



Signatures and Authentication For Everyone

SIGNATURES & AUTHENTICATION FOR EVERYONE

SAFE Bridge Certification Authority

Cross Certification Process

16 February 2006

Version 2.1

Copyright ©SAFE-BioPharma, Association 2005-2006. All rights reserved. SAFE-BioPharma, Association copyrights this SAFE Standard document. This document is confidential material, and is intended for use only by SAFE-BioPharma 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 SAFE-BioPharma.

Document Control

Area	Description
Author(s)	SAFE Core Team
Change Control	SAFE-BioPharma Association Change Management Council
Approver(s)	SAFE-BioPharma Policy Approval Authority (PAA)
Issue Date	16 February 2006
Version	2.1
Source File	SAFE Cross Certification Process Guideline.doc
Security	SAFE Stakeholder confidential
Distribution	The information contained in this document is intended for personnel charged with the management and operation of the SAFE System. Recipients include the SAFE-BioPharma Association, SAFE Members, SAFE Working Group Participants, SAFE Issuers, SAFE Partners, and Regulatory Agencies. This document is controlled and managed under the authority of the SAFE Policy Approval Authority.

Revision History

Revision	Date	Revised By	Summary of Changes/Comments
2.0	31 Jul 2005	R. Furr , M Ramos	Initial procedure
2.1	07 Feb 2006	R. Furr , T. Zagar	Revised logo on cover page to reflect new SAFE logo Added CA Self Assessment checklist Revised requirement for a Memorandum of Understanding Provided additional guidance for cross-certification process

Approval Statements

Once signed by the parties indicated below, this SAFE Cross Certification Process document has been approved by the SAFE Policy Approval Authority Committee and has been incorporated into the SAFE Standard Document Set.

SAFE-BioPharma Association PAA
Chairperson

Date

TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	Purpose	5
1.2	Intended Audience	5
1.3	Definitions.....	5
1.4	References.....	5
2	CROSS CERTIFICATION PROCESS	7
2.1	Phase I – Initiation.....	7
2.2	Phase II Review & Decision Points	10
2.3	Phase III - Testing	11
2.4	Phase IV – Agreement	13
2.5	Phase V - Maintenance	14
3	CRITERIA FOR CROSS CERTIFICATION	19
3.1	General Principles	19
3.2	Conditions	19
3.2.1	Initiation Phase.....	20
3.2.2	Policy Mapping Phase.....	21
3.2.3	Test Phase	23
3.2.4	Agreement Phase.....	24
	APPENDIX A: SAFE CERTIFICATE POLICY MAPPING MATRIX	25
	APPENDIX B: APPLICATION FOR CROSS CERTIFICATION	34
	APPENDIX C: SAFE-ISSUER AGREEMENT	39
	APPENDIX D: APPLICANT CROSS CERTIFICATION REQUEST LETTER TEMPLATE	42
	APPENDIX E: CA SELF-ASSESSMENT AUDIT CHECKLIST	45
	APPENDIX F: CROSS CERTIFICATION LETTER OF AUTHORIZATION TEMPLATE	47

1 Introduction

1.1 Purpose

The purpose of this document is to outline the process and criteria for cross-certification of the Principal Certification Authority of an Applicant's Public Key Infrastructure (PKI) with the SAFE Bridge Certification Authority (SBCA). This document is designed for use by entities (Applicants) that seek to cross certify and interoperate with the SBCA.

In December 2004, the SAFE Steering Committee approved the SAFE Certificate Policy. The policy defines the SBCA as an interoperability mechanism for ensuring trust across disparate domains. Successful cross certification with the SBCA asserts that the Applicant PKI operates in accordance with the standards, guidelines and practices of the SAFE Policy Approval Authority (PAA).

SAFE-BioPharma has accredited and contracted with a Cross Certification Review Agent (CCRA) for the purpose of executing significant portions of the cross certification process. Upon completion of the initial review of the Applicant's application for cross certification, SAFE-BioPharma will notify both the Applicant and the accredited CCRA to proceed with cross certification activities. Details of this process are included in subsequent sections of this process.

The SAFE Cross Certification Process shall be operated on a "Strive for Success" basis that requires all reasonable effort be made to ensure successful cross certification with Issuers.

1.2 Intended Audience

This document is intended for the use of information technology officials, PKI managers, and personnel involved in cross certification activities within SAFE, those entities accredited to operate as SAFE Issuers, and any other parties desiring to cross-certify with the SBCA.

These cross-certification guidelines should be read in conjunction with the SAFE Certificate Policy and the redacted version of the SAFE Certification Practices Statement, available at www.safe-biopharma.org.

1.3 Definitions

For purposes of this SAFE Cross Certification Process document, all terms used shall have the meanings set forth in the SAFE System Documentation Glossary.

1.4 References

This SAFE Cross Certification Process document makes reference to other SAFE documents, including:

- SAFE Operating Policies
- SAFE Functional Specifications

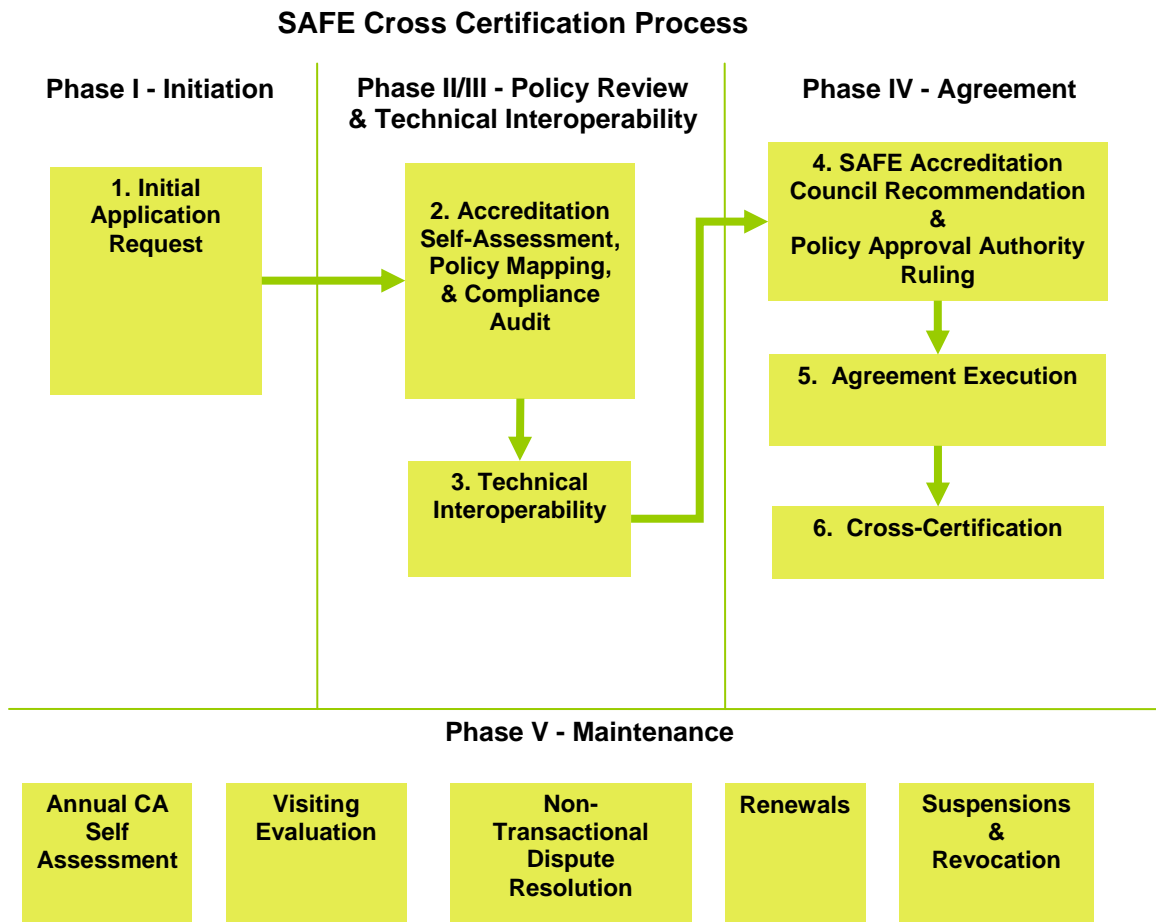
- SAFE Certificate Policy
- SAFE Registration and Certificate Management Technical Specifications
- SAFE Bridge Cross Certification Procedure

This document also references:

- Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

2 Cross Certification Process

A request to cross certify with the SBCA triggers a multi-phase process, depicted graphically below, and designed to achieve a mutually reliable trust relationship.



The Accredited SAFE CCRA conducts portions of Phases II and III of this process.

2.1 Phase I – Initiation

Phase I Overview:

- Request by Applicant to cross-certify with the SBCA
- Initial review of policy, technical and legal issues
- Determination if application is complete and all submissions comply with requirements

- Determination if applicant is an appropriate applicant for cross certification
- SAFE Accreditation Council (AC) decision to reject request or proceed to next phase

Step 1: Prepare Application for Cross Certification:

Purpose:

To prepare and submit the required information to the SAFE-BioPharma Association to cross-certify with the SBCA.

Activities:

1. The Applicant obtains documents and information to assist in the cross certification process with the SBCA. These documents include:
 - a. SAFE Certificate Policy Mapping Matrix (Appendix A)
 - b. Application for Cross Certification (Appendix B)
 - c. SAFE Certificate Policy (<http://www.safe-biopharma.org/images/stories/safe%20certificate%20policy%20v2-0.pdf>)
 - d. SAFE Issuer Agreement (Appendix C)
 - e. Applicant Cross Certification Request Letter template (Appendix D)
 - f. Issuer Self-Assessment Audit Checklist for SAFE Standard Compliance (Appendix E).

If required, the SAFE Technical Operations Staff will execute a non-disclosure agreement (NDA) to assure the applicant that all material presented during the application process will be protected in compliance with the terms of the NDA.

2. The Applicant completes the Application for Cross Certification. Appendix C provides the format and guidance for the Application. The Application includes the following information:
 - a. Information on the Applicant's organization
 - b. Reason(s) for requesting cross certification
 - c. High level information about the Applicant's Certificate Policy and Certification Practices Statement
 - d. High level information about Applicant's PKI architecture
 - e. High level information about Applicant's directory infrastructure
 - f. High level information about Applicant's auditing practices
 - g. Proposed level of assurance at which cross-certification is sought (i.e., proposed policy mapping)
 - h. High level information about Applicant's technical configuration (e.g. cryptographic algorithms, web portals, etc.)

3. The Applicant may be asked to provide additional information, such as but not limited to the following (note that if the Applicant is a national, state or local government, it may not be required to provide some of this information):
 - a. Evidence of the current legal status of the organization operating the PKI
 - b. Evidence of the financial capacity of the organization operating the PKI (such as bonds, letters of credit, insurance demonstrating the organization's ability to meet the financial responsibilities associate with operating a PKI)
 - c. A signed agreement not to disclose any security-related information revealed for the purposes of facilitating cross-certification

Step 2: Assess Mapping of Certificate Policies

Purpose:

To confirm that the Applicant's Certificate Policy (CP) maps to the SAFE Certificate Policy and meets the minimum SAFE System requirements for interoperability and digital certificate trust.

Activities:

1. The Applicant maps their Certificate Policy to the SAFE Certificate Policy, using the Certificate Policy Mapping Matrix. The Applicant may use the Certificate Policy Mapping matrix in Appendix A for this purpose. Note that the completion of this matrix allows the Applicant to assess whether there are any issues in cross-certifying with the SAFE Bridge. If the Applicant's CP does not follow the formatting guidance in RFC 3647, SAFE will require the appropriate mapping to RFC 3647; this matrix may also be used for this purpose.

Step 3: Submit Application Package to SAFE-BioPharma

Purpose:

To review the Applicant's application for cross certification with the SAFE Bridge and identify whether or not any significant issues exist that may impact the cross certification process.

Activities:

1. The Applicant submits one physical and one electronic copy of each document listed below to the Chief Technical Officer (CTO) of the SAFE-BioPharma Association (i.e., the delegated SAFE PAA point of contact for cross certification activities). The physical copy may be sent to the attention of the SAFE CTO at the address shown on the SAFE website (<http://www.safe-biopharma.org>) under the "Contact Us" tab. The items associated with the electronic copy must be in a format compatible with Adobe Reader or Microsoft Office, and should be sent to Bridge@safe-biopharma.org. The needed documents include:
 - a. Completed Application (which has been signed by the appropriate senior official)
 - b. Applicant's Certificate Policy

- c. Redacted version of Applicant's Certification Practices Statement
 - d. Applicant's completed CP mapping matrix (required only if Applicant's CP is not formatted in accordance with RFC 3647; recommended otherwise)
 - e. Applicant's most recent CA Audit Report Summary (recommended but not required)
2. Within 30 calendar days of submission of the above listed documents, the SAFE Technical Operations staff reviews the application to ensure all required documents and inputs are included.

The SAFE CTO prepares a recommendation to proceed for approval by the SAFE Accreditation Council (AC) and forwards it to the AC for action. The AC considers the recommendation and makes its determination based on the CTO's recommendation. The AC Chair advises the CTO of its decision and the CTO advises the Applicant point of contact (POC).

If the decision is to proceed, the CTO advises the Applicant POC to contact the CCRA to initiate its review and audit activities. The CTO also notifies the SBCA Operational Authority of the decision to proceed. The SAFE Technical Operations staff logs the application, and forwards it to the SAFE CCRA. The CCRA contacts the Applicant POC to arrange for mapping the Applicant's CP to the SAFE CP and for conducting interoperability testing of the Applicant's CA system and certificates.

If the decision is made to not proceed with the cross certification process, the CTO sends a letter to the Applicant POC enumerating the reason(s) why the Application has been rejected and steps the Applicant may take to reinitiate the process.

3. When notified of a decision to proceed, the Applicant enters into a contract with the CCRA for policy mapping and interoperability testing. All fees are paid directly to the CCRA by the Applicant. Fees for mapping may be paid separately from fees for interoperability testing based on the Applicant's progress in the cross certification process. The cross certification process then continues with Phase II for formal mapping of certificate policies. If the timing for cross certification is on the critical path, Phase II and Phase III may be started in parallel.

2.2 Phase II Review & Decision Points

Phase II Overview:

- Establishment of the Applicant's suitability for cross certification
- Resolution of policy differences and decision whether to continue with the process

Step 1: Review of Certificate Policies Mapping Matrix

Purpose:

To examine the results of mapping the Applicant's Certificate Policy to the SAFE CP in order to establish its equivalency to the SAFE CP.

Activities:

1. The CCRA performs a mapping of the Applicant's CP to the SAFE CP. The Applicant will be required to provide a knowledgeable and authorized representative to the SAFE CCRA for the Certificate Policy mapping process evaluation. The SAFE CCRA reviews the Applicant's Certificate Policy and performs a formal mapping between the Applicant's CP and the SAFE CP. If additional information is needed, or if deficiencies are noted, the CCRA contractor works with the Applicant to resolve. When all deficiencies have been resolved and the CCRA is satisfied that the mapping is complete and accurate, CCRA staff prepares a Certificate Policy Mapping Report, and submits the report to both the SAFE CTO and the Applicant.
2. The CTO reviews the Certificate Policy Mapping Report to determine if there are areas of non-compliance with the SAFE CP and performs an assessment as to the need to amend the SAFE CP, the need to request amendments to the Applicant's CP, or the reasonableness of issuing a waiver for certain differences. Any recommended waiver may include a recommended timeframe for resolution of such differences. The CTO recommends one of the following:
 - a. Proceed without any CP amendments or waivers.
 - b. Proceed with recommended SAFE and/or Applicant CP amendments and recommended waivers.
3. The CTO informs the Applicant of the recommendation. If the recommendation is acceptable to the Applicant, the process may move to Phase III, Step 1 - Technical Interoperability Testing (if it has not already begun). If the recommendation is not acceptable to the Applicant, the Applicant and SAFE will jointly decide if the outstanding issues are resolvable, and whether or not to continue the cross certification process. Phase IV may not begin until the Applicant and SAFE mutually agree on the resolution to any such issues. The SAFE CTO will work to assure the continuing integrity and best interests of the overall SAFE System during any issue discussions.

2.3 Phase III - Testing

Step 1: Technical Interoperability Testing

Purpose:

To identify and resolve any incompatibilities between the Applicant's PKI technologies and those of the SBCA in order to minimize the risk of introducing potential incompatibilities with CAs already cross-certified with the Production SBCA. SAFE-BioPharma has established a SBCA Test Environment, collocated with the SBCA facility, which is available for interoperability testing purposes.

Activities:

1. If not already agreed, the Applicant agrees to pay any CCRA fees associated with technical interoperability testing.

2. The CCRA and the Applicant POC schedule a meeting to allow the SBCA OA and/or Technical Lead to introduce and identify participants in the process and to discuss the technical interoperability testing process.
3. The CCRA communicates with key personnel to confirm architectural and key POC information. This provides information on the technical configuration of the Applicant's PKI relative to its, and the SBCA's, ability to interoperate at a technical level. (The Applicant's CA may be either its intended production or test-bed CA. If it is the Applicant's test-bed CA, it must accurately represent the properties and specifications of the Applicant's production CA for the purposes of cross-certification.)
4. Having shared their respective technical data, the Applicant, the CCRA, and the SBCA OA undertake a test cross-certification with the test-bed SBCA. As this process is technology-dependent, it is not described here; however, it must demonstrate:
 - a. Successful exchange of PKI certificates
 - b. Directory interoperability
 - c. The ability of each party to validate the other's CA certificates and Cross Certificates
 - d. The ability to access the proper On-Line Certificate Status Protocol Responder (OCSP)
 - e. Appropriate validity and/or re-issuance periods for certificate revocation lists (CRLs), OCSP Responder certificates, CA certificates, and Subscriber certificates.
5. The CCRA documents the results of the test in an Interoperability Evaluation Report and forwards this report to both the CTO and the Applicant. The CTO reviews the Interoperability Evaluation Report and determines if there are areas of technical non-compliance with the SAFE System. The CTO performs an assessment as to the need to make changes to the SAFE System or documentation, the need to request changes to the Applicant's PKI or documentation, or the reasonableness of issuing a waiver for certain differences. Any recommended waiver may include a recommended timeframe for resolution of such differences. With respect to technical interoperability, the CTO recommends one of the following:
 - a. Proceed to Phase IV without any changes or waivers.
 - b. Proceed to Phase IV, with recommended changes and/or waivers.
6. The SAFE CTO prepares a decision brief for the SAFE Accreditation Council (AC) based on the recommendations developed in Phase II - Step 1 - Activity 2 and Phase III – Step 1 – Activity 5. The SAFE CTO provides the decision briefing, the Certificate Policy Mapping Report, and the Interoperability Evaluation Report to the SAFE AC.
7. The SAFE AC reviews the CTO recommendations and meets to decide whether to accept the recommendations.

The Chair of the SAFE AC opens the floor to questions from the AC membership pertaining to the CTO's recommendations. Once all questions have been addressed, the Chair calls for a vote on its recommendation to the SAFE PAA.

The SAFE AC may recommend one of four possible courses of action:

- a. Cross certify
 - b. Cross certify only with Applicant's written acceptance of any amendments, changes or waivers.
 - c. Stay the proceedings while resolving outstanding issues
 - d. Reject the cross-certification request
8. The SAFE AC forwards its recommended course of action to the SAFE Policy Approval Authority (PAA) for approval. The PAA reviews the recommended course of action and votes to approve one of the four possible courses of action.

If the PAA approves conditional acceptance of the cross-certification request, the SAFE PAA Chair directs the SAFE CTO to ask the Applicant to provide a written response within 30 calendar days of the date of the approval letter, or such other time as may be agreed.

- a. The Applicant is responsible for repeating any step(s) in the process necessitated by an approval for conditional acceptance.
- b. Following the resolution of any issues identified in the original letter of decision, the CTO generates a second letter of decision for the signature of the SAFE PAA Chair. Upon signature, the process moves to Phase IV - the Agreement Phase.

2.4 Phase IV – Agreement

Step 1: Completion of the SAFE-Issuer Agreement

Purpose:

- To negotiate the terms and conditions of the SAFE-Issuer Agreement.

Activities

1. In consultation with legal counsel, the SAFE PAA completes the SAFE-Issuer Agreement (Appendix C) with the Issuer.

Step 2: Issuance of Cross-Certificates

Purpose:

- To allow the Applicant and the SBCA OA to issue cross-certificates. Further guidance on this step is provided in the SAFE Bridge Cross Certification Procedures document. This document is provided by the SBCA Operational Authority (OA) to those Applicants successfully completing Phase III.

Activities

1. The Applicant submits a Cross Certification Request Letter on official letterhead to the SAFE CTO (Appendix D provides an example template). The letter requests the SBCA OA to perform cross certification and is signed by the senior official responsible for the operations of the Applicant Principal CA. The letter includes the following information:
 - a. Identification of key Applicant CA personnel, including primary and alternate technical and managerial contacts
 - b. Applicant's Policy OID(s) for inclusion in the cross certificate
 - c. Directory information tree for subject names in certificates issued by the Applicant (i.e., identification of permitted and excluded sub-trees)
 - d. Distinguished name of the Applicant CA
2. Following the receipt and review of the request letter from the Applicant, the SAFE CTO prepares a Letter of Authorization for PAA Chair signature to the SBCA OA (Appendix F), to initiate cross certification with the Applicant.
3. The SBCA OA reviews the Cross Certification Letter of Authorization.
4. The SAFE CTO, SBCA OA, and the Applicant POC determine an appropriate date for the cross-certification.
5. Following a satisfactory review of the technical data provided by both parties, the SBCA OA and the Applicant agree to issue cross-certificates and take the necessary procedural and technical steps to do so.
6. Appropriate notification concerning the cross-certification ceremony is provided to interested parties.
7. Upon completion of the cross-certification ceremony, the Applicant will officially be designated as a SAFE Issuer.

2.5 Phase V - Maintenance

Phase V Overview:

It is important to ensure that, once in place and for its duration, cross-certification continues to guarantee the agreed upon level of trust between the SBCA and each cross certified Issuer. Each cross-certification is governed by the SAFE-Issuer Agreement entered into in Phase IV. The Maintenance Phase provides mechanisms both for managing the relationship between cross-certified Certification Authorities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions, or at the desire of either party. The elements of this phase are not sequential and they will apply as circumstances warrant. Activities include:

- Compliance Review
- Problem Resolution
- Change Management
- Renewal or Termination.

Compliance Review

Purpose:

- To determine if the Cross Certified PKI is operating in compliance with its stated policies and practices.

Activities

The agreement between the parties will contain a number of actions which each party must undertake and provide to the other party as evidence of continued compliance with the agreement. Such actions include completion of an annual Issuer Self-Assessment Audit Checklist for SAFE Standard Compliance (see Appendix E) of the Applicant's cross certified PKI. The Cross Certified PKI shall submit the resulting Self-Assessment Audit report to the SAFE CTO. The CTO shall review the report and forward it, along with any recommendations for corrective action or continued cross certification to the SAFE AC. The SAFE AC shall ensure that all SAFE-BioPharma required actions are performed in a timely fashion, and that all required Issuer actions are submitted to SAFE in a timely fashion.

The audit shall include:

- A summary audit report indicating that CPS fulfills the requirements of the CP, and that PKI's operations follow its CPS
- A signed audit summary report containing:
 - Identification of the Applicant's PKI's operations evaluated for conformance to requirements of its CPS, and resultant findings
 - Statement that PKI's CPS conforms to the PKI's CP; and any resultant findings.

The auditor should provide:

- Their name, organization, and contact info
- A summary of his/her experience / qualifications / certifications in auditing PKI systems
- Relationship to Issuer (i.e., independence of auditor from part of Issuer operating or managing PKI)

1. The CTO prepares a Compliance Review Report and provides a copy to the SAFE AC Chair. This report is for internal SAFE-BioPharma use only. The Compliance Review Report will either:
 - a. Indicate no problem exists and recommend continuation of the affiliation unchanged;
 - b. Indicate any deficiencies and suggest corrective action, but recommend that the cross certified PKI continues to be cross-certified at its current assurance level;
 - c. Recommend renewal, but further recommend that the AC downgrade the assurance level of the cross certificate; or
 - d. Recommend that SAFE terminate the cross-certification.

2. The SAFE AC Chair reviews the report and forwards its recommendation to the PAA. The PAA will make the final decision and inform the SBCA OA, and other Cross Certified PKIs of the its decision.

Problem Resolution

Purpose:

- To report and correct problems the parties may encounter during the effective period of the cross-certification agreement.

Activities:

Either party to the cross-certification arrangement may notify the other of problems and request resolution. Problem resolution procedures are specific to the problem encountered and will be agreed upon between the parties.

Change Management

Purpose:

- To manage changes to the SBCA or Cross Certified PKI and to decide what actions to take as a result of implementing such changes.

Activities:

1. Either cross certified party may initiate this process. If either the SBCA or Cross Certified PKI is contemplating changes that impact the terms of the SAFE-Issuer Agreement, then a notice of the change, including specific changes to any documents or certificate structures, must be provided to the other party.
2. Each party reviews the notice and determines the appropriate response:
 - a. Unconditional acceptance of the proposed change(s);
 - b. Conditional acceptance, with follow-up required (the change is accepted but the next Compliance Review must pay particular attention to the change implementation); or
 - c. The change is found to be unacceptable.
3. If a change implemented to the infrastructure by one of the parties is deemed unacceptable to the other Members, such implementation may cause termination of the cross-certification arrangement.

Renewal and Termination

Purpose:

- To decide whether to renew or terminate an existing cross-certification arrangement, and to specify the process for either renewal or termination.

Activities (General):

Should the SBCA OA, or the SAFE CTO become aware of any information that indicates that there has been a failure in the integrity of the Cross Certified PKI that is deemed by

any of the Entities to have the potential to adversely affect the security of the SBCA and its other Cross Certified PKIs, then the SAFE PAA Chair, at his or her discretion, may instruct the SBCA OA to revoke the cross-certificate of the Cross Certified PKI. The SAFE PAA informs the Cross Certified PKI POC of the revocation. The SAFE PAA Chair then informs the SAFE PAA membership and other Cross Certified Certification Authorities of the revocation.

Activities for Renewal of Existing Arrangement with an External PKI

1. The SBCA OA provides the SAFE CTO with a Renewal Notice indicating the cross-certificate is due to expire, so the SAFE AC may make a determination concerning renewal or termination. The notice will contain a summary of all relevant issues and information from various documents, including:
 - a. The most recent Compliance Audit Report;
 - b. All Problem Resolution Reports since the arrangement was signed or last renewed; and
 - c. All Change Management Reports since the arrangement was signed or last renewed
2. The SBCA OA notifies the SAFE CTO 180 days before the expiration date of any cross certification arrangement, to provide the SAFE PAA time to consider whether to renew it.
3. The SAFE CTO contacts the Cross Certified PKI to ascertain whether there is interest in renewing the cross certification arrangement, and to seek any information the party may wish the SAFE AC to consider in its deliberations.
4. The SAFE PAA reviews the Renewal Notice and decides either to:
 - a. Recommend the SAFE PAA Chair renew the cross certification arrangement, for a specified period of time, with no changes; or
 - b. Enter into negotiations to revise the cross certification arrangement and, depending on the outcome of the negotiations, subsequently to recommend to the SAFE PAA Chair to execute the new cross certification arrangement.
 - c. Terminate the SAFE-Issuer Agreement.
5. If the SAFE PAA decides that the agreement be renewed with no changes, it informs the Cross Certified PKI.
6. If the SAFE PAA decides to negotiate a new agreement, it informs the Cross Certified PKI in writing. If the Cross Certified PKI wishes to proceed, then the usual procedures will apply.
7. If the SAFE PAA decides to terminate the agreement or the Cross Certified PKI declines the SAFE AC recommendation, the agreement will expire according to its own terms.

Activities for Cross Certified PKI Request for Termination of Agreement

1. Any party to an external cross certification agreement may submit a termination request at any time during the life of the agreement. The request must include the reason(s) for seeking termination, and the desired termination date.
2. The SAFE PAA, in consultation with the SBCA OA and the Cross Certified PKI's POC, determines a mutually agreeable termination date. The SBCA OA and the Cross Certified PKI carry out the appropriate termination procedures.
3. The SBCA OA notifies the SAFE PAA upon the completion of all termination procedures and the revocation of cross-certificates.
4. The SAFE PAA informs all Cross Certified PKIs of the withdrawal.

Activities for Cross Certified PKI's Removal from the SBCA

1. Pursuant to the SAFE-Issuer Agreement, the SAFE PAA may remove a Cross Certified PKI from the SBCA for cause. The SAFE PAA notifies the Cross Certified PKI in writing of this action, noting the reason(s) for removal and the termination date, as stipulated in the SAFE-Issuer Agreement.

3 CRITERIA FOR CROSS CERTIFICATION

3.1 General Principles

The full benefits of public key cryptography will be achieved through the widespread cross-certification of Public Key Infrastructures. However, given the need to carefully allocate resources within SAFE, some parameters must be established in order to prioritize cross-certification activities.

Note: It must be emphasized that cross-certification with the SAFE Bridge Certification Authority (SBCA) is not a right, nor should any discussions be considered a commitment to issue cross-certificates.

Certificates are issued and revoked at the sole discretion of the SAFE PAA. When the SBCA issues a cross-certificate it does so for the convenience of SAFE. Any review by the SBCA of another entity's certificate policy is for the use of the SBCA in determining whether or not interoperability is possible, and if possible, to what extent the other entity's certificate policy maps to the SBCA policy. Another entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of another entity's certificate policy by the SBCA is not a substitute for due care and mapping of certificate policies by the other entity.

Subject to this document, SAFE will consider applications for cross-certification from any organization or government operating a Certification Authority if such cross-certification is in support of SAFE initiatives, specifically to facilitate electronic business applications and operating programs that require digital signatures and secure authentication.

All applicants for cross-certification with the SBCA must obtain unique policy OIDs in the standard ISO object identifier registry from the appropriate commercial or national Registration Authority.

3.2 Conditions

At any point in the Cross-Certification Process with the exception of final approval or rejection (limited to PAA action), the SAFE AC will make a determination with respect to proceeding to the next step – at any stage of the process – with or without conditions. Proceeding to the next step with conditions means that the SAFE AC is of the opinion that some aspect of the Applicant's operational environment – based on a review of the documentation presented or test-bed results – indicates some concern as to whether the Applicant Certification Authority operates in an appropriately secure manner for the assurance level required. The creation and acceptance of conditions means that such concerns can be allayed with changes in the operations of the Applicant PKI and that such changes have to be made before any positive decision by the SAFE AC concerning cross-certification will be made.

A decision not to proceed means that the SAFE AC is of the view that the Applicant's PKI does not demonstrate that it can operate in a manner commensurate with one of the SBCA assurance levels.

3.2.1 *Initiation Phase*

Upon receipt of an Application for Cross Certification, the SAFE AC will make a preliminary determination as to whether the Application is complete and all required documentation, as set out in the instructions for the Application for Cross Certification, has been submitted. This determination will precede the SAFE AC's consideration of the Application.

A statement explaining why the Applicant is applying for cross-certification with the SBCA must accompany the Application. Applications will be signed by an appropriate senior official (an officer or executive) of the organization responsible for the PKI who is authorized to commit the organization to completing the cross-certification process. Such a commitment would include bearing any expenses incurred by the organization during the cross-certification process, and the authorization of any submission of information or statement required from the Applicant.

Generally, an Application will be considered if it is from:

1. A commercial organization doing, or with firm projections to do, business with one or more SAFE Members.
2. A non-commercial organization, if it will assist in the furtherance of the SAFE objectives.
3. A government entity whether national, state, local, or tribal, in the US or other country, where it would be in the interests of SAFE to cross-certify.

Applicants, unless otherwise exempted, must provide evidence of the current legal status of the entity responsible for the PKI. A certificate from the authorities of the jurisdiction in which the organization was created, indicating that the organization is in good standing under the laws of that jurisdiction, may be requested for this purpose.

Non-governmental applicants may be requested to provide evidence of financial capacity to manage risks associated with the operation of a PKI. Financial capacity can be demonstrated if the organization can provide a copy of a performance bond, a letter of credit from a financial institution, a letter indicating that insurance has been put in place, or a commitment letter from a bonding company, financial institution or insurance company.

The purpose of this requirement is to demonstrate the organization's ability to meet any financial responsibility associated with operating a Certification Authority, including any liability to subscribers or others relying on certificates issued and digital signatures verifiable by reference to public keys in such certificates. The nature and sufficiency of the required financial capacity will be determined at the discretion of the SAFE Policy Approval Authority on a case-by-case basis.

Legal status and financial capacity constitute some of the evidentiary requirements needed to lay a foundation of trust between SAFE and applicants.

Applicants exempted from these evidentiary requirements are:

- a. A state, local, or tribal government;
- b. A US or foreign national government; or
- c. Any other entity exempted from this requirement by the SAFE AC.

An Application will not be considered complete until the SAFE AC is satisfied that all relevant documentation, as set out in the requirements, has been submitted.

Generally, a recommendation to proceed shall be made if the SAFE AC is of the view that all of the following exist, demonstrating the ability of the applicant to manage a PKI and that the Applicant has;

- Certificate Policy (or equivalent) in place,
- Certification Practices Statement in place, and
- Security Policy (or equivalent) in place with respect to the protection of the Certification Authority;
- Compliance audit of the Applicant's Principal Certification Authority has been done;
- Processes are in place to enforce the Applicant's Certificate Policy
- Sufficient information, as identified in the Application for Cross Certification (see Appendix B), has been provided with respect to the technology used by the Applicant;
- The technology used by the Applicant is compatible with the technology employed by the SBCA and SAFE Relying Parties (i.e., standards compliant);
- The Applicant is seeking an appropriate level of assurance;
- Adequate information has been provided with respect to the legal status of the organization responsible for the Applicant's PKI;
- Adequate information has been provided with respect to the financial capacity of the Applicant and the financial capacity appears adequate for the operations of the Applicant PKI;

The Applicant must identify a representative to assist the SAFE CTO in evaluating its application. The applicant application will be evaluated for security, privacy, and operational considerations.

The Applicant must identify which of its Certificate Policies are to be considered for cross-certification with the SBCA. It must be recognized that the Certificate Policy and Certification Practices Statement may or may not be combined into one document (Certificate Policy/Certification Practices Statement). In any event, the SAFE CTO will examine specific elements within the Certificate Policy and evaluate the Applicant PKI as providing a level of assurance equivalent to a specific level identified in the SAFE Certificate Policy.

Certificate Policy documents may support multiple levels of assurance. Additional evaluation may be required to map the Applicant PKI to the appropriate level in the SAFE Certificate Policy.

An Applicant's Certificate Policy must follow a current or recent version of the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Presenting a Certificate Policy in this format expedites the comparison with the SAFE Certificate Policy. The SAFE CCRA will map the SAFE and Applicant certificate policies by category and element for consistency.

3.2.2 Policy Mapping Phase

Policy mapping is a process of comparing and contrasting the Applicant PKI Certificate Policy to the SAFE Certificate Policy and evaluating the extent to which the applicant PKI demonstrates

policies, practices and procedures consistent with those of the SBCA. The categories to be used are found in the Mapping Matrix. Any review of the Applicant PKI's Certificate Policy involves looking at each section of the document to determine whether each section is comparable or equivalent to its counterpart in the SAFE Certificate Policy.

Bear in mind that:

- a. There may be more than one section that applies for each element;
- b. There may be differences in section headings;
- c. Some certificate policies may have a different number of sub-fields for each element in the Certificate Policy;
- d. The Certificate Policy may refer to other documents such as the Certification Practices Statement. In this situation, if there is insufficient information present in the section, it must be flagged for additional consideration and further examination of the referenced documents;
- e. There may be differences in terminology and usage. For example, the term "trusted" may have specific implications to one organization that do not carry over when compared to another organization's Certificate Policy.

The results of the policy mapping exercise are recorded in the Mapping Matrix. All categories and elements that are not found in the Applicant PKI's Certificate Policy must be noted in the Mapping Matrix Brief Assessment. If there is a requirement for additional information to support or detail the comment, additional documentation may be used as long as the information is referenced correctly.

Policy mapping is a subjective exercise. Equal degrees of protection can be accomplished using different means. Policy mapping is an exercise to determine the "equivalency" between different means in order to establish that the policies provide a comparable degree of assurance (or to what degree they differ). Once this equivalency is established, the construction of cross-certificates, representing the trust placed by each PKI in the other, is performed. It is expected that the Applicant would also engage in a comparable policy mapping exercise to assure itself of the degree of assurance represented by the SAFE Certificate Policy in question. SAFE recommends including the results of the Applicant's CP mapping exercise as part of the Application process to facilitate subsequent discussions.

3.2.2.1 Evaluation of Applicant's Information Technology Security and Policy Compliance

Trustworthiness of an Applicant must be evaluated for the purposes of cross certification. This requires the Applicant implement a certificate policy enforcement process. A key element of the enforcement process must include independent compliance audits as defined in the Applicant PKI's Certificate Policy. Applicant must present evidence that their policy enforcement process is performed as stated. For example, evidence may include additional audit reports for various components of the Applicant PKI, such as subordinate Certification Authorities and Registration Authorities.

As Public Key Infrastructure/Certification Authority audit standards evolve and become more accepted, then adherence to an international standard, with verification through an independent audit performed by qualified auditors, may become a pre-requisite for cross certification with the SBCA. Given the absence of such standards at this time, audits will be accepted when

performed by independent third parties, with demonstrated knowledge of PKI systems using accepted auditing methodologies. Performance of a compliance audit on the Applicant PKIs Principal Certification Authority is a pre-requisite for cross certification with the SBCA. The compliance audit must demonstrate that the Principal Certification Authority is operated in accordance with its Certificate Policy and Certification Practices Statement. The Applicant must deliver a summary of the Principal Certification Authority's compliance audit report to the Policy Authority as part of its cross-certification application. Government entities may elect to use an Inspector General or other internal independent auditing capabilities to satisfy this requirement.

3.2.3 Test Phase

Technical interoperability testing is used to ensure technical interoperability between the SBCA and the Applicant's Principal Certification Authority. The objective is to determine whether there can be a successful exchange of cross-certificates and directory interoperability. The SBCA will not issue cross-certificates before successful completion of the interoperability tests. The SBCA OA operates the SBCA development/test system on behalf of the SAFE-BioPharma Association. It is configured to be a duplicate of the Production SBCA. The Applicants' Certification Authority technical personnel will be required to work with the CCRA to complete the technical interoperability testing.

An Applicant may use a test-bed facility, set and configured in a manner identical to its production Certification Authority (the Certification Authority to be permanently cross-certified with the SBCA), or may use its production Certification Authority for the technical interoperability testing. Any costs incurred by the Applicant Certification Authority resulting from technical interoperability testing will be the responsibility of the Applicant.

In preparing a technical interoperability report, the CCRA describes the results of the tests and provides it to the SAFE CTO.

At a minimum, the technical interoperability test will demonstrate:

- a. Network connectivity is achieved using all required protocols;
- b. The directories of the SBCA and the Applicant are interoperable;
- c. The cross-certificate is correctly constructed by the SBCA, and exchanged and recognized by the Applicant Certification Authority;
- d. The cross-certificate is correctly constructed by the Applicant Certification Authority, exchanged with the SBCA, and recognized by the SBCA;
- e. A test transaction, using a test subscriber of the Applicant PKI, can be successfully validated; and,
- f. The ability to share revocation information between the SBCA and the Applicant PKI.

The Report will also include a description of deficiencies identified during the test. Deficiencies may include technical interoperability deficiencies and potential performance issues that were not specifically identified by the test criteria. The report will also include the anticipated consequences of the deficiencies and a recommendation by the SBCA Operational Authority.

The successful completion of the technical interoperability test should complete the technical requirements for cross-certification.

3.2.4 Agreement Phase

3.2.4.1 Negotiation of Cross-Certification Agreement

The overall evaluation of the Applicant's PKI compliance involves an assessment of the information collected in the technical interoperability testing and the results of the policy mapping. If these results reveal the Applicant PKI meets the requirements of a SBCA assurance level, and the Applicant accepts these results, the SAFE AC may commence negotiations for the purpose of entering into a Cross Certification SAFE Issuer Agreement.

The relationship between SAFE-BioPharma Association and an organization operating a PKI will be governed by the SAFE-Issuer Agreement to be signed by the SAFE PAA Chair on the recommendation of the SAFE AC. Any SAFE AC recommendation to do so follows a sufficient examination of an Applicant application and the negotiation of a draft SAFE-Issuer Agreement in a form suitable to the SAFE AC and CTO. The Applicant PKI cognizant authority must also sign the agreement.

An assessment to determine whether an agreement is in a suitable form cannot be undertaken in the abstract. A model SAFE Issuer Agreement, intended as a guide, is available at Appendix C. Deviations from this model, while not preferred, may be necessary to achieve agreement.

3.2.4.2 Relationship Maintenance, Continuation and Termination

Upon execution of a SAFE-Issuer Agreement and the issuance of cross-certificates, SAFE-BioPharma and the Applicant (now Cross Certified) PKI enter into a relationship subject to periodic review. The agreement will specify the period for review.

The SAFE PAA may terminate the agreement and revoke the cross certificate when it determines the cross certification is no longer in SAFE-BioPharma interests.

Appendix A: SAFE Certificate Policy Mapping Matrix

The following scoring guideline shall be used in Certificate Policy mapping:

- Equivalent – When the SAFE CP and the Issuer CP have same or roughly the same requirement language.
- Comparable – When the SAFE CP and the Issuer CP have similar requirement language or when the different requirement language provide equivalent assurance.
- **Does not comply** – When the Issuer CP does not address all the topics in SAFE CP, when the Issuer CP is not as stringent as the SAFE CP, or when the Issuer CP requirement can not be compared to the SAFE CP requirement.
- Complies – When the SAFE CP imposes no requirement on the Issuer CP.
- Exceeds – When the Issuer CP requirement exceeds the SAFE CP requirements

The above scoring is done for each lowest level of section in the SAFE CP.

If the Issuer CP is rated as "**Does not comply**" in an area, a rationale for non-compliance is provided.

If there is a separation of CP responsibilities across several service providers (e.g., separation of Certification Authority and Registration Agent functions), identify the other service provider(s) in the CP Mapping Verdict column. It is recommended that all such service providers collaborate in the CP mapping process.

Once the Issuer CP passes or the Issuer decides to make no more changes, the final mapping and recommendation is submitted to SAFE-BioPharma.

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
1.0	Introduction		
1.1	Overview		
1.1.1	Certificate Policy (CP)		
1.1.2	Relationship between the SAFE CP & the SBCA CPS		
1.1.3	Relationship between the SAFE CP and the Issuer CP		
1.1.4	Relationship between the SAFE CP and the SAFE Standard		
1.1.5	Scope		
1.1.6	Interaction with PKIs External to SAFE		
1.2	Identification		
1.3	PKI Entities		
1.3.1	PKI Authorities		
1.3.1.1	SAFE Policy Approval Authority (PAA)		
1.3.1.2	SBCA Operational Authority (SBCA OA)		
1.3.1.3	SBCA OA Program Manager		
1.3.1.4	SAFE Bridge Certification Authority (SBCA)		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
1.3.1.5	Issuer Principal Certification Authority (CA)		
1.3.1.6	Issuer Certification Authority (CA)		
1.3.2	Registration Authority (RA)		
1.3.3	Subscribers		
1.3.4	Relying Parties		
1.3.5	Other Participants		
1.3.5.1	Local Registration Authority (LRA)		
1.3.5.2	Trusted Agent (TA)		
1.3.5.3	Certificate Status Authority (CSA)		
1.3.5.4	Machine Operator		
1.4	Certificate Usage		
1.4.1	Appropriate Certificate Uses		
1.4.2	Prohibited Certificate Uses		
1.5	Policy Administration		
1.5.1	Issuer Administering the Document		
1.5.2	Contact Person		
1.5.3	Person Determining CPS Suitability for the Policy		
1.5.4	CPS Approval Procedures		
2.0	Publication & Repository Responsibilities		
2.1	Repositories		
2.1.1	Repository Obligations		
2.2	Publication of Certification Information		
2.2.1	Publication of Certificates and Certificate Status		
2.2.2	Publication of CA Information		
2.2.3	Interoperability		
2.3	Frequency of Publication		
2.4	Access Controls on Repositories		
3.0	Identification & Authentication		
3.1	Naming		
3.1.1	Types of Names		
3.1.2	Need for Names to be Meaningful		
3.1.3	Anonymity or Pseudonymity of Subscribers		
3.1.4	Rules for Interpreting Various Name Forms		
3.1.5	Uniqueness of Names		
3.1.6	Recognition, Authentication, & Role of Trademarks		
3.2	Initial Identity-proofing		
3.2.1	Method to Prove Possession of Private Key		
3.2.2	Authentication of Issuer Identity		
3.2.3	Identity-Proofing of Individual Identity		
3.2.3.1	Identity-Proofing of End User Subscribers		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
3.2.3.2	Identity-Proofing of Machine Subscribers		
3.2.4	Non-verified Subscriber Information		
3.2.5	Validation of Authority		
3.2.6	Criteria for Interoperation		
3.3	Identification and Authentication for Re-key Requests		
3.3.1	Identification and Authentication for Routine Re-key		
3.3.2	Identification and Authentication for Re-key after Revocation		
3.4	Identification and Authentication for Revocation Requests		
4.0	Certificate life-cycle		
4.1	Application		
4.1.1	Submission of Certificate Application		
4.1.2	Enrollment Process and Responsibilities		
4.2	Certificate Application Processing		
4.2.1	Performing Identity-proofing Functions		
4.2.2	Approval or Rejection of Certificate Applications		
4.2.3	Time to Process Certificate Applications		
4.3	Issuance		
4.3.1	CA Actions During Certificate Issuance		
4.3.2	Notification to Subscriber of Certificate Issuance		
4.4	Acceptance		
4.4.1	Conduct Constituting Certificate Acceptance		
4.4.2	Publication of the Certificate by the CA		
4.4.3	Notification of Certificate Issuance by the CA to Other Entities		
4.5	Key Pair and Certificate Usage		
4.5.1	Subscriber Private Key and Certificate Usage		
4.5.2	Relying Party Public Key and Certificate Usage		
4.6	Certificate Renewal		
4.6.1	Circumstance for Certificate Renewal		
4.6.2	Who May Request Renewal		
4.6.3	Processing Certificate Renewal Requests		
4.6.4	Notification of New Certificate issuance to Subscriber		
4.6.5	Conduct Constituting Acceptance of a Renewed Certificate		
4.6.6	Publication of the Renewal Certificate by the CA		
4.6.7	Notification of Certificate Issuance by the CA to Other Entities		
4.7	Certificate Re-Key		
4.7.1	Circumstance for Certificate Re-key		
4.7.2	Who May Request Certification of a New Public Key		
4.7.3	Processing Certificate Re-keying Requests		
4.7.4	Notification of New Certificate Issuance to Subscriber		
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
4.7.6	Publication of the Re-keyed Certificate by the CA		
4.7.7	Notification of Certificate Issuance by the CA to Other Entities		
4.8	Certificate Modification		
4.8.1	Circumstance for Certificate Modification		
4.8.2	Who May Request Certificate Modification		
4.8.3	Processing Certificate Modification Requests		
4.8.4	Notification of New Certificate Issuance to Subscriber		
4.8.5	Conduct Constituting Acceptance of Modified Certificate		
4.8.6	Publication of the Modified Certificate by the CA		
4.8.7	Notification of Certificate Issuance by the CA to Other Entities		
4.9	Revocation & Suspension		
4.9.1	Circumstance for Revocation of a Certificate		
4.9.2	Who Can Request Revocation of a Certificate		
4.9.3	Procedure for Revocation Request		
4.9.4	Revocation Request Grace Period		
4.9.5	Time within which CA must Process the Revocation Request		
4.9.6	Revocation Checking Requirements for Relying Parties		
4.9.7	CRL Issuance Frequency		
4.9.8	Maximum Latency of CRLs		
4.9.9	Online Revocation Checking Availability		
4.9.10	Online Revocation Checking Requirements		
4.9.11	Other Forms of Revocation Advertisements Available		
4.9.11.1	Checking Requirements for Other Forms of Revocation Advertisements		
4.9.12	Special Requirements Related To Key Compromise		
4.9.13	Circumstances for Suspension		
4.9.14	Who can Request Suspension		
4.9.15	Procedure for Suspension Request		
4.9.16	Limits on Suspension Period		
4.10	Certificate Status Services		
4.10.1	Operational Characteristics		
4.10.2	Service Availability		
4.10.3	Optional Features		
4.11	End of Subscription		
4.12	Key Escrow & Recovery		
4.12.1	Key Escrow and Recovery Policy and Practices		
4.12.2	Session Key Encapsulation and Recovery Policy and Practices		
5.0	Facility Management & Operations Controls		
5.1	Physical Controls		
5.1.1	Site Location & Construction		
5.1.2	Physical Access		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
5.1.3	Power and Air Conditioning		
5.1.4	Water Exposures		
5.1.5	Fire Prevention & Protection		
5.1.6	Media Storage		
5.1.7	Waste Disposal		
5.1.8	Off-Site backup		
5.2	Procedural Controls		
5.2.1	Trusted Roles		
5.2.1.1	CA Administrator		
5.2.1.2	CA Agent		
5.2.1.3	CA Auditor		
5.2.1.4	CA Operator		
5.2.1.5	CSA Administrator		
5.2.1.6	CSA Auditor		
5.2.1.7	Registration Authority (RA)		
5.2.1.8	Local Registration Authority (LRA)		
5.2.1.9	Trusted Agent (TA)		
5.2.1.10	Machine Operator		
5.2.2	Number of Persons Required per Task		
5.2.3	Identity-proofing for Each Role		
5.2.4	Separation of Roles		
5.3	Personnel Controls		
5.3.1	Background, Qualifications, Experience, & Security Clearance Requirements		
5.3.2	Background Check Procedures		
5.3.3	Training Requirements		
5.3.4	Retraining Frequency & Requirements		
5.3.5	Job Rotation Frequency & Sequence		
5.3.6	Sanctions for Unauthorized Actions		
5.3.7	Contracting Personnel Requirements		
5.3.8	Documentation Supplied To Personnel		
5.4	Audit		
5.4.1	Types of Events Recorded		
5.4.2	Frequency of Processing Data		
5.4.3	Retention Period for Security Audit Data		
5.4.4	Protection of Security Audit Data		
5.4.5	Security Audit Data Backup Procedures		
5.4.6	Security Audit Collection System (Internal or External)		
5.4.7	Notification to Event-Causing Subject		
5.4.8	Vulnerability Assessments		
5.5	Archive		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
5.5.1	Types of Events Archived		
5.5.2	Retention Period for Archive		
5.5.3	Protection of Archive		
5.5.4	Archive Backup Procedures		
5.5.5	Requirements for Time-Stamping of Records		
5.5.6	Archive Collection System (Internal or External)		
5.5.7	Procedures to Obtain & Verify Archive Information		
5.6	Key Changeover		
5.7	Compromise & Disaster Recovery		
5.7.1	Incident and Compromise Handling Procedures		
5.7.2	Computing Resources, Software, and/or Data Are Corrupted		
5.7.3	CA Private Key Compromise Recovery Procedures		
5.7.4	Business Continuity Capabilities after a Disaster		
5.8	CA & RA Termination		
5.8.1	CA Termination		
5.9	RA Termination		
6.0	Technical Security Controls		
6.1	Key Pair Generation & Installation		
6.1.1	Key Pair Generation		
6.1.2	Private Key Delivery to Subscriber		
6.1.3	Public Key Delivery to Certificate Issuer		
6.1.4	CA Public Key Delivery to Relying Parties		
6.1.5	Key Sizes		
6.1.6	Public Key Parameters Generation and Quality Checking		
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field)		
6.2	Private Key Protection & Crypto-Module Engineering Controls		
6.2.1	Cryptographic Module Standards & Controls		
6.2.2	CA Private Key Multi-Person Control		
6.2.3	Private Key Escrow		
6.2.4	Private Key Backup		
6.2.4.1	Backup of CA Signing Private Key		
6.2.4.2	Backup of Subscriber Signing Private Keys		
6.2.5	Private Key Archival		
6.2.6	Private Key Transfer into or from a Cryptographic Module		
6.2.7	Private Key Storage on Cryptographic Module		
6.2.8	Method of Activating Private Keys		
6.2.9	Methods of Deactivating Private Keys		
6.2.10	Method of Destroying Private Keys		
6.2.11	Cryptographic Module Rating		
6.3	Other Aspects of Key Management		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
6.3.1	Public Key Archive		
6.3.2	Certificate Operational Periods and Key Usage Periods		
6.4	Activation Data		
6.4.1	Activation Data Generation & Installation		
6.4.2	Activation Data Protection		
6.4.3	Other Aspects of Activation Data		
6.5	Computer Security Controls		
6.5.1	Specific Computer Security Technical Requirements		
6.5.2	Computer Security Rating		
6.6	Life-Cycle Security Controls		
6.6.1	System Development Controls		
6.6.2	Security Management Controls		
6.6.3	Life Cycle Security Ratings		
6.7	Network Security Controls		
6.8	Time Stamping		
7.0	Certificate, CRL, and OCSP Profiles		
7.1	Certificate Profile		
7.1.1	Version Numbers		
7.1.2	Certificate Extensions		
7.1.3	Algorithm Object Identifiers		
7.1.4	Name Forms		
7.1.5	Name Constraints		
7.1.6	Certificate Policy Object Identifier		
7.1.7	Usage of Policy Constraints Extension		
7.1.8	Policy Qualifiers Syntax & Semantics		
7.1.9	Processing Semantics for the Critical Certificate Policy Extension		
7.2	CRL Profile		
7.2.1	Version Numbers		
7.2.2	CRL & CRL Entry Extensions		
7.3	OCSP Profile		
7.3.1	Version Number		
7.3.2	OCSP Extensions		
8.0	Compliance Audit & Other Assessments		
8.1	Frequency Of Audit Or Assessments		
8.2	Identity & Qualifications Of Assessor		
8.3	Assessor's Relationship To Assessed Entity		
8.4	Topics Covered By Assessment		
8.5	Actions Taken As A Result Of Deficiency		
8.6	Communication of Results		
9.0	Other Business & Legal Matters		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
9.1	Fees		
9.1.1	Certificate Issuance/Renewal Fee		
9.1.2	Certificate Access Fees		
9.1.3	Revocation or Status Information Access Fee		
9.1.4	Fees for Other Services		
9.1.5	Refund Policy		
9.2	Financial Responsibility		
9.2.1	Insurance Coverage		
9.2.2	Other Assets		
9.2.3	Insurance/warranty Coverage for End-Entities		
9.3	Confidentiality of Business Information		
9.3.1	Scope of Confidential Information		
9.3.2	Information not within the Scope of Confidential Information		
9.3.3	Responsibility to Protect Confidential Information		
9.4	Privacy of Personal Information		
9.4.1	Privacy Plan		
9.4.2	Information treated as Private		
9.4.3	Information not deemed Private		
9.4.4	Responsibility to Protect Private Information		
9.4.5	Notice and Consent to Use Private Information		
9.4.6	Disclosure Pursuant to Judicial/Administrative Process		
9.4.7	Other Information Disclosure Circumstances		
9.5	Intellectual Property Rights		
9.6	Representations & Warranties		
9.6.1	CA Representations and Warranties		
9.6.2	RA Representations and Warranties		
9.6.3	Subscriber Representations and Warranties		
9.6.4	Relying Parties Representations and Warranties		
9.6.5	Representations and Warranties of other Participants		
9.6.5.1	Repository Representations and Warranties		
9.6.5.2	CSA Obligations		
9.7	Disclaimers Of Warranties		
9.8	Limitations of Liability		
9.9	Indemnities		
9.10	Term & Termination		
9.10.1	Term		
9.10.2	Termination		
9.10.3	Effect of Termination and Survival		
9.11	Individual Notices & Communications		
9.12	Amendments		

SAFE CP Section	Section Title	Issuer CP Section	CP Mapping Verdict
9.12.1	Procedure for Amendment		
9.12.2	Notification Mechanism and Period		
9.12.3	Circumstances under which OID must be changed		
9.13	Dispute Resolution Provisions		
9.14	Governing Law		
9.15	Compliance with Applicable Law		
9.16	Miscellaneous Provisions		
9.16.1	Entire agreement		
9.16.2	Assignment		
9.16.3	Severability		
9.16.4	Enforcement (Attorney Fees/Waiver of Rights)		
9.16.5	Force Majeure		
9.17	Other Provisions		
9.17.1	Fiduciary relationships		
9.17.2	Administrative processes		
10.0	Certificate, CRL, and OCSP Formats		
10.1	SBCA → Principal CA Certificate		
10.2	Principal CA → SBCA Certificate		
10.3	Issuer CA Certificate		
10.4	Subscriber Signature Certificate		
10.5	Subscriber Encryption Certificate (included for reference purposes)		
10.6	OCSP Responder Certificate		
10.7	CRL Format		
10.8	OCSP Request Format		
10.9	OCSP Response Format		
11.0	Directory Interoperability Profile		
11.1	Protocol		
11.2	Authentication		
11.3	Naming		
11.4	Object Class		
11.5	Attributes		
12.0	References		
13.0	Acronyms & Abbreviations		
14.0	Glossary		
15.0	SAFE Standard Applicability to the SAFE CP		

Appendix B: Application for Cross Certification

Instructions for Completing the Application for Cross Certification with the SBCA

Applicant should submit the information requested either using separate pieces of paper, or in an electronic format. In addition to the requested application information, the Applicant must submit one copy of each document listed below:

- a. Applicant's Certificate Policy
- b. Redacted version of Certification Practices Statement
- c. Applicant's completed CP mapping matrix (optional)
- d. Copy of latest audit report results (optional, if available)

Submit all documents in both writing (hardcopy/wet signature) and electronically to the Chief Technical Officer (CTO) of the SAFE-BioPharma Association (i.e., the delegated SAFE PAA point of contact for cross certification activities) The physical copy may be sent to the attention of the SAFE CTO at the address shown on the SAFE website (<http://www.safe-biopharma.org>) under the "Contact Us" tab. The items associated with the electronic copy must be in a format compatible with Adobe Reader or Microsoft Office, and should be sent to Bridge@safe-biopharma.org.

1. INFORMATION ON THE APPLICANT'S ORGANIZATION

- Applicant Organization Name
- Applicant Organization Address
- Applicant Organization's Representative or Designated Agent:
 - Name and Title
 - Postal Address with Zip Code
 - Office Phone Number
 - Office E-mail Address
- Applicant Organization's Secondary Contact(s) (to be used if Representative or Designated Agent cannot be reached):
 - Name(s) and Title(s)
 - Postal Address with Zip Code
 - Office Phone Number
 - Office E-mail Address

2. **INFORMATION ON THE APPLICANT'S CERTIFICATE POLICY AND CERTIFICATION PRACTICES STATEMENT**

(The Applicant's Certificate Policy and Certification Practices Statement for the Certification Authority to be cross-certified with the SBCA (hereinafter referred to as the "Principal CA"), must be attached for this application to be considered. The Applicant may also include any other relevant documentation deemed appropriate.)

Please indicate whether the attached Certificate Policy conforms with the X.509 standard and is RFC 3647 format. If not, please explain how the Certificate Policy differs from the X.509 standard, and how its contents map to the elements contained in the RFC 3647 format.

Answer: (indicate here whether the Applicant's CP and CPS are written in compliance with RFC 3647 format)

For the Principal CA, please ensure the following information is provided either as part of the CP, CPS or separately:

- a. Principal CA product employed including configuration information

Answer: (identify the CA application software and any associated support software such as OCSP responder applications)

- b. Principal CA hardware platform including operating system configuration

Answer: (identify the CA hardware platforms and associated operating systems)

- c. Signature and encryption algorithms supported

Answer: (identify CA's ability to support SHA1 with RSA signature algorithm; SHA-256 with RSA signature algorithm; one or more of DES, 3DES and AES encryption algorithms)

- d. Directory product employed including configuration information

Answer: (identify the directory software used by the CA; indicate support for LDAP and/or HTTP)

3. INFORMATION ON THE APPLICANT'S PKI ARCHITECTURE

For applications involving interoperability at the "Basic" or "Medium" levels of assurance (as defined in the SAFE CP, Sections 1.1 and 1.2):

- a. Provide a list of those CAs under the Applicant's control which are either subordinate to, or have any other trust relationship with, the Applicant's Principal CA. If any of those CAs provides certificates asserting object identifiers not covered in the attached CP, provide a copy of the relevant CP under which those OIDs are defined.

Answer: *(identify the CA hierarchy in use; identify any existing cross certificates with other PKIs)*

- b. Provide a list of those CAs not under the Applicant's control which have any trust relationship (e.g., cross-certificate) with the Applicant's Principal CA or any CA under the Applicant's control that is subordinate to, or has any other trust relationship with, the Applicant's Principal CA.

Answer: *(identify any existing cross certificates with other PKIs)*

- c. Briefly describe each application within the Applicant's organization currently supported by the Applicant's PKI as encompassed within the attached CP and CPS. This should include any CAs under the control of the Applicant which are subordinate to or have any other trust relationship with the Applicant's Principal CA.

Answer: *(identify any other PK-enabled applications or services supported)*

4. INFORMATION ON APPLICANT'S DIRECTORY ARCHITECTURE

Describe the Applicant's directory structure and how the Applicant will accomplish interoperability with the SBCA directory. For applications involving interoperability at the "Basic" or "Medium" levels of assurance, describe how the Applicant will ensure proper namespace control for distinguished naming.

Answer: *(identify directory / certificate accessibility from the Internet; identify current namespace control approaches)*

5. INFORMATION ON THE APPLICANT'S AUDITING PRACTICES

For applications involving interoperability at the "Basic" or "Medium" levels of assurance, describe how the Principal CA, and any other CA under the control of the Applicant

which is subordinate to or has any other trust relationship with the Principal CA, is audited. This should include who performs the audits, and their frequency. Attach a copy of the latest audit report attesting to compliance with the Applicant's CP and CPS.

Answer: (identify current audit processes and frequency of audit for primary CA operations and systems)

6. **INFORMATION ON CERTIFICATE POLICY MAPPING**

State what mapping(s) the Applicant proposes between the certificate levels of assurance covered under the Applicant's CP, and those set forth in the SAFE CP. For any proposed mapping at the "Basic" or "Medium" levels of assurance, explain the basis for the proposed mapping(s) by comparing the two CPs and providing whatever other information the Applicant deems relevant.

Answer: (identify at which assurance level(s) you plan to cross certify; identify the Principal CA that would cross certify with the SBCA)

7. **INFORMATION ON TECHNICAL CONFIGURATION**

For applications involving interoperability at the "Basic," or "Medium" levels of assurance:

- a. Please indicate whether the Applicant's Principal CA, and any other CA under the control of the Applicant which is subordinate to or has any other trust relationship with the Principal CA, employs digital signature key generation and signing operations in a hardware cryptographic module meeting FIPS 140, and if so, at what level of assurance. If a module is used that does not meet FIPS 140, please describe in detail the nature of the module and why it should be considered as acceptable.

Answer: (identify the HSM hardware in use; confirm that each of CAs HSMs conform with FIPS 140-2 Level 3)

- b. Please indicate whether the Applicant is producing or has the ability to produce certificates conforming to the SAFE-BioPharma Association PKI Certificate Profile respecting extensions in the SAFE CP and the SAFE Certificate, CRL and OCSP Profiles Guidance document.

Answer: (confirm ability to issue certificates conforming to SAFE certificate profile requirements and guidance)

- c. Please indicate which algorithms are used by the Applicant's Principal CA, and any other CA under the control of the Applicant which is subordinate to or has any trust relationship with the Principal CA, for signature and encryption. Please indicate whether the signature algorithms are executed in conformance with FIPS 186; if not, please explain how they are performed so as to provide a comparable or superior level of assurance.

Answer: (confirm support for RSA signatures algorithm in compliance with FIPS 186-2; confirm support for SHA1 hashing algorithm in compliance with FIPS 180-1; indicate support for SHA-256 hashing algorithm)

The above information is true and correct to the best of my knowledge and belief.

Signed: _____ Date: _____

Applicant's Authorized Official
(Print name and title)

Appendix C: SAFE-Issuer Agreement

THIS SAFE ISSUER AGREEMENT (this "Agreement") is between SAFE-BioPharma, Association, a Delaware limited liability company ("SAFE") and the entity executing this Agreement below as "Issuer." In consideration of the mutual promises in this Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, SAFE 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 System Documentation Glossary" contained in the current version of the SAFE Standard Document Set in effect as of the signing of this Agreement.
2. Standards and Operating Policies. All of the provisions of the documentation comprising the current version of the SAFE Standard Document Set in effect as of the signing of this Agreement, and as may be amended by SAFE, 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 Operating Policies." Issuer hereby agrees to abide by all of the terms and conditions of such documentation that are applicable to SAFE Issuers.
3. Term and Termination. This Agreement shall be effective as of the date SAFE executes this Agreement and shall continue until Issuer is suspended or terminated in accordance with Section 2.5 of that certain document entitled "SAFE Cross Certification Process" contained in the current version of the SAFE Standard Document Set in effect as of the signing of this Agreement, and as may be amended by SAFE in future periods. The provisions of Sections 4 and 5 of this Agreement shall survive any termination of this Agreement.
4. Notices. All notices, requests, consents, approvals, agreements, authorizations, acknowledgments, waivers and other communications required or permitted under the SAFE Operating Policies shall be delivered to the respective address of each Party as indicated below, or such other address as such Party last provided to the other Party by written notice.
5. Fees. Issuer agrees to promptly pay SAFE any annual certification fees, other fees or expenses invoiced to the Issuer by SAFE according to its published fee schedule as attached in Annex A and as modified from time to time by the SAFE Board. SAFE shall provide Issuer with written notice of changes to published fees with a minimum of 60 days notice prior to their taking affect.
6. Miscellaneous.
 - a. Entire Agreement. This Agreement, together with the documentation comprising the current version of the SAFE Standard Document Set in effect as of the signing of this Agreement and as may be amended by SAFE, 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 SAFE Operating Policies.

c. Assignment; Binding Effect. Assignment of this Agreement shall be governed by the SAFE 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.

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

SAFE-BioPharma, Association

Issuer

By: _____
Name: _____
Title: _____
Date: _____
Address: _____

By: _____
Name: _____
Title: _____
Date: _____
Address: _____

Annex A

**SAFE-BioPharma, Association
Accredited Issuer Fee Schedule – January, 2006**

Initial Accredited Issuer Certification Fee (1):	\$10,000
Annual Accredited Issuer Certification Fee (1)(2):	\$ 3,000
Cross Certification Audit Review (CCRA) Fees (3):	
- Certificate Policy Mapping (4)	CCRA List Price
- Interoperability Testing & Evaluation (4)	CCRA List Price
- Remediation Consulting Support	CCRA List Price
- Issuer Training	CCRA List Price
Periodic SAFE Bridge Cross-Certification Fees (5):	
- Initial Cross-Certification	no-charge
- Cross-Certificate Revocation	Time & Materials plus 8%
- Cross-Certificate Re-Issuance	Time & Materials plus 8%
Compliance Exception Audit Fees (5)(6):	
- Compliance Exception Audit	Time & Materials plus 8%

NOTES:

- (1) Fee payment is due to SAFE-BioPharma within 30 days of receipt of Invoice.
- (2) This annual fee is assessed as of the first anniversary of the signed SAFE Issuer Agreement and yearly thereafter for the life of the Agreement.
- (3) These services are all available through the SAFE CCRA contractor.
- (4) These services are required for initial cross-certification.
- (5) Fees will be assessed on a pass through cost basis.
- (6) These fees are only applicable in the event of a perceived compliance issue on the part of SAFE-BioPharma, and are only as necessary to properly assess and resolve any substantive compliance exceptions.

Appendix D: Applicant Cross Certification Request Letter Template

To	SBCA OA Manager
Subject	Letter of Request for Cross-Certification with SBCA
Request	<Applicant> requests to cross certify with the SAFE Bridge Certification Authority (SBCA) and confirms its readiness to proceed with the cross certification process.

APPLICANT INFORMATION	
Applicant	<applicant name>
Applicant CA Location	<address of applicant CA>
URL for Applicant Certificate Directory	<URL>
URL for Applicant OCSP Responder(s)	<URL 1> <URL 2> <URL n>
Applicant Personnel Participating in Cross-Certificate Ceremony	<name 1>, <title> <name 2>, <title> <name n>, <title>
Applicant Principal Point of Contact (POC)	<name> Title: <title> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
Applicant Alternate Point of Contact (POC)	<name> Title: <title> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
Authentication Password for Applicant POCs	<password>

APPLICANT KEY PERSONNEL INFORMATION	
<Role 1>	<name> Citizenship: <country> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
<Role 2>	<name> Title: <title> Citizenship: <country> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
<Role n>	<name> Title: <title> Citizenship: <country> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>

CROSS CERTIFICATE INFORMATION	
Validity Period	10 years
Cryptographic Algorithm & Key Size	RSA encryption with 1024 bits
Medium Assurance Policy Mapping	Applicant OID: SAFE OID: 1.3.6.1.4.1.23165.1.3
Basic Assurance Policy Mapping (optional)	Applicant OID: SAFE OID: 1.3.6.1.4.1.23165.1.2
Applicant CA Distinguished Name	
Applicant CA Permitted & Excluded Sub-Trees	
Maximum Number of Sub-CAs in Applicant CA's Trust Path (path length)	

APPROVAL			
Signature		Date	
By		Title	

Appendix E: CA Self-Assessment Audit Checklist

SAFE Issuer Self Assessment

Yes – The SAFE Issuer fully meets the acceptance criteria.

No – The SAFE Issuer does not meet the acceptance criteria in any way.

Partly – The SAFE Issuer meets the acceptance criteria to some extent, but not completely.

SAFE Issuer Acceptance Criteria	Assessment	Comments
Is there a currently signed legal agreement between the SAFE Issuer and SAFE? (Current SAFE Issuers Only)		
Does the SAFE Issuer have an Issuer Agent?		
Does the SAFE Issuer have documentation describing the designation, role, and responsibilities of an Issuer Agent?		
Does the SAFE Issuer include the organization attribute as part of the SAFE Issuer distinguished name?		
Does the SAFE Issuer use distinguished subject names in conformance with X.501 or X.520 naming conventions?		
Does the SAFE Issuer have a Subscriber Certificate validity period that does not exceed five (5) years?		
Does the SAFE Issuer use a subject public key based on RSA encryption algorithm with at least 1024-bit encryption?		
Does the SAFE Issuer include an RFC 822 format Internet Mail "addr-spec" address in the subject alternative name extension as a non-critical extension?		
Does the SAFE Issuer include CRL distribution points extensions as non-critical extensions when the CA that issues the Digital Certificate also exposes and publishes a CRL for external use?		
Does the SAFE Issuer include the authority information access extensions with a registered object identifier (OID) for the CA's SAFE Certificate Policy?		
Do the SAFE Issuer's CA Digital Certificates conform to RFC 3280 profiles and X.509 version 3?		
Do the SAFE Issuer's CA Digital Certificates mark as critical only those extensions designated as critical by SAFE?		
Do the SAFE Issuer's CA Digital Certificates use SHA-1 with RSA encryption as the signature algorithm?		
Do the SAFE Issuer's CA Digital Certificates employ distinguished organization attributes as part of the SAFE Issuer's distinguished name?		
Do the SAFE Issuer's CA Digital Certificates employ distinguished subject name in conformance with X.501 or X.520 naming conventions?		

SAFE Issuer Acceptance Criteria	Assessment	Comments
Do the SAFE Issuer's CA Digital Certificates include the organization attribute as part of the subject distinguished name?		
Do the SAFE Issuer's CA Digital Certificates have a validity of less than 10 years if established after May 31, 2004 or 20 years if established before May 31, 2004?		
Does the SAFE Issuer's Root CA include key usage extension as a critical extension?		
Does the SAFE Issuer's CA or subordinate CA include key usage extension as a critical extension?		
Does the SAFE Issuer's CA include basic constraints as a critical constraint?		
Does the SAFE Issuer's CA include certificate policies as a non-critical extension and identify the Subject as a CA?		
Responder Digital Certificates		
Do the SAFE Issuer's Responder Digital Certificates conform to RFC 3280 profiles and X.509 version 3?		
Do the SAFE Issuer's Responder Digital Certificates mark as critical only the extensions listed by SAFE as critical?		
Do the SAFE Issuer's Responder Digital Certificates use SHA-1 with RSA encryption as the signature algorithm?		
Do the SAFE Issuer's Responder Digital Certificates employ distinguished issuer name in conformance with X.501 or X.520 naming conventions?		
Do the SAFE Issuer's Responder Digital Certificates employ distinguished organization attributes as part of the SAFE Issuer distinguished name?		
Do the SAFE Issuer's responder Digital Certificates employ distinguished organization attributes as part of the subject distinguished name?		
Do the SAFE Issuer's responder Digital Certificates have a validity of less than 2 years?		
Do the SAFE Issuer's responder Digital Certificates include key usage extension as a critical extension?		
Do the SAFE Issuer's responders Digital Certificates include Certificate Policies extension as a non-critical extension with a registered object identifier (OID) for CA's SAFE Certification Policy?		

Appendix F: Cross Certification Letter of Authorization Template

To	SBCA OA Manager
Subject	Letter of Authorization for Cross-Certification with <Applicant>
Authorization	The SAFE Policy and Approval Authority (PAA) reviewed the information provided by <Applicant>, and has approved their application for cross certification with the SAFE Bridge. This authorizes the SAFE Bridge Certification Authority (SBCA) Operational Authority (OA) to proceed with the cross certification of the SBCA and the <Applicant>'s Principal CA.

SAFE PERSONNEL INFORMATION	
SAFE Agent Participating in Cross-Certificate Ceremony	<name> Title: <title> Email: <name@address> Work: <work phone> Cell: <cell phone>
Other SAFE Personnel Participating in Cross Certificate Ceremony	<name 1>, <title> <name 2>, <title> <name n>, <title>

APPLICANT PERSONNEL INFORMATION	
Applicant	<applicant name>
Applicant Personnel Participating in Cross-Certificate Ceremony	<name 1>, <title> <name 2>, <title> <name n>, <title>
Applicant Principal Point of Contact (POC)	<name> Title: <title> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
Authentication Password for Applicant POC	<password>

APPLICANT PERSONNEL INFORMATION	
Key Applicant Primary POC	<name> Title: <title> Citizenship: <country> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>
Key Applicant Alternate POC	<name> Title: <title> Citizenship: <country> Email: <email@address> Work: <work phone> Cell: <cell phone> Home: <home phone> Pager: <pager number>

SAFE CROSS CERTIFICATE INFORMATION	
Validity Period	10 years
Cryptographic Algorithm & Key Size	RSA encryption with 1024 bits
Medium Assurance Policy Mapping	SAFE OID: 1.3.6.1.4.1.23165.1.3 Applicant OID:
Basic Assurance Policy Mapping (optional)	SAFE OID: 1.3.6.1.4.1.23165.1.2 Applicant OID:
Applicant CA Distinguished Name	
Applicant CA Permitted & Excluded Sub-Trees	
Maximum Number of Sub-CAs in Applicant CA's Trust Path (path length)	

AUTHORIZATION			
Signature		Date	
By		Title	SAFE PAA Chair