisions of this document will be coordinated with applicable Federal Government agencies and other appropriate private sector stakeholders, such as TFPs, for comment and feedback.

APPENDIX A – TRUST CRITERIA

The below sets the Trust Criteria for LOA 1 through 4.

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

Security

Assurance Level 1 Security Trust Criteria	**Comment**
1. A unique identifier shall be generated and assigned to each CSP applicant.	The intent is to assure that the CSP has a way to uniquely distinguish the person to whom they have issued a credential to within its system boundaries.
2. Transmission of data must take place over a protected session.	The intent here is to make sure that interactions between the user and the CSP and between the CSP and the RP takes place over a protected session.

Privacy

Assurance Level 1 Privacy Trust Criteria	**Comment**
1. The CSP should assign a unique pair-wise identifier to the applicant for each RP, and, by default, only this unique pair-wise identifier shall be forwarded to a Government RP.	The intent is to use a directed identity approach in order to minimize the loss of unlinkability that results when using the same identifier at multiple RPs.
2. Any additional personal information sent from the CSP to the RP shall be limited to only that which has been explicitly requested by the RP with the individual's consent.	The intent is to follow data minimization principles to assure that the CSP does not automatically deliver personal information beyond the identifier. If the RP needs additional information, it will explicitly request it, and only that requested information, if available, should be delivered to the RP.

Assurance Level 1 Privacy Trust Criteria	Comment
3. Non-federal CSPs must not disclose information on end user activities with the government RP to any party, or use the information for any purpose other than federated authentication, except as necessary to comply with law or legal process.	The intent is to limit the use, by the CSP, of user and transactional information gained during the authentication process solely for that purpose.

Conformance to the above trust criteria MAY be self-asserted by the identity service to its TFP.

A-2 Assurance Level 2

Registration and Issuance

Assurance Level 2 R&I Trust Criteria	Comment
1. A trusted relationship shall always exist between the RA and CSP.	The RA can be a part of the CSP, or the RA can be a separate and independent entity. Mechanisms and policies should be in place to ensure each party and its obligations are known to the other. The trust relationship is often contractual, but the trust relationship may also be based on laws and regulations. Mechanisms and policies should be in place to ensure each party and its obligations are known to the other.
2. An Applicant must undergo identity proofing by a trusted RA.	Requires presentation of identifying materials or information.
3. Resist token issuance disclosure threat.	Issue the 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 or credential data that he or she may receive.
5. Resists unauthorized token issuance threat.	Establish procedure to ensure that the individual who receives the token is the same individual who participated in the registration procedure.
6. Resist repudiation of registration threat.	Protect against a Subscriber denying registration, claiming that they did not register that token.
7. Sensitive data collected during the registration and identity proofing stage shall be protected at all times (i.e., transmission, storage) to ensure their security and confidentiality.	Sufficiently protect all sensitive data including Personally Identifiable Information (PII) (as defined by the Federal Government; See TFPAP Identity Manager Services) obtained during registration and identity proofing.
8. The results of the identity proofing step (which may include background investigations of the Applicant) shall be protected to ensure source authentication, confidentiality, and integrity.	
9. The results of the identity proofing step (which may include background investigations of the Applicant) shall be protected to ensure source authentication, confidentiality and integrity.	Sufficiently protect all identity proofing information to ensure it is not tampered with and comes from known, trusted sources.

Assurance Level 2 R&I Trust Criteria	Comment
10. Either the RA or the CSP shall maintain a record of each individual whose identity has been verified and the steps taken to verify his or her identity, including any information collected from the Applicant.	A record of the facts of registration and proofing.
11. The CSP shall have the capability to provide records of identity proofing to RPs if required.	In the event of detected or suspected identity fraud the CSP may be required to provide the detailed records of registration and credential issuance as part of an investigation. Refer to applicable privacy laws, rules of evidence, etc., for what circumstances make it is necessary and/or appropriate for the CSP to provide this information.
12. The identity proofing and registration processes shall be performed according to applicable 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.
13. If the RA and CSP are remotely located and communicate over a network, the entire registration transaction between the RA and CSP shall occur over a mutually authenticated protected session. In all cases, Approved cryptography is required. Equivalently, the transaction may consist of time-stamped or sequenced messages signed by their source and encrypted for their recipient.	See TFPAP Appendix C for definition of "Approved."
14. The CSP shall be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. The CSP shall be capable of conveying this information to Verifiers.	Ensure a person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person.
15. When the identifier associated with a Subscriber is pseudonymous, the RA or CSP shall retain the actual identity of the Subscriber. In addition, pseudonymous credentials shall be distinguishable from credentials that contain verified names.	The identifier associated with the Subscriber may be pseudonymous. Therefore, associate a person's pseudonym to the person's real name and support a mechanism to specify whether the name in the credential is real or pseudonym.
16. PII collected as part of the registration process shall be protected.	See TFPAP Appendix C for definition of PII.
17. The Applicant shall supply 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 personally identifiable information.	

Assurance Level 2 R&I Trust Criteria	**Comment**
18. For In-Person Proofing: *a)* Possession of a valid current primary Government Picture ID that contains Applicant’s picture, and either address of record or nationality of record (e.g. driver’s license or Passport) shall be required. *b)* The RA shall inspect the photo-ID, compare picture to Applicant, record ID number, address and date of birth (DOB). *c)* If photo ID appears valid and the photo matches Applicant then: *i)* If personal information in the records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use; OR *ii)* If ID confirms address of record, the RA authorizes or the CSP shall issue credentials. Notice shall be sent to the address of record; OR *iii)* If ID does not confirm address of record, the CSP shall issue credentials in a manner that confirms the claimed address. *d)* Employers and educational institutions who verify the identity of their employees or students by means comparable to those stated here may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through online processes, where notification is via the distribution channels normally used for sensitive, personal communications.	If the ID does not confirm address of record, then the issuance process should include a mechanism to confirm the address of record. Employers and educational institutions who verify the identity of their employees or students by means comparable to those stated here may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through online processes, where notification is via the distribution channels normally used for sensitive, personal communications.

19. For Remote Proofing: *a)* Possession of a valid Government ID (e.g. a driver’s license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card, or tax ID) confirmed via records of either the government ID or account number shall be required. *b)* The RA shall inspect both ID number and account number supplied by the Applicant (e.g. for correct number of digits). *c)* The RA shall verify the information provided by the 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 and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) *d)* Address/phone number confirmation and notification shall be done as follows: *i)* The CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in records; OR *ii)* If personal information in records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days; OR iii) The CSP shall issue credentials. The RA or CSP shall send a notice to an address of record confirmed in the records check. *e)* Employers and educational institutions who verify the identity	Note that confirmation of the financial or utility account may require supplemental information from the applicant. The requirement for a financial account or utility account number may be satisfied by a cellular or landline telephone service account under the following conditions: • The phone is associated in Records with the Applicant's name and address of record; AND • The applicant demonstrates that they are able to send or receive messages at the phone number. Methods (i) and (ii) are recommended to achieve better security. Method (iii) is especially weak when not used in combination with knowledge of account activity.

of their employees or students by means comparable to those stated here may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through online processes, where notification is via the distribution channels normally used for sensitive, personal communications.	
20. Registration, identity proofing, token creation/issuance, and credential issuance are separate processes that can be broken up into a number of separate physical encounters or electronic transactions. (Two electronic transactions are considered to be separate if they Electronic Authentication Guideline are not part of the same protected session.) In these cases, to ensure that the same party acts as Applicant throughout the processes: *a)* For electronic transactions, 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. *b)* For physical transactions, the Applicant shall identify himself/herself in person by either using a secret as described above, or by biometric verification (comparing a captured biometric sample to a reference biometric sample that was enrolled during a prior encounter).	
21. Federal or State laws and regulations impose requirements for institutions in certain businesses to confirm the educational and licensing credentials for selected employees or affiliates. Where institutions in these businesses rigorously confirm the identity, education, and licensing credentials of a licensed professional through an in-person appearance before employment or affiliation, issuance of e-authentication credentials without repeating the identity proofing process is allowed as follows: a) The initial process for confirming the identity, education, and licensing credentials of a licensed professional through an in-	For example, a health care organization that has accepted the Medicare "Conditions for Participation" is required to examine the credentials for each candidate for the medical staff.

person process shall include the following steps: i) Verification of a current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., a driver's license or passport); ii) Verification of post-secondary education/training of two or more years appropriate for the position (e.g., an appropriate medical degree); AND iii) Verification of current state or federal licensure (e.g., as a physician) based on an examination process, with requirements for continuing education or active professional participation as a condition of valid licensing. b) Institutions that have performed a process satisfying these conditions may issue e-authentication tokens and credentials to those employees and affiliates with verified credentials provided that the issuance process is either: i) In-person; OR *ii)* The remote issuance process incorporates the address/phone number confirmation appropriate for that level; AND *iii)* They meet the corresponding provisions of the Token, Token and Credential Management, Authentication Process, and Assertion tables.	

22. Before issuing any derived credential the CSP shall verify the original credential status and shall verify that the corresponding token is possessed and controlled by the Claimant. The status of the original credential should be re-checked at a later date (e.g. after a week) to confirm that it was not compromised at the time of issuance of the derived credential. (This guards against the case where an Attacker requests the desired credential before revocation information can be updated.) The CSP shall record the details of the original credential used as the basis for derived credential issuance.	Where the Applicant already possesses recognized authentication credentials, the CSP may choose to identity proof the Claimant by verifying possession and control of the token associated with the credentials and issue a new derived credential.

Tokens

Assurance Level 2 Tokens Trust Criteria	**Comment**
1. Resist token theft threat.	Protect a token with a physical manifestation 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.

Assurance Level 2 Tokens Trust Criteria	Comment
4. For memorized secret tokens: a) The memorized secret shall be: i) A randomly generated PIN consisting of 6 or more digits; OR ii) A user generated string consisting of 8 or more characters chosen from an alphabet of 90 or more characters; OR iii) A secret with equivalent entropy. b) The CSP shall implement dictionary or composition rules to constrain user-generated secrets. c) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period.	A Memorized Secret Token is a secret shared between the Subscriber and the CSP. Memorized Secret Tokens are typically character strings (e.g., passwords and passphrases) or numerical strings (e.g., PINs.) See NIST SP 800-63 Appendix A, Table A.1 for details on entropy. While a throttling implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See NIST SP 800-63 Section 8.2.3 for more detailed advice.
5. For pre-registered knowledge tokens: a) The secret shall provide at least 20 bits of entropy. b) An empty answer shall be prohibited. The entropy in the secret shall not be directly calculated (e.g., the user chosen or personal knowledge questions). If the questions are not supplied by the user, the user shall select prompts from a set of at least seven questions. c) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period.	See NIST SP 800-63 Appendix A, Table A.1 for details on entropy. While a throttling implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See NIST SP 800-63 Section 8.2.3 for more detailed advice.
6. For Look-up secret tokens: a) The token authenticator shall have 64 bits of entropy; OR b) The token authenticator shall have at least 20 bits of entropy, and the Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period.	See NIST SP 800-63 Appendix A, Table A.1 for details on entropy. While a throttling implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See NIST SP 800-63 Section 8.2.3 for more detailed advice.

Assurance Level 2 Tokens Trust Criteria	**Comment**
7. For Out of Band tokens: a) The token shall be uniquely addressable and shall support communication over a channel that is separate from the primary channel for e-authentication. *b)* The Verifier generated secret shall: i) Have at least 64 bits of entropy; OR ii) Have at least 20 bits of entropy, and the Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period.	See NIST SP 800-63 Appendix A, Table A.1 for details on entropy. While a throttling implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See NIST SP 800-63 Section 8.2.3 for more detailed advice.
8. For Single Factor, One-Time Password Device: a) The token shall use Approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password. b) The one-time password shall have a limited lifetime, on the order of minutes. *c)* The cryptographic module performing the verifier function 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. See TFPAP Appendix C for definition of "Approved." See TFPAP Appendix B for reference to FIPS 140-2 document
9. For single factor cryptographic devices: a) The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher. *b)* Verifier-generated token input (e.g., nonce, challenge) shall have at least 64 bits of entropy.	See TFPAP Appendix B for reference to FIPS 140-2 document. See NIST SP 800-63 Appendix A, Table A.1 for details on entropy.
10. When a multi-token authentication scheme is being used, the new level assurance shall be determined in accordance with NIST SP 800-63 Table 7. Using multiple tokens to achieve an increased level of assurance shall require the use of two different factors of authentication.	Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained. Factors of authentication include *something you have* and *something you know.* 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.

Assurance Level 2 Tokens Trust Criteria	**Comment**
11. Multi-stage authentication processes, which use a single-factor token to obtain a second token, shall not constitute multi-factor authentication.	The level of assurance associated with the compound solution is the assurance level of the weakest token.

Token and Credential Management

Assurance Level 2 T&C Management Trust Criteria	**Comment**
1. Files of shared secrets used by CSPs shall be protected by 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 should 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; OR 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.	Sufficiently protect shared secrets such as passwords. See TFPAP 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 other party except Verifiers operated by the CSP; however, session (temporary) shared secrets may be provided by the CSP to independent Verifiers. Cryptographic protections shall be required for all messages between the CSP 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 session to an authenticated party to ensure confidentiality and tamper protection. If the CSP sends the Verifier a message that either asserts that a weakly bound credential is valid, or that a strongly bound credential has not been subsequently revoked, 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 CSP. 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.	Sufficiently protect long term shared authentication secrets. Alternatively, the time stamped message, binding, and credential may all be signed by the CSP, although, in this case, the three in combination would comprise a strongly bound credential with no need for revocation.

Assurance Level 2 T&C Management Trust Criteria	**Comment**
3. The CSP 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 CSP allowing renewal and re-issuance. Passwords shall not be renewed; they shall be re-issued. After expiry of current token and any grace period, renewal and re-issuance shall not be allowed. Upon re-issuance, token secrets shall not be set to a default or reused in any manner. All interactions shall occur over a protected channel such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS).	
4. CSPs 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 CSP issues credentials that expire automatically within 72 hours then the CSP is not required to provide an explicit mechanism to revoke the credentials. CSP that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.	For PKI credentials, Federal ICAM relies on the proven criteria and methodology of the FPKIPA.

Assurance Level 2 T&C Management Trust Criteria	Comment
5. A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representative. The record retention period of data is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs 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. The CSP should establish policies for token collection to avoid the possibility of unauthorized use of the token after it is considered out of use.	The CSP 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. The authentication process shall resist online guessing threat.	Protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. The authentication process shall 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. The authentication process shall 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 2 Authentication Process Trust Criteria	**Comment**
4. The authentication process shall resist eavesdropping threat. Approved cryptography shall be 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."
5. The authentication process shall at least 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. For example, sending a password over server authenticated TLS is weakly resistant to man-in the middle attacks. The browser allows the Claimant to verify the identity of the Verifier; however, if the Claimant is not sufficiently vigilant, the password will be revealed to an unauthorized party who can abuse the information.
6. Successful authentication shall require 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.
7. 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.
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. Session data transmitted between the Claimant and the RP following a successful authentication shall be protected.	This includes addressing transmission confidentiality and integrity.

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.

Ongoing Verification

[NOTE: This trust criterion is currently optional.It is recommended that TFPs integrate this into their trust framework.]

Assurance Level 2 Ongoing Verification Trust Criteria	Comment
1. Implement an out-of-band identity verification mechanism for account maintenance activities.	Use a channel, other than the web channel, in order to implement a verification mechanism before permitting high value account management functions such as password resets.
2. The authentication process shall implement a device fingerprinting capability.	Implement the ability to fingerprint (based on device configuration, Internet Protocol (IP) address, geo-location, etc.) with the initial binding of the fingerprint to the user utilizing an out-of-band identity verification mechanism.
3. The authentication process shall implement internet protocol (IP) reputation based tools to mitigate fraudulent activity.	Implement an IP blacklisting capability to block connection to servers from IP addresses known or suspected to be associated with fraudulent activities.
4. The authentication process shall implement an “out-of-wallet” question capability.	Implement a capability that is capable of leveraging internal data (i.e., not residing in public databases in order to authorize higher risk transactions).
5. The authentication process shall include an anomaly detection capability.	Implement a capability that is capable of detecting fraudulent behavior (e.g., velocity of transactions, customer history and behavior).

Privacy

Assurance Level 2 Privacy Trust Criteria	Comment
1. Opt In	CSP 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. CSP should allow End Users to opt out of individual attributes for each transaction.
2. Minimalism	CSP must transmit only those attributes that were explicitly requested by the RP application or required by the federal profile.
3. Activity Tracking	Commercial CSP must not disclose information on End User activities with the government to any party, nor use the information for any purpose other than federated authentication or to comply with law or legal process.
4. Adequate Notice	CSP 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.
5. Termination	In the event a CSP ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.

A-3 Assurance Level 3

Registration and Issuance

Assurance Level 3 R&I Trust Criteria	Comment
1. A trusted relationship shall always exist between the RA and CSP.	The RA can be a part of the CSP, or the RA can be a separate and independent entity. Mechanisms and policies should be in place to ensure each party and its obligations are known to the other. The trust relationship is often contractual, but the trust relationship may also be based on laws and regulations. Mechanisms and policies should be in place to ensure each party and its obligations are known to the other.
2. An Applicant must undergo identity proofing by a trusted RA.	Requires presentation and verification of identifying materials or information.
3. Resist token issuance disclosure threat.	Issue the 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 or credential data that he or she may receive.
5. Resists unauthorized token issuance threat.	Establish procedure to ensure that the individual who receives the token is the same individual who participated in the registration procedure.
6. Resist repudiation of registration threat.	Protect against a Subscriber denying registration, claiming that they did not register that token.
7. Sensitive data collected during the registration and identity proofing stage shall be protected at all times (i.e., transmission, storage) to ensure their security and confidentiality.	Sufficiently protect all sensitive data including PII (as defined by the Federal Government; See Appendix C) obtained during registration and identity proofing.
8. The results of the identity proofing step (which may include background investigations of the Applicant) shall be protected to ensure source authentication, confidentiality and integrity.	Sufficiently protect all identity proofing information to always ensure it is not tampered with and comes from known, trusted sources.

Assurance Level 3 R&I Trust Criteria	Comment
9. Either the RA or the CSP shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including any information collected from the Applicant.	A record of the facts of registration and proofing.
10. The CSP shall have the capability to provide records of identity proofing to RPs if required.	In the event of detected or suspected identity fraud the CSP may be required to provide the detailed records of registration and credential issuance as part of an investigation. Refer to applicable privacy laws, rules of evidence, etc. for what circumstances make it necessary and/or appropriate for the CSP to provide this information.
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.	`
12. If the RA and CSP are remotely located and communicate over a network, the entire registration transaction between the RA and CSP shall occur over a mutually authenticated protected session. In all cases, Approved cryptography is required.	See TFPAP Appendix C for definition of "Approved." Equivalently, the transaction may consist of time-stamped or sequenced messages signed by their source and encrypted for their recipient.
13. The CSP shall be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber. The CSP shall be capable of conveying this information to Verifiers.	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 verified.	Pseudonyms are not allowed, and therefore the CSP must verify real names.
15. PII collected as part of the registration process shall be protected.	See TFPAP Appendix C for definition of PII.
16. The Applicant shall supply 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 personally identifiable information.	

Assurance Level 3 R&I Trust Criteria	Comment
17. For In-Person Proofing: a) Possession of a verified current primary Government Picture ID that contains the Applicant’s picture and either address of record or nationality (e.g. driver’s license or passport) shall be required. b) The RA shall inspect the Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. c) The RA shall confirm that name, DOB, address and other personal information in the records are consistent with the application. d) The RA shall compare the picture to the Applicant and records the ID number. e) If the ID is valid and the photo matches the Applicant then: *i)* If the personal information in the records includes a telephone number, the CSP shall issue 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 alternative means that establish an equivalent level of non-repudiation; OR *ii)* If the ID confirms the address of record, the RA shall authorize or the CSP shall issue credentials. A notice shall be sent to the address of record; OR iii) If the ID does not confirm address of record, the CSP shall issue credentials in a manner that confirms the claimed address.	
18. For Remote Proofing: a) Possession of a valid Government ID (e.g. a driver’s license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via records of both numbers shall be required.	Note that confirmation of the financial or utility account may require supplemental information from the Applicant.

Assurance Level 3 R&I Trust Criteria	**Comment**
b) The RA shall verify information provided by the Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases. c) The RA shall confirm that name, DOB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. d) At a minimum, the records check for both the ID number AND the account number s shall confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) e) For address confirmation: *i)* The CSP shall issue credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; OR *ii)* If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant’s name, and are consistent with the information provided by the applicant, then the CSP may issue credentials in a manner that confirms ability of the Applicant to receive messages (SMS, voice or email) sent to the electronic address. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days. f) The requirement for a financial account or utility account number may be satisfied by a cellular or landline telephone service account under the following conditions: *i)* The phone is associated in Records with the Applicant's name and address of record; AND *ii)* The applicant demonstrates that they are able to send or receive messages at the phone number.	

Assurance Level 3 R&I Trust Criteria	**Comment**
19. Registration, identity proofing, token creation/issuance, and credential issuance are separate processes that can be broken up into a number of separate physical encounters or electronic transactions. (Two electronic transactions are considered to be separate if they Electronic Authentication Guideline are not part of the same protected session.) In these cases, to ensure that the same party acts as Applicant throughout the processes: a) For electronic transactions, the Applicant shall identify ` reused. If the CSP issues permanent secrets during a physical transaction, then they shall be loaded locally onto a physical device that is issued in person to the Applicant or delivered in a manner that confirms the address of record. b) For physical transactions, 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. If the CSP issues permanent secrets during a physical transaction, then they shall be loaded locally onto a physical device that is issued in person to the Applicant or delivered in a manner that confirms the address of record.	

Assurance Level 3 R&I Trust Criteria	Comment
20. Federal or State laws and regulations impose requirements for institutions in certain businesses to confirm the educational and licensing credentials for selected employees or affiliates. Where institutions in these businesses rigorously confirm the identity, education, and licensing credentials of a licensed professional through an in-person appearance before employment or affiliation, issuance of e-authentication credentials without repeating the identity proofing process is allowed as follows: a) The initial process for confirming the identity, education, and licensing credentials of a licensed professional through an in-person process shall include the following steps: i) Verification of a current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., a driver's license or passport); ii) Verification of post-secondary education/training of two or more years appropriate for the position (e.g., an appropriate medical degree); AND iii) Verification of current state or federal licensure (e.g., as a physician) based on an examination process, with requirements for continuing education or active professional participation as a condition of valid licensing. b) Institutions that have performed a process satisfying these conditions may issue e-authentication tokens and credentials to those employees and affiliates with verified credentials provided that the issuance process is either: **i)** In person; OR ii) The remote issuance process incorporates the address/phone number confirmation appropriate for that level; AND *iii)* They meet the corresponding provisions of the Token, Token and Credential Management, Authentication Process, and Assertion tables.	For example, a health care organization that has accepted the Medicare "Conditions for Participation" is required to examine the credentials for each candidate for the medical staff.

Assurance Level 3 R&I Trust Criteria	Comment
21. PKI credentials shall be issued by a CA cross-certified with the Federal Bridge Certification Authority (FBCA) under FBCA Certificate Policy (CP), Common 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 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 Multi-Factor Software Cryptographic Tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication. The Verifier-generated token input (e.g., a nonce or challenge) shall have at least 64 bits of entropy.	See TFPAP Appendix B – Reference DocumentationAppendix B for reference to FIPS 140-2 document. See NIST SP 800-63 Appendix A, Table A.1 for details on entropy.

Assurance Level 3 Tokens Trust Criteria	**Comment**
5. When a multi-token authentication scheme is being used, new level assurance shall be in accordance with NIST SP 800-63 Table 7. Using multiple tokens to achieve an increased level of assurance shall require the use of two different factors of authentication.	Combining multiple factors and/or multiple tokens may achieve a higher assurance level than would otherwise be attained. 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. LOA 3 can be achieved using two tokens rated at Level 2 that represent two different factors of authentication. Since the use of biometrics as a stand-alone token for remote authentication is not addressed, achieving Level 3 with separate Level 2 tokens implies *something you have* and *something you know*.
6. Multi-stage authentication processes, which use a single-factor token to obtain a second token, shall not constitute multi-factor authentication.	The level of assurance associated with the compound solution is the assurance level of the weakest token.

Token and Credential Management

Assurance Level 3 T&C Management Trust Criteria	Comment
1. Files of long-term shared secrets used by CSP or Verifiers shall be protected by 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 Federal Information Processing Standards (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.	Strongly bound credentials support tamper detection mechanisms such as digital signatures, but weakly bound credentials can be protected against tampering using access control mechanisms as described in the first column. See TFPAP Appendix B for reference to FIPS 140-2 document.
2. CSPs shall provide a secure mechanism to allow Verifiers or RPs to ensure that the credentials are valid. Such mechanisms may include on-line validation servers or the involvement of CSP servers that have access to status records in authentication transactions. Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party Verifiers, as a part of the verification services offered by the CSP, 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 TFPAP Appendix C for definition of "Approved."

Assurance Level 3 T&C Management Trust Criteria	Comment
3. Renewal and re-issuance shall only occur prior to expiration of the current credential. Claimants shall authenticate to the CSP 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. CSPs 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.	
5. A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representative. The record retention period of data is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs 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. The CSP should establish policies for token collection to avoid the possibility of unauthorized use of the token after it is considered out of use.	The CSP 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 3 Authentication Process Trust Criteria	**Comment**
1. The authentication protocol shall resist online guessing threat.	Protect against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. The authentication protocol shall 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. The authentication protocol shall 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.
4. The authentication protocol shall resist eavesdropping threat. Approved cryptography shall be 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."
5. The authentication protocol shall 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/RP, and revealing sensitive information, downloading harmful software or contributing to a fraudulent act.

Assurance Level 3 Authentication Process Trust Criteria	**Comment**
6. The authentication protocol shall at least 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. For example, sending a password over server authenticated TLS is weakly resistant to man-in the middle attacks. The browser allows the Claimant to verify the identity of the Verifier; however, if the Claimant is not sufficiently vigilant, the password will be revealed to an unauthorized party who can abuse the information.
7. At least two authentication factors shall be required.	The three types of authentication factors are something you know, something you have, and something you are.
8. Authentication shall be based on proof of possession of the allowed types of tokens through a cryptographic protocol. Authentication shall require 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.
9. Strong cryptographic mechanisms shall be used to protect token secret(s) and authenticator(s).	
10. Long-term shared authentication secrets, if used, shall never be revealed to any party except the Claimant and CSP. However, session (temporary) shared secrets may be provided to Verifiers by the CSP, possibly via the Claimant.	
11. 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.

Assurance Level 3 Authentication Process Trust Criteria	**Comment**
12. 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.
13. Session data transmitted between the Claimant and the RP following a successful authentication shall be protected.	Protect data exchanged between the end user and the RP. This includes addressing transmission confidentiality and integrity.
14. Approved cryptographic techniques shall be used for all operations, including the transfer of session data.	See Appendix C for definition of "Approved."

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.

Ongoing Verification

[NOTE: This trust criterion is currently optional. It is recommended that TFPs integrate this into their trust framework]

Assurance Level 2 Ongoing Verification Trust Criteria	**Comment**
1. Implement an out-of-band identity verification mechanism for account maintenance activities.	Use a channel, other than the web channel, in order to implement a verification mechanism before permitting high value account management functions such as password resets.
2. The authentication process shall implement a device fingerprinting capability.	Implement the ability to fingerprint (based on device configuration, IP address, geo-location etc.) with the initial binding of the fingerprint to the user utilizing an out-of-band identity verification mechanism.

Assurance Level 2 Ongoing Verification Trust Criteria	**Comment**
3. The authentication process shall implement internet protocol (IP) reputation based tools to mitigate fraudulent activity.	Implement an IP blacklisting capability to block connection to servers from IP addresses known or suspected to be associated with fraudulent activities.
4. The authentication process shall implement an “out-of-wallet” question capability.	Implement a capability that is capable of leveraging internal data i.e. not residing in public databases in order to authorize higher risk transactions.
5. The authentication process shall include an anomaly detection capability.	Implement a capability that is capable of detecting fraudulent behavior e.g. velocity of transactions, customer history and behavior etc.

Privacy

Assurance Level 3 Privacy Trust Criteria	**Comment**
1. Opt In	CSP 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. CSP should allow End Users to opt out of individual attributes for each transaction.
2. Minimalism	CSP must transmit only those attributes that were explicitly requested by the RP application or required by the federal profile.
3. Activity Tracking	Commercial CSP must not disclose information on End User activities with the government to any party, nor use the information for any purpose other than federated authentication or to comply with law or legal process.
4. Adequate Notice	CSP 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.
5. Termination	In the event a CSP ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.

A-4 Assurance Level 4

LOA 4 PKI is addressed in the cross-certification process of the FPKIPA, a FICAM TFS-adopted TFP.

APPENDIX B – REFERENCE DOCUMENTATION

[1] HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
https://www.dhs.gov/homeland-security-presidential-directive-12#1

[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/sites/default/files/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] Fair Information Practice Principles
http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

[9] X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
http://www.idmanagement.gov/sites/default/files/documents/FBCA_CP_RFC3647.pdf

[10] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
http://www.idmanagement.gov/sites/default/files/documents/CommonPolicy.pdf

[11] Citizen and Commerce Class Common Certificate Policy
http://www.idmanagement.gov/sites/default/files/documents/citizen_commerce_cp.pdf

[12] 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.idmanagement.gov/sites/default/files/documents/crosscert_method_criteria%20v3.0%20%282%29_2.doc

APPENDIX C – TERMINOLOGY

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 RP 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 CSP audit processes, and ongoing TFP CSP 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 RP has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the RP.
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 CSP is the determination that the CSP'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.
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 RP. The assertion is used by the Claimant/Subscriber to authenticate to the RP.
E-Authentication	An object that authoritatively binds an identity (and optionally, additional attributes) to a

Term	Definition
Credential	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 RP 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.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP 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 RP. In this model, the assertion reference is used by the Claimant/Subscriber to authenticate to the RP. The RP 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 a CSP.
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.
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.

Term	Definition
Multi-factor Authentication	Use of two or more of the 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.
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.

Term	Definition
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 dependent upon the token authenticator, but they may or may not explicitly contain it.
Trust Criteria	Set of benchmarks used to measure a CSP'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 a CSP'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 CSPs 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.
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
ATOS	Authority To Offer Services
CA	Certification Authority
CISA	Certified Information System Auditor
CP	Certificate Policy
CSP	Credential Service Provider
DOB	Date of Birth
EGTS	E-Governance Trust Services
FBCA	Federal Bridge Certification Authority
FCIOC	Federal Chief Information Officers Council
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal Public Key Infrastructure Policy Authority
HSPD-12	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ID	Identification
IP	Internet Protocol
IT	Information Technology
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
SP	Special Publication
SSL	Secure Sockets Layer
TFET	Trust Framework Evaluation Team
TFP	Trust Framework Provider
TFPAP	Trust Framework Adoption Process
TFS	Trust Framework Solutions
TLS	Transport Layer Security