Trust Framework

Certification Process

Trust Framework Solutions Program

Version 0.2

Nov 17, 2017

Table of Contents

[1. Introduction 4](#_Toc498692271)

[1.1. Audience 4](#_Toc498692272)

[1.2. Scope 4](#_Toc498692273)

[1.3. Objectives 4](#_Toc498692274)

[1.4. Exemptions 5](#_Toc498692275)

[2. Roles and Responsibilities 5](#_Toc498692276)

[2.1. Trust Framework Solutions Program 6](#_Toc498692277)

[2.2. U.S. Federal Agencies 6](#_Toc498692278)

[2.3. Trust Frameworks 7](#_Toc498692279)

[2.4. Credential Service Providers 8](#_Toc498692280)

[3. Independent Third Party Auditor 8](#_Toc498692281)

[4. Certification Process 9](#_Toc498692282)

[4.1. Phase 1: Pre-requisite Self-Assessment 10](#_Toc498692283)

[4.2. Phase 2: Audit Letter Review 10](#_Toc498692284)

[4.3. Phase 3: Business Case & Sponsor Presentation 11](#_Toc498692285)

[4.4. Phase 4: Certification Package Submission 11](#_Toc498692286)

[4.4.1. Trust Framework Application 12](#_Toc498692287)

[4.4.2. Trust Framework Charter 12](#_Toc498692288)

[4.4.3. Credential Service Provider Assessment Methodology 12](#_Toc498692289)

[4.4.4. Policy Mapping Analysis 13](#_Toc498692290)

[4.4.5. Phase 5: Certification Package Assessment 13](#_Toc498692291)

[4.4.6. Phase 6: Technical Review and Testing 14](#_Toc498692292)

[4.4.7. Phase 7: Certification 14](#_Toc498692293)

[5. Annual Certification Renewal 15](#_Toc498692294)

[6. Authorization to Operate 16](#_Toc498692295)

[7. Audits and Authorizations to Operate 16](#_Toc498692296)

[Appendix A - Certification Prerequisite Checklist 18](#_Toc498692297)

[Appendix B – Trust Framework Certification Application 20](#_Toc498692298)

**Revision History Table**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
|  | 0.1.0 | Distribute to Internal Government Review | GSA OGP |
|  | 0.2.0 | Updated from Internal Government Review Comments | GSA OGP |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 

# Introduction

The GSA Trust Framework Solution (TFS) Program enables identity federation for the Federal Government by leveraging Trust Frameworks that provide secure, privacy enhancing and cost controlled identity assurance and authentication assurance services.

CW: Do agencies always want Identity Federation? I don’t think so. Do TFO’s only offer federated TFs? No. It seems that there is pre-set notion that identity federation is the thing that agencies require and the thing that TFS offers, which is not substantiated by the operational reality to date.

# Audience

This document is for:

* Trust Frameworks (commercial) who would like to establish a relationship with the Federal Government; CW: KI is a non profit, so is it out of scope for this?
* Auditors who are analyzing the Trust Frameworks and their Credential Service Providers (Providers); and
* Federal agencies who would like to understand how Trust Frameworks are certified.

# Scope

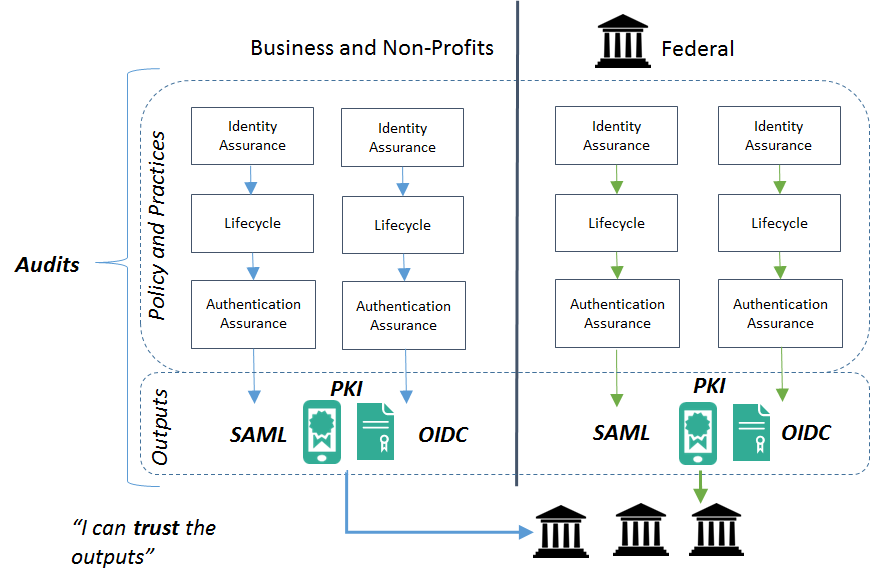
This document outlines the Policies, Practices and Audits for Trust Frameworks and their respective members.

# Objectives

A Trust Framework enables an ecosystem or marketplace to be interoperable, secure, and allows users to share reliable identity information. The objective is to provide a starting point [CW: A TF is more than a starting point, as an objective, so this statement is not correct, unless it means the objective of this document?] from which a Community of Interest (COI) can organize participation from their constituency to customize and implement the business, legal, technical, privacy, certification, and audit components of their Trust Framework specification. The Program achieves this objective by certifying Trust Frameworks that demonstrating comparability to Federal Government policies, legal/business procedures, security, and interoperability standards.

This certification provides accountability to the Frameworks and Credential Providers.[CW: provides accountability to Federal agencies, by the Frameworks and CPs?? Something not quite flowing with the to/from/by actors in this sentence.] The Frameworks and Providers must demonstrate that they arrange for accurate auditing and interoperability testing. The auditing and testing allows the Federal Government to trust credentials issued by Providers in the Trust Framework’s ecosystem.

Below illustrates the processes and services the government requires, displays the role of audits, and lists the outputs.[CW: This is a very high level view that does offer meaningful information to a reader]



# Exemptions

Government to government agreements may be managed through existing laws and regulations covered by trade, defense, standards development arrangements, or other. Governments pursuing a trusted relationship may contact the Program directly, instead of being certified through a commercial/non-profit Trust Framework to help determine the appropriate policy and legal arrangements pursuant to U.S. public law.

# Roles and Responsibilities

A Trust Framework establishes the set of rules and policies that govern how their trusted identity federation [CW: There is no binary connection between a federation and a TF. It can do, but does not have to incorporate federation, and Kantara and some other TFs in TFS do not for the most part. There is no reference to a definition or standard to determine the authoritative basis for this statement]. members will operate and interact. These rules and policies include how to:

* Conduct identity management responsibilities;
* Protect and securing identity information;
* Perform operational and administrative roles within the federation; and
* Manage liability and legal issues.

[CW: Kantara does all these but not in the way that this document states them. The authors of this document have a fixed notion in mind of a TF which does not reflect the operational reality on the ground in the majority of TFOs].

Trust Frameworks establish multilateral agreements among all identity federation members enabling the trust and governance of a federation’s operations.

[CW: This statement is only correct if there is a federation structure. Otherwise, the agreements are not multilateral, rather a string/series of unilateral agreements. It is given as a statement of fact which is not supported by the operation of many TFs in TFS today.

It is absolutely critical that the authors and the TFOs engage to determine what sits behind these statements. It is not clear if it is s genuine misunderstanding of how at least 2, if not more, of the TFs on the TFS program operate today, or whether it is a ‘future state’ statement. We cannot go on in this process if there is no clear and accurate understanding of the current operating practice].

# Trust Framework Solutions Program

There are many Trust Frameworks throughout the identity assurance and credential landscape. The Program is establishing parameters to centralize the certification of Trust Frameworks that meet federal standards. [CW: It has to be assumed only in the Federal context. GSA has no business centralizing the certification of Trust Frameworks outside of its remit].

Federal agencies and missions in need of trusted credential services are the primary customer of the Trust Framework Solutions. The Program designed the processes outlined for certification and auditing to remove burden from agencies who are required to ensure systems and services comply with federal guidelines. The Program will assemble a committee of federal agency representatives (federal employees) who use one or more Trust Frameworks to accept trusted credential service providers. The committee members are primary stakeholders and beneficiaries of the Program and will provide input into the decision-making, acceptance, and maintenance of Frameworks. The Program has final decision-making responsibility about certifying Trust Frameworks.

When the Program enters into an agreement with and certifies a Trust Framework, it does so for the benefit of the Federal Government’s mission and delivery of mission services. The Program may issue or revoke agreements at its discretion.

[CW: Please note that the GSA has an TFP MOA in force with Kantara signed on August 31st 2010 between Judith Spencer, Joni Brennan and Matthew Gardiner. Please confirm that none of this draft text and request form comments constitutes a a re-negotiation of that instrument. If it were to be, then the terms and timeframes around changing that Agreement need to followed, not the proposed terms and timeframes shown below]

# U.S. Federal Agencies

U.S. federal agencies recognize the value of Trust Frameworks and their Providers as an economic and privacy enhancing benefit. Part of their mission might include building or managing Credential Service Providers, and/or identity federation services to enable cross-government federation for users across many communities of interest [CW: This indicates that the Government is going to lock out the private sector in the provision of services for some sections of its own market. While in theory there is nothing to prevent such a strategy, the message it sends to private sector providers, on top of the other messages conveyed in this draftdoc, is one that removes confidence in the marketplace working on equal terms and for a sustained period]. All users in the communities of interest may:

* not have access to a federated trusted identity option, or
* be affiliated with an organization that has chosen not to participate in a trust framework, or
* choose to opt out (personal choice) of using a third-party option and require a government provided option, or
* represent a population not having solutions or choices available meeting their cost, legal, or demographic (geographic or other) constraints.

Agencies who offer these services, [CW: is this supposed to be a references to DoJ NIEF GTRI?] trusted by entities outside the government, are joining the trusted identity ecosystem [CW: is this supposed to be a reference to IDESG?] and must adhere to the process for Credential Service Providers [CW: ..which, given the absence of any references to authoritative sources, is being hand curated in this doc]. These processes include publicly posting information and performing annual third-party audits. [CW: Many existing standards do that but are not mentioned here e.g. RFC 3647 nternet X.509 Public Key Infrastructure, ertificate Policy and Certification Practices Framework]. Agencies do not have to establish agreements with an independent Trust Framework. They are considered a member of the U.S. Government’s trust governance framework. [CW: What is a governance TF vs a TF?] [CW: The implication in this sentence is that independent TFs are the ‘the option of last resort’, and that the Agencies potentially operate by a different set of rules. Else why call out these requirements in this section and not refer Agencies to the mainstream set of rules being curated in this doc].

# Trust Frameworks

Trust Frameworks [CW: can, or may not] facilitate identity federation between organizations within a COI. They do not perform identity verification, manage credentials, or manage and operate the provider services directly. Instead they establish digital trust relationships across a COI based on legal, policy, and technical requirements to which members of the community agree. Trust Frameworks establish trust by assessing Providers against their established standards for the community they serve. Frameworks ensure that Providers adhere to those agreements and standards. Providers are considered members of the Trust Framework.

In order to establish a relationship with the government, Trust Frameworks shall assess Providers against their established standard in the following categories: [CW: It is concerning that this chart does not reference any existing standard that already essentially does these things.. ISO 17025, ISO 17065, RFC3647, and more. The only ones referenced in item 4 are not truly ‘like for like’ in any event].

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Category** | **Type** | **Questions Addressed** |
| 1 | Publication of Practices | Policy | Providers must make all Credential/Certificate Policies and Credential/Certificate Policy Statements available on public websites |
| 2 | Identification and Authentication Processes | Technical | How well does the Provider register and proof the identity of the credential applicant, and issue the credential to the approved applicant?  What is the Provider’s authenticator technology and how well does the technology intrinsically resist fraud, tampering, hacking, and other such attacks? |
| 3 | Lifecycle Operations | Technical | How well does the Provider manage and protect authenticators and credentials over their full life cycle?  What compensating controls does the Provider implement that provides an ongoing identity verification capability?  How well does the privacy policies of the Provider adhere to the Fair Information Practice Principles? |
| 4 | Facilities, Management, and Operational Controls | Technical | Is the provider’s service implementing and monitoring 800-53 (or equivalent ISO 27001) security controls for moderate and high systems, based on the use of the system? [CW: 27001 is Requirements. Is perhaps 27002 Controls meant to be referenced? These two referenced above are not equivalent in any event, but it is appreciated that 27002 is not a management standard]. |
| 5 | Technical Security Controls | Technical | Is the provider’s service implementing and monitoring 800-53 (or equivalent ISO 27001) security controls for moderate and high systems, based on the use of the system? [CW: Ditto above]. |
| 6 | Profiles | Technical | What federation assurance profiles does the provider implement? [CW: Unclear exactly what this means as it could be interpreted in a number of ways. Could examples be offered?]. |
| 7 | Compliance audits | Policy | What are the audit procedures and plans that the provider adheres to? Are audits independent, to an established standard, and posted for any public review? |
| 8 | Other Business and Legal Matters | Legal | Which laws and legal framework does the provider operate within? Does the provider have legal protections and recourses available to users and federal systems that are commensurate with U.S. government requirements? |

# Credential Service Providers

Credential Service Providers (Providers) ensure identity assurance, issue, and maintain the authenticators individuals use to access online services. Providers operate and maintain appropriate services by conforming to requirements set by the COI. This includes:

* Patching and continuous monitoring;
* Updating the policies, standards, procedures, and processes; and
* Ensure audits have been conducted for the entirety of the Provider's’ system, resolving all issues identified, and submitting annual audit reports to the Trust Framework.

# Independent Third Party Auditor

To be certified by the Federal Government, Trust Frameworks and member Providers are required to pass an independent third-party audit.

The Program does not specify which audit methodology to use, however, the Trust Framework and the Provider’s policy must submit the methodology {CW: Clarify by giving an exmple]. The Program will review the methodology for comparability and acceptance during the annual renewal process.

In order to be qualified, an auditor must:

* Perform audits as a regular ongoing business activity;
* Demonstrate competence in the field of identity assurance, cryptography, credentialing and compliance audits – there must be a history of performing compliance audits that span several years;
* Be thoroughly familiar with the requirements of the Federal policy and practice statements associated with the systems and services being provided;
* Be a Certified Information System Auditors (CISA) and IT security specialist – or equivalent; and
* Provide attestations of independence from the audited organization.

Auditors need to ensure both the Trust Framework and the Providers operating within the Trust Framework comply to the following:

* Have a practice statement implementing the requirements of the Trust Framework’s Policy;
* Maintain operations adhering to their practice statements;
* For Providers, provide artifacts of each identity assurance and authenticator type to the Trust Framework to be tested for interoperability and security during the 12-month audit period, and ensure all issues identified during testing were resolved;
* Comply with all provisions and obligations detailed in the Memorandum of Agreement established with the Program and the Trust Framework;
* Have an agreement, such as a Registration Authority Agreement (RAA), executed between the Provider and any third-party organization performing delegated services;
* Remediate any previous annual audit opinion and findings.

If services receive separate audits by different auditors or group of auditors, then the Annual Review package must include these separate audit opinion letters.

# Certification Process

[CW: Given the significant overlap with ISO 17000 series Certification Body standards suite, why does the GSA need to create a duplicate process that adds expense and effort for all stakeholders? At least baseline on it and add additional requirements as a profile or overlay. Why start from scratch with no reference to any certification standard?].

An application submission is necessary for the Program to ensure each Trust Framework meets government standards and mission needs. The Program will review the application to ensure the Trust Framework will provide a demonstrable benefit to the government and enforces standards and practices consistent with NIST Special Publications and appropriate Policy. The subsequent sections detail the seven phases of the certification process:

* Phase 1: Pre-requisite Self-Assessment
* Phase 2: Auditor Letter Review
* Phase 3: Business Case and Sponsor Presentation
* Phase 4: Certification Package Submission
* Phase 5: Certification Package Assessment
* Phase 6: Technical Review & Testing
* Phase 7: Certification

The Program may deny a Trust Framework at any point during the process. [CW: This is yet another indicator that serves to make the CSP lose confidence in the market because it cannot manage the risk]. Reasons for denial include:

* Insufficient benefit to the Federal Government in entering into an identity federation agreement with the Trust Framework and their member Providers, or
* Risks or concerns identified by certifying the Trust Framework, or
* The Trust Framework’s policies, standards, processes, and procedures are not comparable to those of the Federal Government.

# Phase 1: Pre-requisite Self-Assessment

A Trust Framework pursuing certification from the Trust Framework Solutions Program begins with a self-assessment of their adherence to the prerequisites. The self-assessment requires the Trust Framework to have a federal sponsor. The federal sponsor is a federal agency representative seeking to accept one or more of the Trust Framework’s member Provider’s credentials for identity federation. The last component of the self-assessment includes evidence of an audit conducted on the Trust Framework and their member Providers.

[CW: This is a significant ‘pre-sale’ effort that its hard to imagine either side being motivated to do. What this implies is that the TF has costed a business case with the Agency in advance with requisite target revenues, but with no contract to instantiate it because Agencies are unable to undertake contracts outside of the process].

Appendix A of this document lists the self-assessment requirements in full.

# Phase 2: Audit Letter Review

A Trust Framework wanting to be certified by the Program must demonstrate an audit by an independent third party for certification.

The auditor must:

* Demonstrate competence in the field of compliance audits,
* Be thoroughly familiar with identity federation, protocols, credential practice statements, and credential policies, [CW: Why? The TF does not do this. The CSP does, as this doc states further up]
* Perform compliance audits as a regular ongoing business activity
* Be a certified information system auditor (CISA) or IT security specialist, and an identity credential subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.
* Be from a private firm that is independent from the entities being audited or be organizationally separated from those entities to provide an unbiased, independent evaluation.

The audits must demonstrate:

* The Trust Framework practices statement adequately addresses all of the requirements of their Policy;
* The Trust Framework operations and management correctly implements the practice statement; and
* The Trust Framework has at least two operational Providers operating in compliance with the Trust Framework’s policies, with no conflicts of interest.

The Program will review the audit letters and inform the Trust Framework whether or not they may proceed to Phase 3 of the Certification Process.

[CW: While the intent is accepted and understood, the additional cost of compliance in relation to the price point of the authenticated credential at LoA1 – LoA3 non PKI, is likely to disincentivise CSPs from further engagement].

# Phase 3: Business Case & Sponsor Presentation

The Trust Framework, with its Federal sponsor, must formally present their business case to the Program. The business case must address:

* A Use Case including agency mission services that will be accepting identities and credentials issued by the Trust Framework’s member Providers;
* A business case for why any existing certified Trust Frameworks and their member providers do not meet the sponsor’s requirements;[CW: Arriving at this point in the doc, it seems to imply that the system is for new Trust Frameworks, and not existing ones. Is that correct? If so, that clarification should be made explicit in the scope at the top of the document].
* Benefits the Trust Framework and their member Providers give to the federal agency sponsor;
* A financial disclosure to demonstrate sustainability of the Trust Framework, and how organizational and financial conflicts of interest have been managed, avoided, or de-conflicted. [CW: Much more detail needed here.. is it historic? Is it based on a forecast of future sustainability? Some aspects feel incredibly invasive and outside of the GSA’s mandate to request].

The Program requires federal sponsorship to demonstrate the benefit to the government (specifically the sponsoring agency) to certify the Trust Framework. The Trust Framework must have a Federal sponsor demonstrating the value from federating with the community of interest that Trust Framework supports. The Federal sponsor shall state its intention to trust and accept the credentials of the Providers represented by the Trust Framework and there is a benefit to cross-government missions to enter into the agreements. Based on the business case, and in collaboration with the federal sponsor, the Program will determine if the Trust Framework should proceed to Phase 3 and submit the Certification Application and supporting artifacts. If the Program declines the business case, it will provide reasons and additional guidance. Any Trust Framework may only submit an application or renewal package twice within a single twelve (12) month period.

[CW: Again, on the face of it, the cost of compliance will outweigh the benefit of the revenue, and rule the service unviable].

[CW:Furthermore, the sponsorship process to open to abuse. Agencies could horse-trade all manner of accommodations to pit TFs against each other, such is the imbalance of power].

# Phase 4: Certification Package Submission

Once the Program approves the sponsorship, the Trust Framework may submit their Certification Package. The Certification Package includes:

* Trust Framework Certification Application;
* Trust Framework Charter;
* Provider Assessment Methodology;
* Policy Mapping Analysis; and
* Audit letters.

# Trust Framework Application

The application is Appendix B. The information must include:

* **Organization Information:** The Trust Framework’s name, address, and points of contact;
* **Levels of Assurance:** A designation of the various assurance levels at which the Trust Framework is seeking to be certified, including the Identity Assurance Levels, Authenticator Assurance Levels, and Federation Assurance Levels;
* **Information on the Trust Framework model:** A description of the Trust Framework’s existing trust relationships, including any architecture diagrams; [CW: Clarify please]
* **Trust Framework Community of Interest Overview:** A description of the COI the Trust Framework currently services; [CW: It does not always serve a COI, and again is arguably beyond GSA’s mandate for an independent TF].
* **Federal Sponsor and Use Case:** The contact information for the Trust Framework’s Federal Sponsor and details of the application that will be leveraging identity credentials issued from the Trust Framework’s Providers;
* **Knowledge, Skills, and Abilities:** A description of the Trust Framework’s management and operational abilities, including resumes, roles, and the amount of relevant experience of staff; and
* **Signature:** Digital signatures of the senior official (an officer or executive) of the Trust Framework and the Trust Framework’s Federal Sponsor.

The Program will only consider applications that are submitted with responses to all sections and that are accompanied with all required documentation.

[CW: The rigid structure means that there is too effort that risks being wasted, before an indication of success is know. A further disincentive for TFs to engage].

# Trust Framework Charter

The Trust Framework must provide a Charter, detailing the following items:

* Background Information;
* Mission and Purpose;
* Membership Roles, Functions, and Duties;
* Rules of Engagement; and
* Conflict Resolution Processes and Procedures.

# Credential Service Provider Assessment Methodology

The Trust Framework must detail the requirements that Providers must meet to become a member of the Trust Framework and the methodology used to assess these Providers as to their compliance with those requirements. The methodology must consist of documented processes and required artifacts, which shall include at a minimum:

* Governance model;
* Annual auditing process and requirements with which Providers must comply; and
* Procedures used to test that Providers are complying with policies, practices, standards, federation, and security requirements.

# Policy Mapping Analysis

Trust Frameworks must map their policies, standards, procedures, and processes to the Federal Government’s requirements. The policies and standards include:

1. NIST SP 800-53 security controls; and
2. NIST SP 800-63 for identity assurance, authenticator assurance, federation assurance, and privacy protections;.

Frameworks shall publish all policies, including credential policies, and ensure they are publicly accessible and posted on a website at all times, in an open and transparent model. The Trust Framework shall submit its mapping for review by the Program.

# Phase 5: Certification Package Assessment

An evaluation committee will assess the Trust Framework’s Certification Package. The committee will be comprised of:

* Members of the Trust Service Program;
* Federal agency program managers of applications utilizing credentials provided by approved Providers; and
* Federal agency representatives appointed by the Federal CIO Council.

The committee may meet with the Trust Framework during the assessment process to ask questions or obtain clarifications. After reviewing the information provided, the committee will make a final determination and provide a Summary Report indicating:

1. The extent of the Trust Framework’s comparability to the Program’s requirements for each category listed in Appendix A; and
2. Sufficient review of the Trust Framework’s member Providers, their auditing, and re-certification processes.

After completing the assessment, the Program will provide a Summary Report to the Trust Framework notifying them whether or not they can proceed to the next phase. If the Program rejects the Certification Application, it will provide the reason(s) for rejection.

# Phase 6: Technical Review and Testing

The Program will review the Trust Framework’s test plan and regular procedures. Federation testing will be conducted between the Provider’s credentials and the sponsor’s application. The Trust Framework shall submit a test plan including how initial and annual testing is conducted for each provider in their community pursuing approval by the Program.. [CW: It could be argued that this conflicts with the TF scope laid out in Section 2.3].

Technical federation testing shall demonstrate:

* Conformant credentials can be successfully generated and exchanged using one or more federation assertion protocols (examples: security assertion markup language, Open ID Connect, etc.);
* All Provider service endpoints are properly secured through transport and message layer protections applicable to the federation technology and identity scheme;
* All Provider production services are internet accessible and maintain the agreed upon service level agreement specified in the Trust Framework’s policies for their COI; and
* If applicable, the directories, protocols, and attribute schemes of the Federal Government and the Trust Framework’s member Providers are interoperable.

The Trust Framework is responsible for any costs related to establishing a testing capability. The Trust Framework shall maintain the testing capability and provide an environment for testing Trust Framework and Provider changes, including new functionality, patches, and new Providers.

# Phase 7: Certification

Once the Program has completed its review of the application, supporting artifacts, test plan and results, the program will decide if it will accept the Trust Framework. The Program will send the Trust Framework representative a written notification letter regarding its certification. The Program will strive to provide feedback within 30 days. If the Program cannot provide a response within 30 days, it will communicate with the applicant Trust Framework and establish an agreeable response timeline. [CW: Check the timeframes against current MOA]

If feedback is given by the Program to the applying Trust Framework and remediation is needed for legal, technical, security, or other reasons, then that Framework may only re-apply one more time during a twelve month period after resolving all items identified.

The relationship between the Federal Government and a Trust Framework shall be governed by the Memorandum of Agreement signed by a senior official authorized to enter into agreements on behalf of the Trust Framework and by the Trust Framework Solutions Program Manager. The Program will provide a tailored Memorandum of Agreement template as a starting point for discussions. The Memorandum of Agreement shall be signed only after all issues have been resolved to the satisfaction of both parties.

# Annual Certification Renewal

Every year, a Trust Framework must renew their certification with the Program. The certification renewal package is a subset of artifacts included in the initial certification package. The Trust Framework is responsible for providing all artifacts, including the member Provider artifacts.

The required items for the Trust Framework are:

* An audit letter for the Trust Framework, including the date the audit was completed, with the auditor's name and associated organization;
* An updated Provider Assessment Methodology (if changes have been made);
* An updated Policy Mapping Analysis (if changes have been made); and
* An updated Trust Framework Certification Application.

For each Trust Framework member Provider approved to interoperate with the U.S. Government, the Trust Framework shall provide:

* Audit Letters for the Providers that are members of the Trust Framework;
* The designated Identity Assurance Level(s), Authenticator Assurance Level(s), and Federation Assurance Level(s) at which the Provider was successfully assessed;
* A detailed description(s) of how the Provider met the Trust Framework’s policies and procedures;
* A confirmation from the Trust Framework’s Federal Sponsor stating that the sponsorship will continue for the next 12 months;
* A detailed description of the identity assurance processes, including the types of data sources used;
* A description of the types of authenticators supported;
* A notice to the trust community with the publicly accessible information required to be maintained for review by any individual or entity;
* Authorization to Operate letters;
* Confirmation of Testing; and
* Sample testing artifacts from production environments including, federation metadata and / or discovery artifacts.

# Authorization to Operate

There are two models for trusted identity federations and credential service providers:

Scenario A: Organization A has affiliated users, and government agencies only accept the service for access to government systems. This is the traditional and typical identity federation.

In Scenario A, the government and mission applications are accepting an existing identity and authenticator assertion based on an arrangement that already exists between the person, the Trust Framework and the Providers. For example:

* I am John Adams, a doctor affiliated with the Hospitals of Great Medicine
* I am Jane Adams, a researcher affiliated with the University of Top Notch Education

Scenario B: Organization B has a commercial or non-profit service, and government agencies *requires or directs* users to use the service.

In Scenario B, the government and mission applications are procuring or directing individuals to use the Provider’s service and provide personally identifiable information to the service for the purposes of identity assurance procedures. As a federally-contracted service, the Provider is required to obtain and maintain a FISMA Authorization to Operate at the appropriate moderate or high security control baseline. The Program will collaborate with the Providers to help determine the appropriate path for attaining the FISMA Authorization to Operate (ATO) including leveraging FedRamp or other cross-government services.

[CW: It seems that Kantara’s TF falls into Scenario B by virtue of the fact that the CSPs we approve, follow this pattern. Scenario A looks like GTRI NIEF DoJ). A range of use cases may fall in between].

# Audits and Authorizations to Operate

An ATO demonstrates the system meets government security standards. This regulation requires continuous monitoring of security vulnerabilities, patching, system security plans, and penetration testing.

Audits look at the credential provider, and trust framework (each gets its own audit) to affirm the actions required under the certificate policies, mappings, avoidance of conflicts of interest and management of the provider by the framework are addressed.

Federal agencies require that both processes. The technical requirements demonstrates security and the business requirements demonstrates that the system is suitable.

# Appendix A - Certification Prerequisite Checklist

A Trust Framework seeking certification with the Trust Framework Solutions Program must meet the criteria listed below for their application to be considered:

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| Demonstrate why it is beneficial for the Federal Government to certify the Trust Framework. The Trust Framework must have a Federal sponsor that will benefit from federating with the Community of Interest the Trust Framework supports. The Federal sponsor must state its intention to trust and accept the credentials of the Providers represented by the Trust Framework and that there is a benefit to cross-government missions to enter into the agreements. |  |
| Demonstrate that the Trust Framework is operational and has at least two Providers and no conflicts of interest are identified. |  |
| Demonstrate the ability to obtain a third party audit to ensure the Trust Framework’s policy, practices and existing operations are being adhered to with documented evidence of successful Provider operations. |  |
| Provide a Policy demonstrating the ability to provide identity assurance, authenticator assurance, federation assurance, privacy protections and operational activities comparable to the requirements of the Federal Government’s, including alignment with NIST 800-63 and NIST 800-53 controls. |  |
| Provide a Practice Statement demonstrating the Trust Framework and at least two Provider’s operational capabilities satisfy their established Policy. |  |
| Provide a charter describing membership, conflict resolution, authority, and organizational relationships |  |
| Provide documentation of the Trust Framework’s Architecture (to include Providers). |  |
| Provide evidence of the corporate status of the entity responsible for the Trust Framework, and its financial capacity to manage the risks associated with operating the community of interest. |  |
| Provide evidence of the Trust Framework’s knowledge, skills, and abilities in the management and operations of a Trust Framework. Include resumes of key staff, identifying roles, experience and expertise, number of years in the field, etc. |  |

# 

# Appendix B – Trust Framework Certification Application

Trust Framework Certification Application

**Trust Framework’s Date of Submission:** Click here to enter a date

**Approved by GSA OGP Trust Framework Solutions Program on:** Click here to enter a date

**1. Submittal Information**

*Once this Certification Application is complete, please sign it and email an electronic copy to ICAM@gsa.gov.*

**2. Organization Information**

|  |  |
| --- | --- |
| **Trust Framework Organization** |  |
| **Trust Framework Organization Address** |  |

**3. Trust Framework Point of Contact (POC) Information**

*Provide POC information for the representative authorized to speak on behalf of the organization, the person who will support the certification process, and the person who will address technical issues.*

|  |  |
| --- | --- |
| **Organization Representative POC** | Name and Title  Postal Address with Zip Code  Office Phone Number  Office E-mail Address |
| **Technical POC** | Name and Title  Postal Address with Zip Code  Office Phone Number  Office E-mail Address |

**4. Assurance Mapping:**

*Please provide information about your Credential Service Provider (Providers) and the assurance levels they support:*

|  |  |
| --- | --- |
| ***Insert Provider Name*** | |
| **Assurance Level** | **Description** |
| Identity Assurance Level |  |
| Authenticator Assurance Level |  |
| Federation Assurance Level |  |

**6. Trust Framework Community of Interest Overview**

*Provide information about the Trust Framework’s community of interest and their member Providers. Note that the Trust Framework must have experience operating a Trust Framework and have at least two member Providers.*

|  |  |
| --- | --- |
| ***Trust Framework Information Requested*** | ***Trust Framework Response*** |
| The following governance documentation should be identified here and submitted with the certification application:   * Policies, Practice Statement, Charter * Membership requirements (for on-boarding and maintaining membership) * Conflict resolution processes and procedures for the Trust Framework |  |
| Describe the nature of the relationship between member Providers and the Trust Framework- What are the requirements for entering and maintaining affiliation with the Framework? What is the nature of the financial ties? Under what circumstances are Providers dismissed? |  |
| What Community of Interest does the Trust Framework serve? |  |
| How does the Federal Community currently rely on identity assurance and authenticators / credentials issued by Trust Framework Members? |  |
| Describe the Federal Relying Party Application(s) that expect(s) to benefit from the use of these credentials. |  |
| Describe the relationship between the Trust Framework and its U.S. Federal Entity Sponsor. |  |
| Describe the current operational status/practice of the Trust Framework member Providers. For example:  Are the Provider’s services currently operational in the mode in which the Trust Framework intends to certify? |  |
| Are any Providers or part of any system associated with the Trust Framework operated or managed in a foreign country? |  |

**7.Federal Sponsor**

*Provide the name and contact information of the Trust Framework’s Federal Sponsor.*

|  |  |
| --- | --- |
| **Sponsor Name & Title** |  |
| **Sponsor Department/Agency** |  |
| **E-mail** |  |
| **Phone** |  |

**8. Corporate Status**

*Provide evidence of the corporate status of the entity responsible for the Trust Framework, and its financial capacity to manage the risks associated with operating the Community of Interest. The nature and sufficiency of the corporate status and financial capacity will be determined at the discretion of the Trust Framework Program on a case-by-case basis.*

**9. Knowledge, Skills and Abilities**

*Provide evidence of the Trust Framework’s knowledge, skills, and abilities in the management and operations of a Trust Framework. Include resumes of key staff, identifying roles, Identity, Credential, and Access Management experience and expertise, number of years in the field, etc.*

**10. Signature**

*The certification application must be signed and dated by a senior official (an officer or executive) authorized to speak on behalf of the Trust Framework and an authorized representative of the sponsoring agency.*

|  |  |
| --- | --- |
| **Applicant** | **Sponsor** |