Federal Identity, Credential, and Access Management
Trust Framework Solutions

Overview

Version 1.0
02/07/2014

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

Table of Contents

List of Figures

1. BACKGROUND

1.1 Introduction

The Internet is having a profound impact on all our lives, transforming the way we interact on a social, economic, professional and creative level. Most of us regularly conduct online transactions, taking advantage of the convenience and flexibility that online shopping, banking and other services offer. When designed well, online government services are arguably the best way of providing citizens and businesses with a secure, accessible, user friendly, and personalized experience, while driving down costs for government and reducing future public spending commitments.

Transferring government services online means digital channels (e.g. the internet, mobile phones, televisions, etc.) will play an increasingly important role in how citizens and businesses access those services. However, transactions delivered remotely are particularly exposed to security vulnerabilities.

To mitigate the risks associated with online digital transactions involving valuable resources and sensitive personal information, identity is at the core of most government business processes. Once identity is established, all subsequent government online activities, ranging from providing services to granting benefits and status, rely on the accuracy and rightful use of identity.

At the same time, the government is aware of the need to make public services easier for citizens and businesses to access, and that security and privacy are a high priority. As such, it is in the government's best interest to leverage, whenever possible, industry resources that citizens and businesses already utilize.

1.2 Government-wide Policy and National Strategy Implementation

The July 3, 2003 Office of Management and Budget (OMB) policy Memo on "*Streamlining Authentication and Identity Management within the Federal Government*", calls for reducing "... the burden on the public when interacting with government by allowing citizens to use existing credentials to access government services and enabling new services that otherwise could not or would not have been available", as addressed by Section 203 of the E-Government Act (P.L. 104-347) and to comply with the Government Paperwork Elimination Act (P.L. 105-277).

In addition, OMB policy Memorandum M-11-11, issued in February 2011, requires Agencies to align with the Federal Chief Information Officers (CIO) Council's "*Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance*". One of the government-wide governance initiatives under the FICAM Roadmap (*Initiative 2*) is the establishment of a federated identity framework for the U.S. Federal Government.

Other developments have strengthened the push to use trusted third-party credentials via a federated identity framework. The *National Strategy for Trusted Identities in Cyberspace (NSTIC)*, issued in April 2011, calls for the Federal Government to be an early adopter of services under an Identity Ecosystem by *"its own participation in the Identity Ecosystem as both a subject and relying party."* The October 6, 2011 OMB policy Memorandum, *Requirements for Accepting Externally-Issued Identity Credentials*, requires agencies to enable externally-facing applications to accept third-party credentials.

2. OVERVIEW

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. Figure *1* depicts the different elements of the TFS Program.

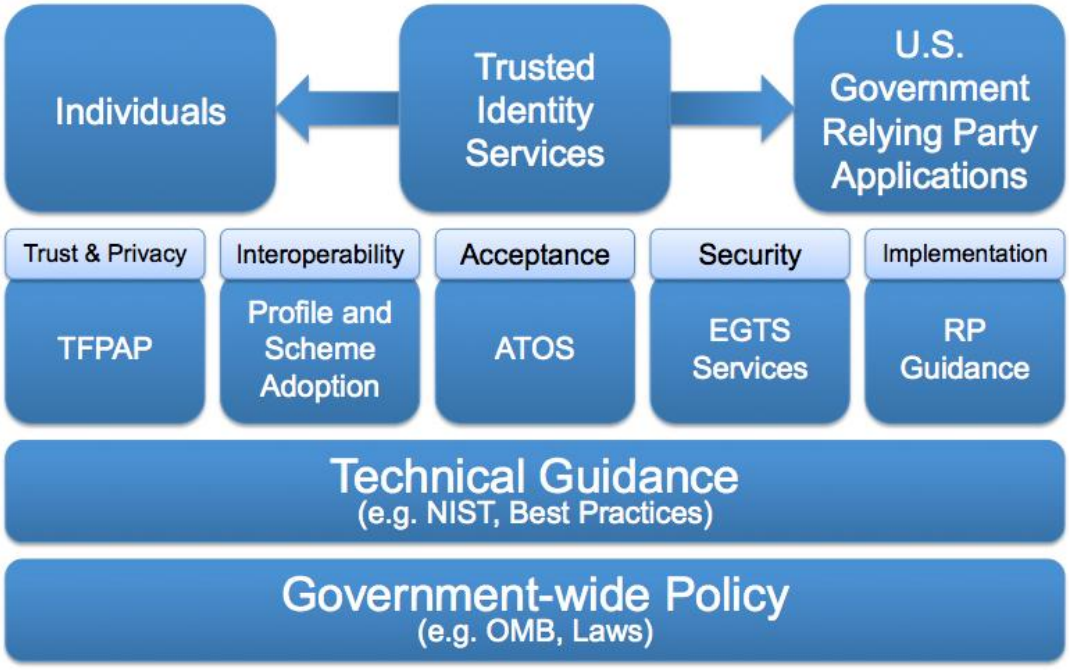

Figure 1: TFS Overview

This document (*Trust Framework Solutions Overview*) provides a holistic overview of the components of the TFS:

- *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-Governance Trust Services Certificate Authority (EGTS CA)
- E-Governance Trust Services Metadata Services (EGTS Metadata Services)

2.1 Terminology

The terms profile, protocol, scheme, and Relying Party are used throughout the Trust Framework Solutions (TFS) documents. In order to establish what each means, we define them as follows:

- **Profile –** Specifies the subset of requirements and functionality within the scheme of a Federal standard, regulation, and/or law that will be used for technical interoperability of government applications, and how they will be used.
- **Protocol –** The technical means by which identity attributes are exchanged. This includes the format and rules for communication between two parties.

- **Scheme –** Precisely scoped subset of an identity management standard.
- **Relying Party** (RP) – The federal agency for which the identity assurance solution is being provided. In some cases federal agencies may contract with external contractors or commercial third parties for certain functions. Such non-federal entities are considered agents of the Federal Government and therefore CSPs must interact with them as if they were interacting with a federal agency application.

2.2 Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance

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

- *The Technical and Operational Specifications 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.

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

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. 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.

2.3 Authority To Offer Services (ATOS) for FICAM TFS Approved Identity 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 the 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), which provide a full service capability that combines authentication, identity proofing and the secure binding of token(s) to identity.

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

Identity services that have been qualified by a FICAM TFS-adopted Trust Framework Provider may optionally apply to the FICAM TFS Program to request approval for the authority to offer their identity services to the Federal Government. Applying to the FICAM TFS Program is optional because some qualified providers may not intend to provide their services to the Federal Government. Directly applying to the Federal Government ensures:

- The establishment of a clear relationship and verifiable points of contact between the parties that will interoperate;
- The fidelity of TFP Trust Frameworks and assessment processes; and
- Ongoing accountability of the identity service through the execution of a detailed Memorandum of Agreement between the parties.

The ATOS will establish a direct relationship between identity service providers and the Federal Government, and will verify technical consistency across the expected range of FICAM TFS-adopted TFPs.

2.4 Identity Scheme and Protocol Profile Adoption Process

In addition to the mechanisms put in place by the TFPAP, the *Identity Scheme and Protocol Profile Adoption Process* enhances the security and privacy at the transaction level through the adoption or creation of FICAM Profiles for use by RPs and CSPs.

The FICAM Profiles do not alter the underlying industry standard upon which it is based, but identify how the specification language is implemented for technical interoperability of government applications.

Proper use of a FICAM Profile assists a CSP and/or a RP by:

- Meeting federal standards, regulations, and laws;
- Minimizing technical risk;
- Maximizing interoperability;
- Ensuring privacy respecting approaches to protocol implementations; and
- Providing users with a consistent context or user experience at a Federal Government site.

Using the *Identity Scheme and Protocol Profile Adoption Process*, the government can assess the efficacy of specific subsets of identity management standards for federal purposes. This helps the RP application and the CSP communicate in a interoperable, secure, and reliable manner.

The FICAM TFS Program may choose to directly create identity schemes and profiles or leverage existing schemes and profiles available in the community after a security and privacy evaluation.

2.5 Relying Party Guidance for Accepting Externally Issued Credentials

The *Relying Party Guidance for Accepting Externally-Issued Credentials* provides agencies with architecture and implementation guidance that addresses existing Identity, Credential, and Access Management (ICAM) objectives and supports the goals for accepting externally-issued credentials.

It provides business and technology owners with specific approaches and direction related to:

- Creating a business case through aligning an organization’s business and technology strategy in order to securely conduct online transactions with individuals outside of the organization;
- Commonly used solution architecture models that can be leveraged to support the acceptance of third-party credentials, based upon clearly defined characteristics of each model;
- Leveraging CSPs approved under the FICAM TFS Program as directed by OMB policy; and

- The recommended processes and technologies to accept third-party credentials while ensuring security, privacy, and liability requirements are upheld when choosing a CSP.

2.6 E-Governance Trust Services Certificate Authority

The Federal Government has been issuing certificates to agencies since September 2004. The latest iteration of this service, the E-Governance Trust Services Certificate Authority (EGTS CA), provides a certificate issuance capability that supports federated identity use cases that require endpoint and message level protections.

In particular it supports the following use cases:

- Providing digital signature and encryption certificate issuance for federation endpoints
  - Agency RP applications
  - Backend Attribute Exchange (BAE) end-points
  - Other end-points that are required to be part of the federal trust fabric
- Facilitating trusted metadata (e.g., signing of metadata by FICAM TFS, TFPs, and federal agency, approved CSPs)

2.7 E-Governance Trust Services Metadata Services

Once the service is implemented and made available, the E-Government Trust Services Metadata Services (EGTS Metadata Services) will provide a trusted mechanism for the collection, aggregation, and display of metadata related to enabling identity federation capabilities.

3. IMPLEMENTATION

3.1 TFS and Government Agencies

The TFS Program supports the Government-wide policy and National Strategy compliance requirements of Executive Branch Federal Government Agencies.

Executive Branch Federal Government Agencies wishing to federate identities for use by other federal agencies and/or state/local governments are not required to apply to the TFS program; however, they are required to follow existing policy, standards, and guidance that govern identity federation.

Non-Executive branch Federal Government Agencies, State, Local, Tribal Government Agencies, or other government entities that have questions regarding the use of any aspect of the TFS Program are encouraged to contact the FICAM TFS Program Manager (TFS.EAO@gsa.gov)

3.2 TFS and Financial Institutions

Federal law, including the Bank Secrecy Act and the USA PATRIOT Act, imposes a duty on financial institutions to "know their customers" and report suspicious transactions to help prevent money laundering and terrorist financing. Many financial institutions are regulated by Federal agencies such as the Office of the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchanges Commission (SEC). These regulators normally require the institutions to implement a Customer Identification Program[2].

[2] From NIST SP 800-63-2, Section 5.3.2.

The federal regulator is a de facto FICAM TFS approved TFP because its trust criteria in implementing a Customer Identification Program are considered comparable to the corresponding TFPAP trust criteria.

The following provisions apply to federally regulated financial institutions, brokerages, and dealers subject to such federal regulation, that implement such a Customer Identification Program:

- Level 2 Comparability - Such institutions may issue credentials to their customers via the mechanisms normally used for online banking or brokerage credentials. By using such online banking or brokerage credentials and tokens in combination with protections and processes required by the FFIEC's Guidance on *Authentication in an Internet Banking Environment*, the FICAM TFS Program recognizes the ability of such an institution, when acting as a CSP, to assert the identity of their customer to a level comparable to OMB M-04-04 Level 2.
- Level 3 Comparability - Depending on the strength of an institution's credentialing solution, some institutions may also qualify to have its solution recognized as being comparable to OMB M-04-04 Level 3. Interested institutions are encouraged to contact the FICAM TFS Program Manager (TFS.EAO@gsa.gov) in order to determine their qualifications.

In all cases, the following apply:

- Financial institutions that seek to offer their services as CSPs or TMs to the Federal Government are exempted from the FICAM TFS-adopted TFP approval requirement;
- Financial institutions that seek to offer their services as CSPs or TMs to the Federal Government are required to follow the procedures in the *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* document to be directly approved by the FICAM TFS Program. In this circumstance, such approval by the FICAM TFS Program may include an assessment against the FICAM TFS Privacy Trust Criteria; and
- The FICAM TFS Program may consult with federal agencies that have regulatory responsibility for the Applicant regarding input into the approval process.

3.3 TFS and the FICAM Testing Program

The FICAM Testing Program provides a comprehensive evaluation capability to support the selection and procurement of qualified on-premise products and services for the implementation of a federated and interoperable ICAM segment architecture. As part of the FICAM Testing Program, the General Services Administration (GSA) manages the Approved Products List (APL). This list provides federal agencies with the products and services related to ICAM implementation that have been approved based on testing done by the FICAM Testing Program.

Federal security controls[3] require federal agencies to employ only FICAM-approved information system components to accept third-party credentials. Therefore, on-premise vendor products that implement FICAM TFS Approved Identity Schemes and Protocol Profiles must be tested and approved by the FICAM Testing Program. Approved products are listed on the GSA APL so that federal agencies can use the GSA Schedules to purchase them.

[3] From NIST SP 800-53 Revision 4, control enhancement IA-8(3).

4. SYNOPSIS OF CHANGES AND UPDATES

The following list provides an overview of the changes that have been implemented in the TFS suite of documents released in the first quarter of 2014:

- Clarification of the approval decision authority of the FICAM TFS Program
- Implementation of a fast-track program for financial institutions to become approved CSPs or Token Managers;
- Establishment of interoperability verification and annual follow-up of identity services for FICAM TFS approval;
- Incorporated requirement to implement and utilize the tested and approved interface by the identity service when offering services to Government RPs using the "FICAM TFS Approved" designation;
- Streamlined of LOA 1 trust criteria ;
- Support for component identity services;
- Updated security trust criteria to incorporate NIST SP-800-63-2
- Direct incorporation of Privacy as a trust criteria for FICAM TFS Approval;
- Ongoing Verification as an OPTIONAL trust criteria has been introduced;
- Incorporated flexibility in adopting industry developed protocol profiles, provided it meets Government needs for security, privacy and interoperability
- Standardization of assurance level URIs to be used in protocol profiles
- Establishment of identity resolution attribute requirements for FICAM TFS CSP and IM approval at Level 2 and higher; and
- An ongoing relationship has been established with the FICAM Testing Program to verify FICAM Protocol Profile Support in on-premise vendor products.

APPENDIX A – ACRONYMS

Acronym	Definition
APL	Approved Products List
ATOS	Authority to Offer Services
BAE	Backend Attribute Exchange
CA	Certificate Authority
CIO	Chief Information Officers
CSP	Credential Service Provider
EGTS	E-Governance Trust Services
FFIEC	Federal Financial Institutions Examination Council
FICAM	Federal Identity, Credential, and Access Management
GSA	General Services Administration
ICAM	Identity, Credential, and Access Management
IM	Identity Manager
LOA	Level of Assurance
NSTIC	National Strategy for Trusted Identities in Cyberspace
OCC	Comptroller of the Currency
OMB	Office of Management and Budget
RP	Relying Party
SEC	Securities and Exchange Commission
TFPAP	Trust Framework Provider Adoption Process
TFS	Trust Framework Solutions
TM	Token Manager