Federal Identity, Credential, and Access Management Trust Framework Solutions

Overview

Version 1.0.0
DRAFT: 11/11/13

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

Table of Contents

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 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 *"offering services online as a relying party,"* and using *"(identity and attribute) services provided by others."*. 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 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.

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-Government Trust Services Certificate Authority (EGTS CA)
- E-Government Trust Services Metadata Services (EGTS Metadata Services)

2.1 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 that have been developed:*
  - to define requirements for the proper operation of the identity system (i.e., so that it works),
  - to define the roles and operational responsibilities of participants, and
  - to 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 Trust Framework Provider Adoption Process (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 Levels of Assurance. Trust Frameworks that are comparable to federal standards are *adopted* through this process, allowing federal Relying Parties (RPs) to trust credential services that have been assessed under the trust framework.

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

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

acquisition and contracting processes, or by the acquisition and contracting processes of Shared Service Provider(s) acting on behalf of an Agency.

2.2 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) 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 Adopted TFP 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.

2.3 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* assists in enhancing the security and privacy at the transaction level through creating 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.

2.4 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 Credential Service Providers (CSP) approved under the FICAM Trust Framework Solutions Initiative 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.

2.5 E-Government Trust Services Certificate Authority

The E-Government 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 relying party 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, Trust Framework Providers, and Federal Agencies, Approved CSPs)

2.6 E-Government Trust Services Metadata Services

The E-Government Trust Services Metadata Services (EGTS Metadata Services) provides a trusted mechanism for the collection, aggregation and display of metadata related to enabling identity federation capabilities.

3. IMPLEMENTATION

3.1 Trust Framework Solutions and Government Agencies

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

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 Trust Framework Solutions Program are encouraged to contact the FICAM TFS Program Manager (TFS.EAO@gsa.gov)

3.2 Trust Framework Solutions 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]

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

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

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 e-authentication 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 to the Federal Government, are exempted from the FICAM TFS adopted Trust Framework Provider approval requirement.
- Financial institutions, that seek to offer their services as CSPs 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.
- The FICAM TFS Program may consult with federal agencies that have regulatory responsibility for the Applicant regarding input into the approval process.

3.3 Trust Framework Solutions and the FICAM Testing Program

The FICAM Testing Program provides a comprehensive evaluation capability to support the selection and procurement of qualified products and services for the implementation of a federated and interoperable ICAM segment architecture. As part of the FICAM Testing Program, 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.

Products that implement TFS Approved Identity Schemes and Protocol Profiles are eligible to be tested via the FICAM Testing Program. If approved, they will be available on the GSA Approved Products List so that Agencies can use the GSA Schedules to purchase them.