



SAFE-BioPharma FICAM Trust Framework Program Overview

08 August, 2014

Version 2.01

Copyright © SAFE-BioPharma, Association 2014. All rights reserved. The SAFE-BioPharma, Association copyrights this SAFE Standard document. This document is confidential material, and is intended for use only by the SAFE-BioPharma, Association and organizations participating in the SAFE System or their authorized agents. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by the SAFE-BioPharma, Association .

Document Control

Author(s): SAFE Trust Framework Provider Program Team

Approver: SAFE-PAA

Issue Date: 08 August 2014

Version: 2.01

Source File: SBP V2.0 FICAM TFP Program Overview Document.doc

Security: SAFE-BioPharma, Association Public

Distribution: The information contained in this document is intended for any entity interested in becoming a member of the SAFE-BioPharma Trust Framework or in affiliating with the SAFE-BioPharma Trust Framework.

Version History

Version	Date	Revised By	Summary of Changes/Comments
2.0	06/13/2014	P. Alterman	Initial draft of updated TFS program
2.01	08/08/2014	P. Alterman	Revised text and editorial corrections

Approval and Authorization

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

<u>Name</u>	<u>Job Title</u>	<u>Signature</u>	<u>Date</u>
P. Alterman	Chief Operating Officer		08/08/2014
G. Secret	Chair, PAA		

Introduction

SAFE-BioPharma started in 2003 when a volunteer taskforce of biopharmaceutical company IT professionals developed a way for industry to manage cyber-identities and to use those identities to apply a higher form of electronic signature to electronic documents. In conjunction with the US CIO Council, the FDA and the European Medicines Agency, they established the **SAFE-BioPharma digital identity and signature standard**, providing standardized, high-assurance identity trust for cyber-transactions across the biopharmaceutical and healthcare sectors. To enable this goal, they created the **SAFE-BioPharma Association**, the not-for-profit industry coalition that manages the SAFE-BioPharma standard. Our members fund the ongoing development and implementation of the SAFE-BioPharma standard and utilize the standard for a broad range of purposes. Our mission is to help industry protect its substantial information assets, move its business processes online, and become paperless in order to improve productivity, reduce costs, and lower time to market. A current list of our members and partners may be found at www.safe-biopharma.org.

SAFE-BioPharma operates three distinct Trust Programs. The first program is the **SAFE-BioPharma PKI Bridge Certification Authority** and the **Trusted Third Party SAFE-BioPharma CA**, issuing digital certificates that are recognized by the US Federal PKI Architecture at Bridge Basic, Medium Commercial Best Practice (CBP) and Medium Hardware CBP. Cross-certification with the Federal Bridge CA has been in place since 2008. The SAFE-BioPharma CA also issues digital certificates recognized by the EU under the Qualified Certificate Policy and the Advanced Electronic Signature standard.

The second program is the **SAFE-BioPharma FICAM Trust Framework** affiliated with the US Government's Federal Identity, Credential and Access Management subcommittee for non-PKI authentication credentials at NIST Levels of Assurance (LOA) 2 and 3. This program has been FICAM-approved since 2011.

The third program is the SAFE-BioPharma Global Trust Framework harmonized with international standards and European Union regulations. These two Profiles are comparable in trustworthiness but are not affiliated.

This document addresses the SAFE-BioPharma FICAM Trust Framework exclusively.

There is a separate Provider Approval Process for each Trust Framework (FICAM and Global) and the choice of which Profile a candidate may wish to join should rest on the business case each one presents. Of course, there is nothing to preclude an Applicant from affiliating with both SAFE-BioPharma Trust Frameworks.

Components of the SAFE-BioPharma Trust Framework

The **FICAM** Trust Framework recognizes four component options. They are Identity Manager, Token Manager, Attribute Manager and the synthesis of all, a Full Service Credential Service Provider.

- 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 **Attribute Manager** (Authentication Service) component may be part of the Token Manager, the Identity Manager or a stand-alone service. Attribute management is required under the FICAM Profile but is optional under the Global Profile. 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. The extended attribute sets required are defined in the SAFE-BioPharma Trust Framework Provider Approval Process documents.
- The **Full Service CSP** provides identity proofing, attribute management and credential management services. The Full Service CSP may perform all functions in-house or be a hybrid synthesizing outsourced multiple services under a single umbrella.

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 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 documented experience in this line of work.

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.

Comparability vs. Compliance

The SAFE-BioPharma Trust Framework Provider Approval Process does not require strict compliance with any particular requirement. Under the FICAM Profile, a candidate may comply with a specific requirement from NIST Special Publication 800-63-2 or it may demonstrate how it achieves a comparable goal using other means. This is because the FICAM Profile is based on NIST standards and practices mandated for US Government programs. Candidates must also satisfy the privacy requirements of the FICAM TFS 2.0 program.

Credential Technologies

In addition to the low-assurance UserID/Password model, the SAFE-BioPharma FICAM Trust Framework defers to the FICAM Trust Framework Solutions program of the US Government 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>. The FICAM TFS 2.0 program has procedures for adopting additional technologies documented in the FICAM *Identity Scheme and Protocol Profile Adoption Process*, also available at www.idmanagement.gov.

Digital certificate (PKI) credential services operate under the SAFE-BioPharma PKI Bridge Certification Policy (CP) and **do not** fall under the SAFE-BioPharma FICAM Trust Framework Program. Entities wishing to cross-certify their CAs with the SAFE-BioPharma PKI Bridge should contact us directly to receive a copy and to make the necessary arrangements of the policy and procedures documents that control cross-certification with the SAFE-BioPharma Bridge CA for audit.

Approval Process

- For FICAM approval see: “SAFE-BioPharma FICAM Trust Framework Provider Approval Process, Version 2.01”
- For Assessor candidates, see the requirements above.

To Apply

Send an email message to Dr. Peter Alterman, Chief Operating Officer, SAFE-BioPharma Association, palterman@safe-biopharma.org stating your interest in applying for membership in the SAFE-BioPharma FICAM Trust Framework. Feel free to contact us about any issue or question you may have.