Federal Identity, Credential, and Access Management
Trust Framework Solutions

Authority To Offer Services (ATOS)

For

FICAM TFS Approved Identity Services

Version 1.0
02/07/2014

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

Table of Contents

List of Tables

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 Federal Identity, Credential, and Access Management (FICAM) Adopted Trust Framework Provider (TFP) to meet FICAM Trust Framework Solutions (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 document is intended for:

- **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;
- **TFPs**, 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; and
- **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 (TFP); and
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); and
- E-Government Trust Services Metadata Services (EGTS Metadata Services).

Organizations that define a Trust Framework and certify entities compliant with it are called 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 TMs which provide the authentication functions, IMs which provide the identity proofing and attribute management functions, and 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 identity 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 TFS-adopted TFP; and
- The Applicant continues to maintain an active approval status under a FICAM TFS-adopted TFP.

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

The two requirements listed above are not applicable to certain Identity Service Providers. This exemption exists since these providers are required to comply with existing trust criteria issued by federal government organizations that are considered de facto FICAM TFS adopted TFPs because their trust criteria are considered comparable to the corresponding TFPAP trust criteria.

Currently, these federal government organizations include:

1. The Federal Public Key Policy Authority; and
2. Federal Regulators such as the Office of the Controller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC).

The FICAM TFS Program may consult with federal programs 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 and Profiles; and
- 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-Approved Interfaces

- At Level 2 and above, 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 billing and investigation of administrative, technical, or physical security breaches 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 that fall outside the above parameters, in advance. Data mining, analyses, and behavior 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. Any changes to the annual release plan must be documented and submitted to the FICAM TFS Program in order to determine whether to continue approval of an identity service's offering to the Government. Electronically signed documents are acceptable. This is separate from any recurring submissions to the TFP.

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 (e.g. no other individual has the same set of attributes.)

Table 1 below lists core identity attributes and supplemental matching criteria that are used to support identity resolution. In most cases, the core identity attributes listed below should be sufficient to uniquely identify an individual. In some cases additional supplemental matching criteria may be needed to uniquely identify an individual.

The Applicant, if an IM or a CSP seeking approval at Levels 2, 3 or 4, MUST:

- Identify which of the **verified**[1] (not self-asserted) core identity attributes from Table 1 the applicant is able to provide to RPs
- Identify which of the supplemental matching criteria from Table 1 the applicant is able to provide to RPs
- Have the technical capability to provide, **upon RP request via approved protocols and profiles,** at least one attribute bundle consisting of a set of attributes from Table 1 to enable identity resolution of at least 95% using a FICAM TFS supported standardized approach (See Appendix A)

Core Identity Attributes

- **Name:** (Legal First Name and Legal Last Name)
- **Partial Current Address:** (Postal Code)
- **Partial 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)
- **Partial Place of Birth:** (City)
- **Partial Place of Birth:** (County)
- **Partial Place of Birth:** (State)
- **Partial Place of Birth:** (Country)

Supplemental Matching Criteria

- **Mother's Name**: (At Birth)
- **Mother's Name**: (Prior to first marriage)
- **Middle Name**
- **Middle Initia**l
- **Partial Current Address:** (Street)
- **Partial Past Address**: (Previous City)
- **Partial SSN:** (First 5 digits)
- **Sex**

Table 1: Identity Attributes

The selection of the above identity attributes is based on an industry study on identity resolution. More information on that work and how it may be leveraged by RPs can be found in Appendix A – Standardization of Identity Resolution (INFORMATIVE) of this document.

The FICAM TFS Program, on a case-by-case basis and based on ongoing lessons learned, may revise and update the listing with elements such as domain specific identifiers and additional attributes or may delete existing elements from the list.

[1] Verified means that the relationship of an attribute to an individual has been established. In the case that an attribute is not verified, the attribute must be asserted from an authoritative attribute source. Asking the individual to self-assert that attribute does not constitute verification.

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

- Applicant, if an IM or a CSP, must make all Metadata available to the FICAM TFS Program for use in compliance verification testing. The FICAM TFS Program may share metadata received and the results of analysis on 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

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, the Applicant should contact the FICAM TFS Program prior to initiating the TFP approval process.

4.2 Approval Package Submission

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

- All Identity Services
  - Program Manager Contact Information
  - Technical POC Contact Information
  - Documentation of the process to alert the TFS Program of changes to the Applicant’s service offering that would impact Government relying parties
  - Technical information (Metadata, Endpoints, Test Credentials etc.) that will enable FICAM TFS Program to remotely test and verify Applicant’s conformance to FICAM protocols, profiles and processes
  - 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.
- Identity Services at Level 1
  - Metadata, if available
  - Public listing of available attributes, if any
- Identity Services at Level 2 and Higher
  - Documentation of Change, Incident and Problem Management Process
  - Annual Release Plan

- Metadata (IM or a CSP)
- Public listing of available verified attributes (IM or a CSP)

4.3 Assessment and Testing

At Level 2 and higher, 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. Testing may involve interoperability verification and an annual follow-up to ensure that approved identity services are being offered in accordance with the FICAM TFS approval.

The TFS Program may, as needed, request additional information or documentation 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, including privacy and security, 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 Memorandum of Agreement (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.

Once approved, the Applicant may request a Certification Letter from the FICAM TFS Program Manager (TFS.EAO@gsa.gov) that demonstrates its authorization to offer services to the Federal Government under the FICAM TFS Program.

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. As part of this process, the Applicant may be required to undergo verification testing.

The FICAM TFS Program has sole discretion on granting this approval. 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.[2]

[2] The ability to grant and revoke approval for organizations to offer their identity services to the government is independent of procurement activities between a Federal Government RP and an organization.

Appendix A – Standardization of Identity Resolution (INFORMATIVE)

The core identity attributes in Section 3.2.1 are based on combinations (See Table *2* below) of identity attributes, from an industry study[3], that are **equivalent in resolving** a unique individual in at least 95%[4] of cases. For RPs seeking to fully resolve an identity, **in cases where the set of core identity attribute combinations has failed**, the study recommends starting with a core identity attribute bundle and utilizing the supplemental matching criteria, which shall be selected incrementally until full resolution of identity is reliably achieved. The RP determines if an identity is fully resolved as identity resolution is always from the RP's perspective.

Bundle	**Core Identity Attribute Combinations** (Sufficient to uniquely resolve at least 95% of the U.S. population)	**Supplemental Matching Criteria** (To be added incrementally to the core to reach 100% resolution.)[5]
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** • **Partial Place of Birth:** (Country) • **Partial Place of Birth:** (State) • **Partial Place of Birth:** (City) • ~~**Partial Current Address:** (State)~~ • ~~**Partial Current Address:** (City)~~ • **Partial Current Address:** (Street) • **Partial Past Address**: (Previous City)

[3] This table is the result of a study by the NASPO IDPV Project, *Establishment of Core Identity Attribute Sets & Supplemental Identity Attributes – Report of the IDPV Identity Resolution Project*. January 27, 2014. The study concluded that the core attribute combinations in the table are sufficient to distinguish between individuals in at least 95% of cases involving the US population. These bundle options are independent of Assurance Level requirements.

[4] The threshold of 95% was selected by the study based on research indicating that it could be readily achieved using combinations of biographic attributes most commonly used in identity-related transactions

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

		- **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** - **Partial Place of Birth:** (Country) - **Partial Place of Birth:** (State) - **Partial Place of Birth:** (City) - **Partial Current Address:** (State) - **Partial Current Address:** (City) - **Partial Current Address:** (Street) - **Partial Past Address**: (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** - **Partial Place of Birth:** (Country) - **Partial Place of Birth:** (State) - **Partial Place of Birth:** (City) - **Partial Current Address:** (State) - **Partial Current Address:** (City) - **Partial Current Address:** (Street) - **Partial Past Address**: (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** • ~~**Partial Place of Birth:** (Country)~~ • ~~**Partial Place of Birth:** (State)~~ • ~~**Partial Place of Birth:** (City)~~ • **Partial Current Address:** (State) • **Partial Current Address:** (City) • **Partial Current Address:** (Street) • **Partial Past Address**: (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** • **Partial Place of Birth:** (Country) • **Partial Place of Birth:** (State) • **Partial Place of Birth:** (City) • **Partial Current Address:** (State) • **Partial Current Address:** (City) • **Partial Current Address:** (Street) • **Partial Past Address**: (Previous City) • **Full Date of Birth** • ~~**Full SSN:** (All 9 digits)~~

		• ~~**Partial SSN:** (First 5 digits)~~ • ~~**Partial SSN:** (Last 4 digits)~~ • **Sex**

Table 2: Identity Attribute Bundles

Appendix B – Acronyms

Acronym	**Definition**
ATOS	Authority to Offer Services
CA	Certificate Authority
CSP	Credential Service Provider
EGTS	E-Governance Trust Services
FFIEC	Federal Financial Institutions Examination Council
FICAM	Federal Identity, Credential, and Access Management
IM	Identity Manager
LOA	Level of Assurance
MOA	Memorandum of Agreement
OCC	Comptroller of the Currency
POC	Point of Contact
RP	Relying Party
SEC	Securities and Exchange Commission
TFP	Trust Framework Provider
TFPAP	Trust Framework Provider Adoption Process
TFS	Trust Framework Solutions
TM	Token Manager