SAFE-BioPharma FICAM Trust Framework Provider Approval Process (FICAM-TFPAP)

16 December, 2016

Version 2.11

Document Control

Author(s):	SAFE-BioPharma Trust Framework Program Team
Approver:	SAFE-PAA
Issue Date:	16 December 2016
Version:	2.11
Source File:	SAFE-BioPharma Trust Framework Provider Approval Process for FICAM Comparability.doc
Security:	SAFE-BioPharma Association confidential
Distribution:	The information contained in this document is intended for personnel charged with the management and operation of the SAFE-BioPharma Association Trust Framework Program. Recipients include SAFE-BioPharma, SAFE Members, SAFE Working Group Participants, Regulatory Agencies, SAFE Partners and Applicants for membership in the FICAM Profile Trust Framework.

Version History

Version	Author	Date	Summary of changes
1.0	Rich Furr	13 Apr 2012	Original Version
1.1	Peter Alterman	16 Oct 2012	Revised and Expanded
1.2	Peter Alterman	29 October 2013	Revised and Expanded
1.3	Peter Alterman	5 February 2014	Revised and Expanded
2.0	Peter Alterman	5 August 2014	New Version Aligned with FICAM TFS 2.0
2.01	Peter Alterman	8 August 2014	Editorial corrections
2.10	Peter Alterman	15 July 2015	Expand non-compliance review and revision processes.
2.11	Peter Alterman	30 November 2016	Insert Revised Issuer Agreement in Appendix A

Approval and Authorization

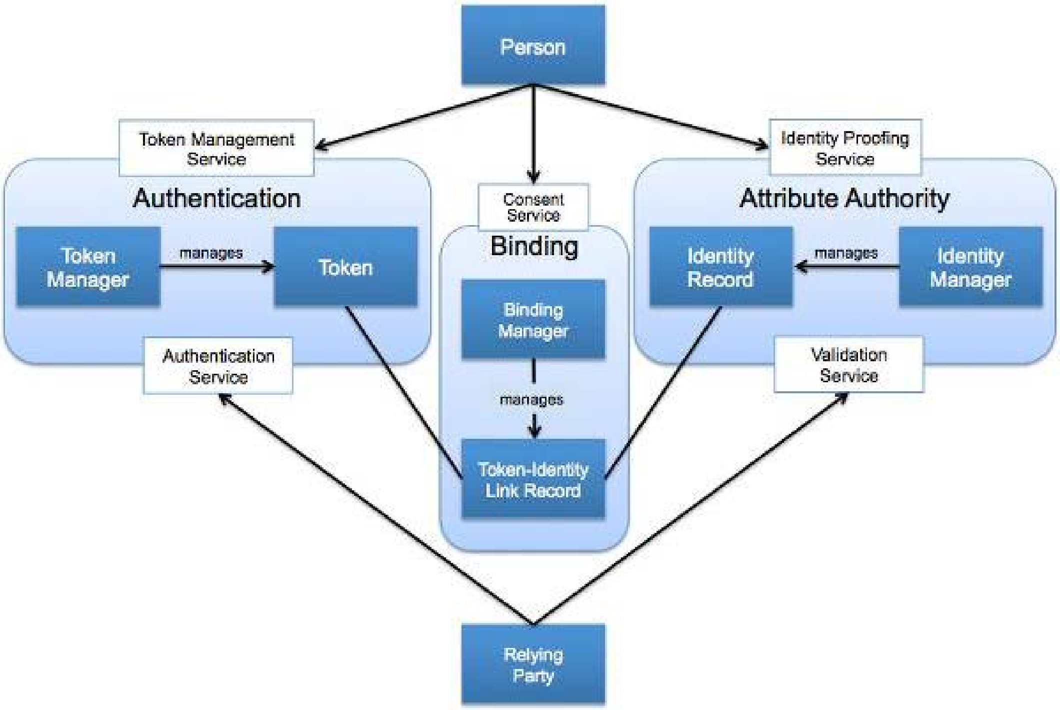
Completion of the following signature blocks signifies the review and approval of this document.

Name	Job Title	Signature	Date (dd/mm/yyyy)
Peter Alterman, Ph.D.	Chief Operating Officer	SAFE-BioPharma® SAFE-BioPharma Association Digitally signed by Peter Alterman DN: c=US, o=SAFE BIOPHARMA, ou=178c538b-dd33-4c21-9cc1-4cbdc142e903, cn=Peter Alterman Date: 2016.12.16 11:05:57 -05'00'	
Gary Secrest, J.D.	Chair, SAFE-BioPharma Policy Authority		

Introduction

Critical to the success of the SAFE-BioPharma Federal Identity, Credential and Access Management (FICAM) Trust Framework Provider (TFP) Program is the assessment for membership of providers who best serve the interests of the biopharmaceutical industry directly or indirectly while satisfying the comparability requirements of the US Government's FICAM program. Membership means that any Identity Manager, Attribute Manager, Token Manager or Full-Service Credential Service Provider certified by the SAFE-BioPharma Trust Framework Provider Program is trusted to provide identity assertions to Federal agency and private sector Relying Party (RP) applications. The SAFE-BioPharma FICAM TFP determines that the IdP's policies and practices are comparable to one or more of the trust models defined herein.

The following adoption process for FICAM provides a consistent, standard, structured means of identifying, vetting, and approving Component Members or Full-Service CSP Members. In addition, this process provides assurance to all affiliated RPs of the validity, and thus dependability, of the member provider's identity credentials and tokens. This confidence is essential to broad acceptance and use of non-local credentials.
FICAM Trust Framework Solutions 2.0 is based on a decoupled services model:



This results in identification of six (6) trust criteria categories:

1. *Registration and Issuance* – how well does the Identity Provider (IdP) register and proof the identity of the credential applicant, and issue the credential to the approved applicant?
2. *Tokens* – what is the Identity Provider's token technology and how well does the technology Intrinsically resist fraud, tampering, hacking, and other such attacks?
3. *Token and Credential Management* – how well does the Identity Provider manage and protect tokens and credentials over their full life cycle?
4. *Authentication Process* – how well does the Identity Provider secure its authentication protocol?
5. *Assertions* – how well does the Identity Provider secure Assertions, if used, and how much information is provided in the Assertion?
6. *Privacy Protections* – how well does the Applicant implement the US Government's Fair Information Practice Principles?

The SAFE-BioPharma FICAM TFP and its members address remote electronic authentication of human users to IT systems over a network. It does not address the authentication of a person who is physically present. TFP certification of Component Members or Full-Service CSP Members means that the identity applicant's policies and practices are comparable to SAFE-BioPharma's FICAM Trust Framework requirements.

At NIST LOA 1, 2, and non-PKI 3 (as defined in NIST SP 800-63-2), each Applicant for Component Member or Full-Service CSP Member must demonstrate comparable trust in each of the above categories for each LOA it wishes its credentials to be trusted by relying party applications (including physical access control systems).

The *SAFE-BioPharma FICAM TF 2_0 Assessment Criteria* Spreadsheet lists out all FICAM requirements and additional SAFE-BioPharma Trust Framework Requirements in an easy-to-use format. This Microsoft Excel spreadsheet is available upon request from the Program Manager.

Table of Contents

Adoption Process

Background

To assist the applicant, SAFE-BioPharma has developed requirements templates presented in the Appendices to this document. Applicants are not required to submit their assertions in any particular format, nor are they required to comply strictly with any particular trust criterion. Instead, the Applicant must demonstrate that its trust specifications meet or exceed the trust criteria in NIST SP 800-63-2. Failure to comply with any particular requirement is not fatal, since alternative mitigation strategies may satisfy trust criteria, especially at LOA 1 and LOA 2. ***Where such alternative mitigation strategies are implemented, the application must describe them and make the case for their comparability to the NIST strategy. Comparability in this context may be considered to be viable alternative means of mitigating the threat vector that the NIST element addresses.***

The Applicant's submission must directly and explicitly build the comparability case for all TFPAP criteria. Merely presenting supporting documents and expecting the Assessment Team to take on the burden of searching for comparability and building the case for the Applicant is not acceptable. Submissions that place the burden of building the case for comparability on the Assessment Team will be returned to the Applicant, which may cause delay in admission to membership in the Trust Framework.

The SAFE-BioPharma Trust Framework Program (TFP) determines whether admission of the Applicant to membership in the SAFE-BioPharma FICAM Trust Framework would be valuable to the health care and biopharmaceutical industry, directly or indirectly. As part of the determination discussion, the SAFE-BioPharma Trust Framework Program team assesses the Applicant's organizational maturity, which may include, but is not limited to the following:

- Applicant legal status;
- Appropriate authorization to operate;
- Financial capacity to manage the risks associated with conducting assessments and certifying Identify Providers;
- Scope and extent of implemented security controls (e.g., access control, confidentiality of Identity Provider information);
- Documentation of policies and procedures;
- Proof that Applicant practices are consistent with documented policies and procedures (e.g., via independent auditor reports, if required by LOA requirements).

The SAFE-BioPharma Trust Framework Program may request Applicant *bona fides* to assess Applicant organizational maturity, legitimacy, stability, and reputation.

Who does the assessment?

For Identity Managers, the SAFE BioPharma TFP performs an internal review of the Applicant's Identity Proofing policies and practices. Since a stand-alone Identity Manager does not generate any output until it affiliates with other Components, its application consists of documentation of policy and practice only and therefore there is no need for an independent Assessment Team to review practice against policy.

For all other Components and the Full Service CSP, assessment of comparability with SAFE-BioPharma TFP requirements is performed by one or more Accredited Assessors. The Assessors are the ones who actually perform the comparability assessments of Applicants (other than Identity Managers) and report their findings to the SAFE-BioPharma Trust Framework Program, which makes the final decision regarding the Applicant's request for membership.

Process Overview

During an assessment, the TFP communicates with the Applicant and its Assessors to ensure accuracy and to allow the Applicant to remedy identified deficiencies. There are two comparability assessments and one legitimacy determination:

- Legitimacy Determination - Determination of whether the Applicant sufficiently demonstrates organizational maturity, legitimacy, stability, and reputation is performed by the SAFE-BioPharma Trust Framework Management Team and approval is required before the application process can proceed.

- Trust Criteria Assessment – the Assessment Team determines whether the Applicant's policies and practices are comparable to the SAFE-BioPharma TFP criteria for each component. Trust criteria assessment includes:

  1. Technical and policy comparability based upon the relevant trust criteria;
  2. Privacy policy comparability using the following requirements:
     a. Opt In – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any relying party applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.
     b. Minimalism – Identity Provider must transmit only those attributes that were explicitly requested by the RP application.
     c. Activity Tracking –Identity Provider must not disclose information on End User activities with government or private sector entity to any party, or use the information for any purpose other than federated authentication.
     d. Adequate Notice – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the

purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice may be incorporated into the Opt In process.

The assessment process is flexible, and depends upon the needs of the Assessment Team. In general, the Team begins by reviewing the Applicant's submission. The Team may meet with the Applicant one or more times throughout the assessment process to ask questions or obtain clarifications. Such meetings become part of the assessment record. When the Team has sufficient information, it makes a final determination of comparability at the desired LOA(s). The Team may determine that there is no comparability at any LOA. The Team documents its findings, with all applicable supporting information, in a Summary Report specific to an Applicant.

The Summary Report indicates:

1. The extent of the Applicant's comparability to the SAFE-BioPharma Trust Framework for each relevant technical and policy trust criteria category;
2. The extent of the Applicant's comparability to the SAFE-BioPharma Trust Framework for each privacy policy;
3. Sufficiency of the identity provider's bona fides.

The Trust Framework team reviews the Summary Report for the Applicant and recommends admission or rejection of the Applicant to membership in the Trust Framework to the SAFE-BioPharma Policy Approval Authority for final decision. Upon adoption, the new member is added to the list maintained by SAFE-BioPharma and posted on appropriate websites. Member firms of the SAFE-BioPharma Association, Federal agencies and other entities are notified of the adoption.

When an approved Identity Manager Component member or an approved Token Manager Component member connects with a counterpart, the created Full-Service Credential Service Provider is subject to an assessment of the manner in which the two components exchange information, since this important element is addressed by neither individual review and is explicitly addressed by NIST SP 800-63-2. When an approved component member affiliates with a non-approved counterpart, both the interchange functions and the non-approved functions shall be subject to assessment under the full-service provider processes. In this case, the approved component does not require re-assessment or review, only interchange and the non-approved component must be assessed. **FICAM does not at the present time allow Components approved by other FICAM-approved Trust Frameworks at the addressed LOA to connect with components approved by the SAFE-BioPharma Trust Framework FICAM Profile, that is, FICAM does not currently allow "mix and match."**

Accredited Assessors

The SAFE-BioPharma Trust Framework Program certifies independent, third-party assessors who have demonstrated the necessary professional competence to evaluate a candidate's conformance with the Trust Framework requirements for all components under either Profile. Accredited Assessors are listed on the SAFE-BioPharma Association website, http://www.safe-biopharma.org/SAFE_Trust_Framework.htm.

Accredited Assessors must:

- Demonstrate competence in the field of compliance assessments;
- Be thoroughly familiar with all requirements that the SAFE-BioPharma FICAM Trust Framework Program imposes on all members;
- Perform such assessments as a regular ongoing business activity; and
- Be Certified Information System Auditors (CISA) and IT security specialists or equivalent, such as accreditation as an ISMS auditor or demonstrated experience performing satisfactory assessments.

Assessor Approval Process

Assessor candidates must present their qualifications to the SAFE-BioPharma Trust Framework Program for approval before they can be certified as Approved Assessors. An assessor candidate who is an Approved Assessor under another FICAM-recognized Trust Framework is considered to have satisfied the requirements and may submit proof of its approval status to satisfy the above requirements.

Assessment Teams

Assessors may need to engage the services of experts in various component areas such as privacy policy and practice or technology implementation. Where such a team is aggregated, the SAFE-BioPharma Trust Framework Program will make a determination as to the adequacy of the team to perform the required assessment. Applicants should submit the *bona fides* of the assessment team to the Program prior to initiation to ensure that the assessment results will be acceptable to us.

Credential Technologies

In addition to the low-assurance UserID/Password pair, the SAFE-BioPharma Trust Framework Program FICAM Profile for credential technologies defers to the FICAM Trust Framework Solutions 2.0 specifications for credential technologies. Both the FICAM-approved technologies and the technical requirements for implementing those technologies can be found at: http://www.idmanagement.gov/adopted-technical-profiles-and-identity-schemes. Should an Applicant wish to employ a credential technology not currently approved by FICAM TFS 2.0, please contact us to discuss how that might be accomplished.

Mapping Process

The FICAM Profile recognizes four component options:

- The **Identity Manager** component is responsible for identity proofing a subscriber according to policies and procedures designed to satisfy the requirements of either Profile. The Identity Manager does not issue online identity credentials but instead sends the data of a successful proofing to a Token Manager according to the aforementioned policies and procedures.
- The **Token Manager** is responsible for issuing and managing electronic identity credentials according to policies and processes designed to satisfy the requirements of either Profile. The Token Manager relies on an Identity Manager to provide the identity proofing component of the online electronic identity credential it issues. The Token Manager and the Identity Manager must exchange data in a *way* that satisfies requirements for privacy protection and data protection conformant with the particular Trust Framework Profile with which it certifies.
- The **Authentication Service** component may be part of the Token Manager, the Identity Manager, the Full-Service CSP or a stand-alone service. This function is responsible for collecting and validating specific extended attributes of a Subscriber for presentation to Relying Parties as required for authentication and/or authorization and for verifying the validity of issued credentials when queried by an RP or middleware service. The extended attribute sets required by FICAM are presented along with the other requirements in the *SAFE-BioPharma FICAM TF 2_0 Assessment Criteria* spreadsheet. Since FICAM requires all the other component options to include the Authentication Service, its requirements are present for each. There is currently no agreed-upon model for a stand-alone Authentication Service so the SAFE-BioPharma Trust Framework 2.0 incorporates these requirements for all components.
- The **Full-Service Credential Service Provider** (CSP) performs all the functions of the Components, above. In general, there are two ways an entity can be certified as a Full-Service CSP: either by performing all functions itself or by aggregating Identity, Authentication and Token Manager functions under an umbrella construct. In the latter, the entity aggregating the individual components' functions is also responsible for ensuring all data exchanges among the components satisfy the FICAM requirements under its policy rule set.

How to Apply

Program requirements for each Component at each NIST Level of Assurance are presented in a convenient spreadsheet matrix that may be requested from the Program manager. After first communicating its desire to become a member to the Trust Framework Program Manager, the Applicant fills out the appropriate matrix and submits it in an electronic format. Application fees and Trust Framework membership fees shall be discussed prior to submission.

As described above, Applicants for Token Manager and Full-Service Credential Service Provider must make arrangements to have their documentation and practices assessed by an Accredited Assessor/Assessment Team. The Assessor evaluates the Applicant submission against the SAFE-BioPharma FICAM Trust Framework Provider requirements in the appropriate tab of the available mapping spreadsheet. As noted above, assessment consists of review of policies, privacy practices, operational practices and technology implementations at each target LOA, so an assessment *team* is often required to address all areas competently.

Identity Manager

Naturally, the Identity Manager will not have to demonstrate comparability with the FICAM technology requirements, nor demonstrate how it hands off identity proofing results to Token Managers. Since no actual processes are implemented by a free-standing Identity Manager component, it is not necessary for an assessor to review an operational process. Thus, the mapping consists of the Applicant filling out the mapping matrix in the *SAFE-BioPharma FICAM TF 2_0 Assessment Criteria* spreadsheet “IdM+AuthN” tab and submitting supporting policy and practice documentation to the SAFE-BioPharma Trust Framework Program Manager. After review by program staff and only if necessary, phone meetings will be arranged to discuss issues that may have arisen and agree upon alignments. If the application is approved, the Applicant becomes an Identity Manager member of the SAFE-BioPharma FICAM Trust Framework and the Program Manager informs FICAM and all other Trust Frameworks affiliated with FICAM of the successful outcome.

Attribute Bundles and Validation Service

In addition to the identity management elements derived from Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) requirements, FICAM requires CSPs, TMs and IMs to support validation of one or more extended attribute bundles and to demonstrate the ability to assert them to FICAM on behalf of US Government relying parties and middleware services. For more on these requirements, see the FICAM ATOS document at: http://www.idmanagement.gov/documents/authority-offer-services-atos-ficam-tfs-approved-identity-services. Applicants who have successfully completed the SAFE-BioPharma FICAM Trust Framework Provider Approval Process must then contact the FICAM Program Office to arrange for ATOS testing. This testing is not part of this Approval Process.

Token Manager – Policy and Practice Assessment by Approved Independent Assessor

The Token Manager component Applicant arranges for an assessor approved by the SAFE-BioPharma TFP to review its policy and practice documents and to monitor its processes to ensure that its practices satisfy its requirements. The Token Manager must operate in a manner that is demonstrably comparable to the requirements of the FICAM Trust Framework Solutions 2.0. This can be done by conforming to the actual requirements of NIST SP 800-63-2 or by demonstrating alternate approaches that are comparable to the NIST requirement. The *SAFE-BioPharma FICAM TF 2_0 Assessment Criteria* “TM+AuthN” tab contains a mapping of the requirements and the Token Manager Applicant must fill out the mapping matrix, demonstrating comparability with FICAM and SAFE-BioPharma Trust Framework requirements. The independent assessor will evaluate the mapping and work with the Applicant to ensure approval.

The Token Manager will also have to demonstrate to its assessor that the token technology it employs meets the FICAM Technology Scheme requirements for that technology.
When the review has been completed by the assessor, the results are presented to the SAFE-BioPharma Trust Framework Program, which reviews the assessor report, reviews documentation and approves or disapproves the application. If the application is approved, the Applicant becomes a Token Manager member of the FICAM Profile SAFE-BioPharma Trust Framework and the Program Manager informs FICAM and all other Trust Frameworks affiliated with the government’s program of the successful outcome.

Full Service CSP - Policy and Practice Assessment by Approved Independent Assessor

The Full Service CSP Applicant arranges for an assessor certified by the SAFE-BioPharma Trust Framework Program to review its policy and practice documents for Identity Proofing, Token Management and Attribute Management. The assessor reviews its documentation and assesses practice against policy and procedure documents to ensure that its practices satisfy requirements.

Full Service CSPs must operate in a manner that is demonstrably comparable to the requirements of the FICAM Trust Framework Solutions 2.0. This can be done by conforming to the actual requirements of NIST SP 800-63-2 or by demonstrating an alternate approach that gives a result comparable to the aim of the NIST requirement.

The Full-Service Credential Service Provider Applicant must fill out the mapping matrix in the *SAFE-BioPharma FICAM TF 2_0 Assessment Criteria* “CSP+AuthN” tab, demonstrating comparability with all FICAM requirements. The independent Assessor will evaluate the mapping and work with the Applicant to ensure approval.

Full Service CSPs will also have to demonstrate to the assessor that the token technology they employ meets the FICAM Technology Scheme requirements for that technology. Those requirements can be found at http://www.idmanagement.gov/adopted-technical-profiles-and-identity-schemes.

When the review has been completed by the assessor, the results are presented to the SAFE-BioPharma Trust Framework Program, which reviews the assessor report and supporting documentation and approves or disapproves the application. If the application is approved, the Applicant becomes a Full Service Credential Service Provider member of the SAFE-BioPharma FICAM Trust Framework and the Program Manager informs the FICAM program office and all affiliated Trust Frameworks of the successful outcome.

Procedures for Resolving Findings of Non-Compliance

Either at time of initial application or at time of renewal review an Accredited Assessor may find an applicant to be not in compliance with Trust Framework requirements. The findings may address policy or actual practice. An assessor must present a complete and substantive report to the SAFE-BioPharma FICAM Trust Framework and the Program Manager of all non-compliant findings sufficient for the Applicant to fully resolve all issues. An incomplete or partial explication of non-compliance by an Assessor will not be acceptable.

Right of the Applicant to Challenge Findings

An Applicant has the right to challenge an assessor’s findings for cause. Such a challenge shall be made in writing to the Program Manager with a copy sent to the Assessor. The Program Manager will schedule a meeting with the Applicant and the Assessor to discuss the issues and attempt to resolve all non-compliant findings. If as a result of the meeting the Applicant revises its policy and/or practice, a full reassessment of the revisions will be required to be submitted to the Program Manager. If, however, the result is concurrence that Applicant’s challenge is valid, then a statement to that effect signed by both parties will be included in the application documentation. These requirements hold for each and every finding.

Further Testing Requirements – FICAM Approval To Offer Services (ATOS)

In order for a Full Service CSP's credentials to be consumed and validated by many US Government relying parties and to qualify to bid on Requests For Proposals (RFPs) that require FICAM approval, the FICAM program has instituted an additional test requirement. Members will have to demonstrate to the FICAM program office that its tokens satisfy additional ATOS requirements. See: http://www.idmanagement.gov/documents/authority-offer-services-atos-ficam-tfs-approved-identity-services. Full Service CSPs that do not successfully complete the ATOS testing program or who choose not to engage it will be reported as Token Managers by FICAM.

ATOS testing is reported to be provided at the Government's expense. At the present time, the SAFE-BioPharma Trust Framework Program does not operate an ATOS test service, though members of the Association may in future provide such services for a fee.

Post-approval Requirements

Memorandum of Agreement

Once an Applicant has successfully completed the application process, the SAFE-BioPharma Trust Framework Program negotiates a Memorandum of Agreement (MOA) with it, documenting the responsibilities of each party. When the MOA has been signed by both parties, the new Member may begin operations and may assert its conformance with the SAFE-BioPharma Trust Framework Program. A copy of the Issuer Agreement is attached at Appendix A. Agreements covering Component Members are available from SAFE-BioPharma.

Ongoing Requirements

An adopted member is subject to the following:

- Determination as to whether it should be discontinued or suspended (i.e., no longer acceptable to the SAFE-BioPharma FICAM Trust Framework. Discontinuance or suspension may be for reasons including, but not limited to:
  - no longer being comparable with applicable SAFE-BioPharma FICAM Trust Framework requirements;
  - Failure to abide by terms of the signed Memorandum of Agreement;
- Comparability re-assessment (i.e., another comparability mapping), as requested by any SAFE-BioPharma FICAM Trust Framework member; and
- Comparability re-audit due to some length of time since last assessment or a significant change to operations or policies (see below).

Recertification Requirements after Discontinuance or Suspension

Should a Discontinued or Suspended Trust Framework member wish to be reinstated to “approved status, it must submit a written request to the Program Manager and a report from an Approved Assessor demonstrating that it has remediated the problem(s) that caused Discontinuance or Suspension. The Program Manager will arrange a meeting of the member, the Assessor and other parties as appropriate to review the report and ensure the problem(s) causing Discontinuance or Suspension have been adequately rectified. Should the reviewers determine that the problem(s) have been adequately remedied; the member will be returned to full active membership status immediately.

Regular Reassessment Requirements

All members are required to undergo regular reassessments and report the results to the SAFE-BioPharma FICAM Trust Framework Program according to the following criteria:

- Identity Managers must submit policy and practice documents for reconsideration whenever significant changes occur;
- Token Managers and Full Service CSPs at LOA 1 may complete self-assessments and submit assertions of compliance with approved policies and practices once every three years or whenever significant changes to policy, practice and/or technology occur;
- Token Managers and Full Service CSPs at LOA 2 and LOA 3 must complete partial reassessment of core functions annually and a full reassessment at least every three years. Significant changes to policy, practice and/or technology also trigger the requirement for a full reassessment. These reassessments must be performed by an Accredited Assessor.

Responsibility to Report Changes in Policy and/or Practices

An adopted Identity Management component is subject to re-review when its policies and/or practices change. When this occurs, it is the responsibility of the component management to inform SAFE-BioPharma of the change and to request a re-review to maintain its membership status. An adopted Token Manager component is subject to re-assessment when its policies and/or practices change and must report significant changes to the Trust Framework Program. Failure to do so promptly will result in suspension of the member from the Trust Framework.

Appendix A: SAFE-BioPharma TRUST FRAMEWORK PROVIDER PROGRAM ISSUER AGREEMENT

THIS SAFE-BioPharma TRUST FRAMEWORK PROVIDER PROGRAM ISSUER AGREEMENT (this “Agreement”) is between SAFE-BioPharma Association, a Delaware limited liability company (“SAFE-BioPharma”) and____________________as “Issuer.” This agreement specifies the rights and permissions for Issuer to issue annually non-PKI credentials to Subscribers that conform to the SAFE-BioPharma Trust Framework Provider program requirements for trustworthiness at levels of assurance listed in #3, below.

In consideration of the mutual promises in this Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, SAFE-BioPharma and Issuer (each, a “Party” and collectively, the “Parties”) hereby agree as follows:

1. Definitions. Capitalized terms not defined herein shall have the meanings given to them in that certain document entitled “SAFE-BioPharma System Documentation Glossary” as referenced in Appendix B.

2. Standards and Operating Policies. All of the provisions of the documentation listed in Appendix B in effect as of the signing of this Agreement are incorporated in this Agreement by this reference as if fully set forth herein, including, without limitation, the provisions of that certain document entitled “SAFE-BioPharma Operating Policies” (the “Operating Policies”). Issuer hereby agrees to abide by all of the terms and conditions of such documentation that are specifically applicable to issuers of non-PKI authentication credentials.

3. Authentication Credential Issuance. Issuer may issue SAFE-BioPharma-approved authentication credentials to end users at one or more of the following NIST Levels of Assurance:

NIST Level of Assurance	Approved
LOA 2	
LOA 3	

4. Subscriber (End User) Requirement. The Operating Policies require Subscribers to sign a Subscriber Agreement with Issuer to use their SAFE-BioPharma-compliant credentials. The

contents of the Subscriber Agreement are described in the "SAFE-BioPharma FICAM TF 2.1 Assessment Criteria" spreadsheet.

5. Rights of the Parties. The Parties agree as follows:

   a. Rights of the SAFE-BioPharma Trust Framework Provider Program (TFP). By entering into this agreement, the TFP acquires the rights to appropriate access to Issuer information such as assessment results, operational information, and testing processes.

      If at any time the TFP determines that the Issuer is not operating at the Level of Assurance specified in this Agreement, the TFP representative shall notify the Issuer and may unilaterally reduce the Level(s) of Assurance expressed in the credential issued by the Issuer and inform all other participants in the US government's FICAM Trust Framework Services Program of such action. The TFP shall provide the Issuer an opportunity to cure the assurance issues and regain its original Level(s) of Assurance.

   b. Rights of the Issuer. The Issuer has the same rights with respect to its governance of its credential issuance service as the rights of SAFE-BioPharma to its governance of its TFP.

6. Responsibilities of the Parties. The TFP and the Issuer agree as follows:

   a. The TFP shall oversee and ensure proper performance of the operation and maintenance of the SAFE-BioPharma Trust Framework Provider Program in accordance with the Trust Framework Provider Program documents listed in Appendix B.

   b. The TFP will maintain compliance with the requirements of this Agreement, or promptly notify the Issuer in the event of an actual or expected nonconformance.

   c. The TFP shall make its compliance assessment reports available to the Issuer, within a reasonable time in response to any requests for information by the Issuer.

   d. The TFP shall promptly advise the Issuer in the event that the PAA becomes aware of a material non-compliance on the part of any other party that is participating in the US government's FICAM Trust Framework Solutions program. Issuer shall be notified by telephone, by digitally signed e-mail, or by any other mechanism agreed upon by the Parties.

   e. The TFP shall review its controlling documents at least once a year for changes that may become necessary from time to time. When the TFP requirements are changed, the Issuer shall receive a copy of the revised document(s) promptly and arrangements made to recertify the Issuer.

f. Issuer agrees that it will comply with the applicable requirements of the SAFE-BioPharma TFP and such other requirements (e.g., laws, regulations, data center requirements) as govern the operation of the Issuer service.

g. Issuer shall:

  - maintain compliance with the requirements of this Agreement, or promptly notify the TFP in the event of an actual or expected nonconformance. Failure to maintain compliance may result in revocation of TFP's approval of Issuer services and may invoke the dispute resolution process described in the Operating Policies.

  - respond within a reasonable time to any requests for information by the TFP.

  - as necessary, review revisions to the TFP requirements when they change.

  - promptly notify the TFP in the event of any change to the information in its Application, if possible before the change takes effect. This includes any change in the Issuer practices, subcontractor relationships or other information upon which the TFP relied when approving the Issuer's practices to the NIST levels of assurance. The notification shall include the former and new versions where the change occurs, and the effective date of the change.

h. The Issuer shall notify the TFP in the event there is any substantial change to the business, to include (but not limited to) acquisitions, bankruptcy, etc.

7. Term and Termination. This Agreement shall be effective as of the date both parties have signed this Agreement and shall continue indefinitely until terminated by one or both of the parties. Both parties retain the same right to terminate the relationship. Notification of termination shall be presented in written form, either electronic or otherwise.

8. Requirement to Protect Personally Identifiable Information of Subscribers After Termination. In the event of termination, the Issuer agrees to continue indefinitely to protect the privacy and confidentiality of all Personally Identifiable Information related to Subscribers, including personal attributes and roles acquired subsequently as part of routine service provision from attribute providers.

9. Notices. All notices, requests, consents, approvals, agreements, authorizations, acknowledgments, waivers and other communications required or permitted under the Operating Policies shall be delivered to the respective address of each Party as indicated below.

10. Fees. Issuer agrees to pay SAFE-BioPharma the specific annual certification fees invoiced to the Issuer by SAFE-BioPharma within 45 days of invoicing according to the fee schedule as attached in Appendix A. Fees published in Appendix A shall be valid for the term of the agreement. Increases to the annual certification fee also are described in Appendix A.

11. Miscellaneous.

a. Entire Agreement. This Agreement, together with the documentation referenced in Appendix B (which is incorporated herein by this reference) represent the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior agreements and understandings relating to such subject matter, and there are no other representations, understandings or agreements between the Parties relative to such subject matter.

b. Amendments and Waivers. Amendments or waivers of any provision of this Agreement shall be governed by the Operating Policies and are subject to mutual agreement between Issuer and SAFE-BioPharma.

c. Assignment; Binding Effect. Assignment of this Agreement shall be governed by the Operating Policies. This Agreement shall be binding upon, and inure to the benefit of, the Parties hereunder and their permitted successors and assigns.

d. Severability. If any provision of this Agreement is determined to be invalid or unenforceable, in whole or in part, such invalidity or unenforceability shall not affect the remainder of this Agreement, and this Agreement shall be deemed amended to the extent necessary to make this Agreement enforceable and valid.

e. Counterparts. This Agreement may be executed in any number of counterparts, each of which will be deemed an original, but all of which taken together shall constitute one single agreement.

f. Governing Law. This Agreement and the rights and obligations of the Parties hereunder shall be governed and construed in accordance with the laws of the State of New York as such laws are applied to agreements entered into and to be performed entirely within New York, without giving effect to the principles thereof relating to the conflicts of laws.

g. Official Points of Contact.
For the purposes of this Agreement, the Official Point of Contact for the PAA shall be
____.
The Official Point of Contact for the Issuer shall be _______________________________.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to execute this Agreement.

SAFE-BioPharma Association

By: ____________________________________
Name:
Title:
Date:

Address: ______________________________
____
____

ISSUER: ________________________________

By: _____________________________________
Name:
Title:
Date:

Address: ______________________________
____
____

Appendix B

SAFE-BioPharma-Biopharma Association
Accredited Trust Framework Provider Program
Credential Issuer Fee Schedule

1. Accredited Credential Issuer Annual Certification Fees:

2016	$10,000
2017	$12,500
2018	$15,000

Subsequent increases shall be limited to no more than 3% annually.

2. Issuer Certificate Fee: this is a per credential fee based on the active (meaning not revoked or expired) PKI certificates issued by Issuer to end entities. The fee is $2.00 per year per active certificate as determined on a quarterly basis for all new certificates issued in the previous quarter or for any certificates which have been renewed in the previous quarter:

Appendix C

Required SAFE-BioPharma Trust Framework Provider Credential Issuer
Standards and Specifications

General Standards

SAFE-BioPharma General Operating Policies V3.0, 29 September, 2016
System Documentation Glossary v2.4 dated 31 March 2011
SAFE-BioPharma Functional Requirements Specification (FRS) v2.5, 31 December 2011