Federal Identity, Credential, and Access Management Trust Framework Solutions

Authority To Offer Services (ATOS)

For

FICAM TFS Approved Identity Services

Version 1.0.0
DRAFT: 11/11/13

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

Table of Contents

1. PURPOSE

This document is the *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* and defines the process by which an Applicant, who has been qualified by a FICAM Adopted Trust Framework Provider (TFP) to meet FICAM TFS Privacy and Security requirements, can apply to the FICAM TFS Program to be approved to offer their services to the U.S. Federal Government.

1.1 Audience

This guideline is intended for:

- **Token Managers, Identity Managers and Credential Service Providers**, who are seeking to offer their services for use by the U.S. federal government.
- **Trust Framework Providers**, who are providing guidance to entities that they have qualified under their trust framework, on how to obtain approval to offer services to the U.S. Federal Government.
- **Security and Privacy Practitioners**, who recommend, design, build or provide solutions that meet U.S. Federal Government requirements

1.2 Usage

1. Read the *Trust Framework Solutions Overview* to understand the background, authorities and components of the FICAM TFS Program
2. 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
3. Read the *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance* to understand the role of the Trust Framework Provider
4. 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.

2. BACKGROUND

The FICAM Trust Framework Solutions (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)

Organizations that define a Trust Framework and certify entities compliant with it are called Trust Framework Providers (TFPs). Once a TFP has been adopted by FICAM TFS Program, it then has the ability to assess and certify various identity services such as Token Managers (TMs) which provide the authentication functions, Identity Managers (IMs) which provide the identity proofing and attribute management functions, and Credential Service Providers (CSPs) who provide a full service capability that combines authentication, identity proofing and the secure binding of token(s) to identity.

The identity services that have been qualified by a FICAM Approved TFP as meeting TFPAP requirements have the option of applying to the FICAM TFS Program to request approval for the authority to offer their services to the U.S. Federal Government provided they can satisfy the requirements outlined in this document.

3. REQUIREMENTS

3.1 General Requirements

3.1.1 FICAM TFS Adopted Trust Framework Provider Approval

- The Applicant must have been assessed and approved by a FICAM Adopted Trust Framework Provider
- The Applicant continues to maintain an active approval status under a FICAM Adopted TFP

NOTE: This requirement does not apply to financial institutions regulated by Federal agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC), who are required to implement a Customer Identification Program. The FICAM TFS Program may consult with federal agencies that have regulatory responsibility for the Applicant regarding input into the approval process.

3.1.2 FICAM TFS Program Testing

- The Applicant must make available to the FICAM TFS Program, on an as-needed basis, an Internet accessible environment, and supporting resources, that enables the Program to verify the Applicant's compliance to FICAM Approved Protocols, Profiles and Processes.
- A TFS Program Approved Testing Facility may conduct the tests and provide the results directly to the TFS Program or the tests may be conducted directly by the TFS Program.

3.1.3 Implement FICAM TFS TFPAP Approved Configuration

- The Applicant, when integrating with a Government Relying Party, MUST implement the FICAM TFS Program tested and approved configuration.

3.1.4 Use of Transaction Data

The Applicant must ensure transaction data of individuals interacting with the Applicant, generated in its interactions with the Government will not be used for data mining or analysis

except for security purposes, which may include investigation of administrative, technical or physical security breaches and which may or may not include a privacy breach.

Security breaches include breaches by internal or external forces and may include but are not limited to suspected malfeasance or misuse of data or systems. The Applicant may only use this data for the security purposes related to the work with Government and must not provide such data to any other entity with the exception of the U.S. law enforcement entities as required by law.

The FICAM TFS Program shall be notified, in writing, of any data mining or analysis for security purposes, in advance. Data mining, analyses and analytics for the purpose of other business objectives and purposes such as for re-sale, marketing, product analysis or product development is prohibited. Such prohibited data mining includes creating user profiles or patterns of use, whether at the level of the individual, identified user groups or the entire user community.

3.1.5 Availability of Annual Release Plan

The Applicant must provide, within 30 days of being requested by the FICAM TFS Program, an up-to-date annual release plan. The annual release plan will identify the schedule, functionality and technical characteristics of any planned changes to the service offered by the Applicant to the Government.

3.1.6 Change, Incident and Problem Management

The Applicant must provide a Change, Incident and Problem Management process. In particular, the Applicant must document and implement a process that alerts the TFS Program of changes to its service offering that would impact Government relying parties.

The Applicant must provide both Administrative and Technical Points of Contact to the FICAM TFS Program and make every reasonable effort to keep the contact information up to date

3.2 System and Operations

3.2.1 Provide Verified Identity Attributes

Identity attributes that are used to uniquely distinguish between individuals (versus describing individuals) are referred to as *identifiers*. Determining uniqueness may also be referred to as *identity resolution*. Identity resolution is the ability to resolve identity attributes to a unique individual (i.e. no other individual has the same set of attributes.)

The Applicant, if an Identity Manager or a Credential Service Provider, seeking approval at Levels 2, 3 or 4, MUST identify which of the **verified** (not self-asserted) attributes, from the listing below, they are able to provide to Relying Parties (RPs):

Table 1: Identity Attributes

Core Identity Attributes	Supplemental Identity Attributes
• **Name:** (Legal First Name and Legal Last Name) • **Current Address:** (Postal Code) • **Current Address:** (City and State) • **Partial Date of Birth:** (Month and Day) • **Partial Date of Birth:** (Year) • **Full Date of Birth** • **Partial SSN:** (Last 4 digits) • **Full SSN:** (All 9 digits) • **Place of Birth:** (City) • **Place of Birth:** (County) • **Place of Birth:** (State) • **Place of Birth:** (Country)	• **Mother's Name**: (At Birth) • **Mother's Name**: (Prior to first marriage) • **Middle Name** • **Middle Initia**l • **Current Address:** (Street) • **Partial Past Address**: (Previous City) • **Partial SSN:** (First 5 digits) • **Sex**

The selection of the above identity attributes is based on open standards work on identity resolution. More information on that work and how it may be leveraged by Agencies can be found in Appendix A of this document.

- Applicant must be capable of technically providing, **upon RP request via approved protocols and profiles,** dynamic combinations of available attributes from the Table 1 listing.
- For Identity Managers and CSPs seeking approval at Levels 2, 3, or 4, the ability to provide attributes that enable identity resolution at the RP using a standardized approach (See Appendix A - Table 2), is a critical factor in the TFS Program approval process.
- The TFS Program, on a case-by-case basis and based on ongoing lessons learned, may approve domain specific identifiers or additional attributes, as alternatives or additions to the list above.

3.2.2 Provide Metadata for incorporation into the E-Government Trust Services (EGTS) Metadata Service

- Applicant, if an Identity Manager or a Credential Service Provider, must make all Metadata available to FICAM TFS Program who will use it for compliance verification testing and share it with Government Relying Parties as appropriate
- The attributes available from the Applicant must be documented in the Metadata provided to the FICAM TFS Program.
- Applicant must notify FICAM TFS Program of any planned Metadata changes no less than 6 weeks in advance of the changes.

4. APPLICANT APPROVAL PROCESS

This section specifies the Applicant approval process.

4.1 Consultation with FICAM TFS Program

The process begins with the Applicant initiating contact with the FICAM TFS Program Manager (TFS.EAO@gsa.gov) to schedule a consultation to discuss the TFS Process.

If the Applicant is interested in offering its services to the Government, it is highly recommended that it contact the TFS Program prior to initiating the TFP approval process.

4.2 Approval Package Submission

The Applicant submits a Request for Approval Package, which includes:

- Technical POC Contact Info
- Program Manager Contact Info
- Technical information (Metadata, Endpoints, Test Credentials etc.) that will enable FICAM Program to remotely test and verify Applicant's conformance to FICAM protocols, profiles and processes
- Identity Services at Level 1 Only
    - Documentation of the FICAM Adopted TFP Approval, including details regarding trust criteria mapping
        - NOTE: At Level 1, this requirement does not apply to financial institutions regulated by Federal agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC), who are required to implement a Customer Identification Program. The FICAM TFS Program may consult with federal agencies that have regulatory responsibility for the Applicant regarding input into the approval process.
    - Listing of available attributes, if any (Identity Manager or a CSP)
- Identity Services at Level 2 and Higher

- Documentation of the FICAM Adopted TFP Approval, including details regarding trust criteria mapping
  - NOTE: At Level 2, this requirement does not apply to financial institutions regulated by Federal agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC), who are required to implement a Customer Identification Program. The FICAM TFS Program may consult with federal agencies that have regulatory responsibility for the Applicant regarding input into the approval process. Contact FICAM TFS Program Manager (TFS.EAO@gsa.gov) regarding Level 3 Requirements.
- Documentation of Change, Incident and Problem Management Process
- Annual Release Plan
- Metadata (Identity Manager or a CSP)
- Listing of available verified attributes (Identity Manager or a CSP)

- Documentation of the process to alert the TFS Program of changes to the Applicant's service offering that would impact Government relying parties

4.3 Assessment and Testing

Testing to verify if the Applicant is compliant to FICAM Approved Protocols, Profiles and Processes is a critical component of the Approval Process. A TFS Program Approved Testing Facility may conduct the tests and provide the results directly to the TFS Program or the tests may be conducted directly by the TFS Program.

The TFS Program may, as needed, request additional information from the Applicant and/or the TFP that qualified the Applicant.

4.4 Approval Decision

The FICAM TFS Program reviews the Test Results, the suitability, value, and long-term viability of the Applicant for Government use, as well as additional factors from consultation with relevant government agencies and organizations to decide on whether or not to approve the Applicant.

The Applicant is informed of the decision and if approved, is required to sign a MOA with the FICAM TFS Program, which delineates the Applicant's responsibilities to be compliant to the FICAM Approved Protocols, Profiles and Processes.

Once the FICAM TFS Program has received the signed MOA, the Applicant is added to the *Approved Identity Services List* maintained by the FICAM TFS Program and posted on appropriate websites; agencies may be notified of the approval, and Federal government RPs can use the Identity Services.

NOTE: Once approved the Applicant may request, from the FICAM TFS Program Manager (TFS.EAO@gsa.gov), a Clearance Letter that demonstrates its compliance to the E-Authentication Architecture.

4.5 Limits on approval

The approval is limited to a period of one year.

Provided all of the requirements continue to be met, applicants may renew their status on an annual basis with the FICAM TFS Program.

The FICAM TFS Program has sole discretion on granting this approval and any associated Trust-Marks. In addition, the TFS Program reserves the right to revoke its approval at any time if the Applicant is not meeting the needs of the Government or the requirements outlined in this document.

5. APPENDIX A – STANDARDS BASED IDENTITY RESOLUTION

The core identity attributes in Section 3.2.1 are based on combinations (See Table 2 below) of identity attributes, from the ANSI/NASPO-IDPV-2013 standard, that are **equivalent in resolving** a unique individual in 96% of cases. For RPs seeking to fully resolve an identity, **in cases where the set of core identity attribute combinations has failed**, the ANSI/NASPO-IDPV-2013 standard recommends starting with a core identity attribute bundle and utilizing the supplemental attributes, which shall be selected incrementally until full resolution of identity is reliably achieved.

Table 2: Identity Attribute Bundles[1]

Bundle	**Core Identity Attribute Combinations** Sufficient to uniquely resolve 96%[2] of the U.S. population	**Supplemental Identity Attributes** (To be added incrementally to the core to reach 100% resolution.[3])
1	• **Name:** (Legal First Name and Legal Last Name) • **Partial Current Address:** (Postal Code) or (City and State) • **Partial Date of Birth:** (month and day) or (year)	• **Mother's Name**: (At Birth or Prior to first marriage) • **Middle Name or Initial** • **Place of Birth:** (Country) • **Place of Birth:** (State) • **Place of Birth:** (City) • ~~**Current Address:** (State)~~ • ~~**Current Address:** (City)~~ • **Current Address:** (Street) • **Previous City** • **Full Date of Birth** • **Full SSN:** (All 9 digits) • **Partial SSN:** (First 5 digits) • **Partial SSN:** (Last 4 digits) • **Sex**
2	• **Name:** (Legal First Name and Legal Last Name) • **Full Date of Birth**: (Month, Day, and Year)	• **Mother's Name:** (At birth or prior to first marriage) • **Middle Name or Initial** • **Place of Birth:** (Country) • **Place of Birth:** (State) • **Place of Birth:** (City)

[1] This table is the result of a study cited in ANSI/NASPO-IDPV-2013 *Requirements and Implementation Guidelines for Assertion, Resolution, Evidence and Verification of Personal Identity*, Working Group Draft Version 3.10. September 20, 2013. The study concluded that the attribute combinations in the table is sufficient to distinguish between individuals in 96% of cases involving the entire US population (approx. 320 million)

[2] The threshold of 96% was selected by ANSI/NASPO-IDPV-2013 based on research indicating that it could be readily achieved using combinations of biographic attributes most commonly used in identity-related transactions

[3] Order of presentation shall not be interpreted as a preferred sequence.

		• **Current Address:** (State) • **Current Address:** (City) • **Current Address:** (Street) • **Previous City** • ~~**Full Date of Birth**~~ • **Full SSN:** (All 9 digits) • **Partial SSN:** (First 5 digits) • **Partial SSN:** (Last 4 digits) • **Sex**
3	• **Name:** (Legal First Name and Legal Last Name) • **Partial Current Address:** (Postal Code) or (City and State) • **Partial SSN:** (Last 4 digits)	• **Mother's Name:** (At birth or prior to first marriage) • **Middle Name or Initial** • **Place of Birth:** (Country) • **Place of Birth:** (State) • **Place of Birth:** (City) • **Current Address:** (State) • **Current Address:** (City) • **Current Address:** (Street) • **Previous City** • **Full Date of Birth** • **Full SSN:** (All 9 digits) • **Partial SSN:** (First 5 digits) • ~~**Partial SSN:** (Last 4 digits)~~ • **Sex**
4	• **Name:** (Legal First Name and Legal Last Name) • **Place of Birth:** (City or County) and (State or Foreign Country) • **Partial Date of Birth:** (month and day) or (year)	• **Mother's Name:** (At birth or prior to first marriage) • **Middle Name or Initial** • ~~**Place of Birth:** (Country)~~ • ~~**Place of Birth:** (State)~~ • ~~**Place of Birth:** (City)~~ • **Current Address:** (State) • **Current Address:** (City) • **Current Address:** (Street) • **Previous City** • **Full Date of Birth** • **Full SSN:** (All 9 digits) • **Partial SSN:** (First 5 digits) • **Partial SSN:** (Last 4 digits) • **Sex**
5	• **Name:** (Legal First Name and Legal Last Name) • **Full SSN:** (All 9 digits)	• **Mother's Name:** (At birth or prior to first marriage) • **Middle Name or Initial** • **Place of Birth:** (Country) • **Place of Birth:** (State)

		• **Place of Birth:** (City) • **Current Address:** (State) • **Current Address:** (City) • **Current Address:** (Street) • **Previous City** • **Full Date of Birth** • ~~**Full SSN:** (All 9 digits)~~ • ~~**Partial SSN:** (First 5 digits)~~ • ~~**Partial SSN:** (Last 4 digits)~~ • **Sex**

267