SAFE IDENTITY

SAFE Identity Bridge Certification Authority Cross Certification Process

December 19, 2019

Version 1.0

Signature

_____

Kyle Neuman
Managing Director, SAFE Identity

Document Control

Area	Description
Author(s)	SAFE Identity CPWG
Approver(s)	SAFE Identity PMA
Issue Date	December 19, 2019
Version	1.0

Revision History

Revision	Date	Revised By	Summary of Changes/Comments
1.0	12/19/2019	---	---

Table of Contents

1 Introduction

The SAFE Identity Certificate Policy (CP) defines the SIBCA as an interoperability mechanism for ensuring trust across independent PKI domains. Successful cross certification with the SIBCA asserts that the Applicant PKI operates in conformance with the CP and the related standards, guidelines and practices of the SAFE Identity Policy Management Authority (PMA).

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

These cross-certification guidelines should be read in conjunction with the current version of the SAFE Identity Certificate Policy.

1.1 Purpose

The purpose of this document is to describe the process and criteria for cross-certification of an Applicant's Public Key Infrastructure (PKI) Certification Authority with the SAFE Identity Bridge Certification Authority (SIBCA). In addition, the document addresses life cycle management of the cross-certification relationship.

1.2 SAFE Identity Policy Management Authority

The SAFE Identity PMA is comprised of the organizations cross-certified with the SIBCA along with vendor and relying party organizations that have requested the privilege of participating. It is responsible for managing and maintaining the SAFE Identity X.509 Certificate Policy and approving organizations for cross-certification with the SIBCA.

The SIPMA is an advisory group created by SAFE Identity, and SAFE Identity reserves the right to override PMA decisions related to (i) policy, technical and business practices and issues related to the SIBCA; and (ii) approval of applicants for cross-certification with the SIBCA. In such instances, SAFE Identity will provide an explanation in writing to the SIPMA.

1.3 Certificate Policy Working Group

The Certificate Policy Working Group (CPWG) is comprised of designated SAFE Identity personnel. It performs day-to-day activities associated with the maintenance of cross certification relationships as well as performing document review and interoperability testing for cross certification and annual renewal of both. The CPWG is primarily responsible for ensuring that the SAFE Identity documentation and guidelines promote secure federation of the PKIs; and secondarily that they maximize interoperability. The CPWG provides its work products to the PMA for review and final disposition.

1.4 Intended Audience

This document is intended for the use of the SAFE membership, candidates for cross certification with the SIBCA in order to be certified as SAFE Identity Digital Certificate Issuers, and the relying party community at large.

1.5 Definitions

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

1.6 References

This SAFE Identity Cross Certification Process document makes reference to Internet Engineering Task Force RFC 3647 and other SAFE Identity documents.

1.7 General Principles

Subject to this document, SAFE Identity and the SAFE Identity PMA will consider applications for cross certification from any entity operating a CA.

Cross-certificates are issued and revoked by the SIBCA at the sole discretion of SAFE Identity based on guidance from the PMA. Any review by SAFE Identity and the PMA of information from an applicant PKI is for use in determining whether or not cross certification is possible and appropriate – in short, whether the applicant PKI conforms to the requirements of the SAFE Identity CP for trust and interoperability.

For SIBCA cross certification, the SAFE Identity CPWG will conduct a review of the applicant's CP in relation to the SAFE Identity X.509 CP at the assurance levels requested in the application.

Similarly, applicants for SIBCA cross certification should determine whether to reciprocally issue a cross certificate to SAFE Identity by conducting a review of the SAFE Identity X.509 CP in relation to the applicant's own. The applicant must determine if the SAFE Identity CP provides criteria that meet the applicant's policy and legal requirements. CPWG review and mapping plus the PMA acceptance of an applicant CP is not a substitute for due care and mapping of certificate policies by the applicant.

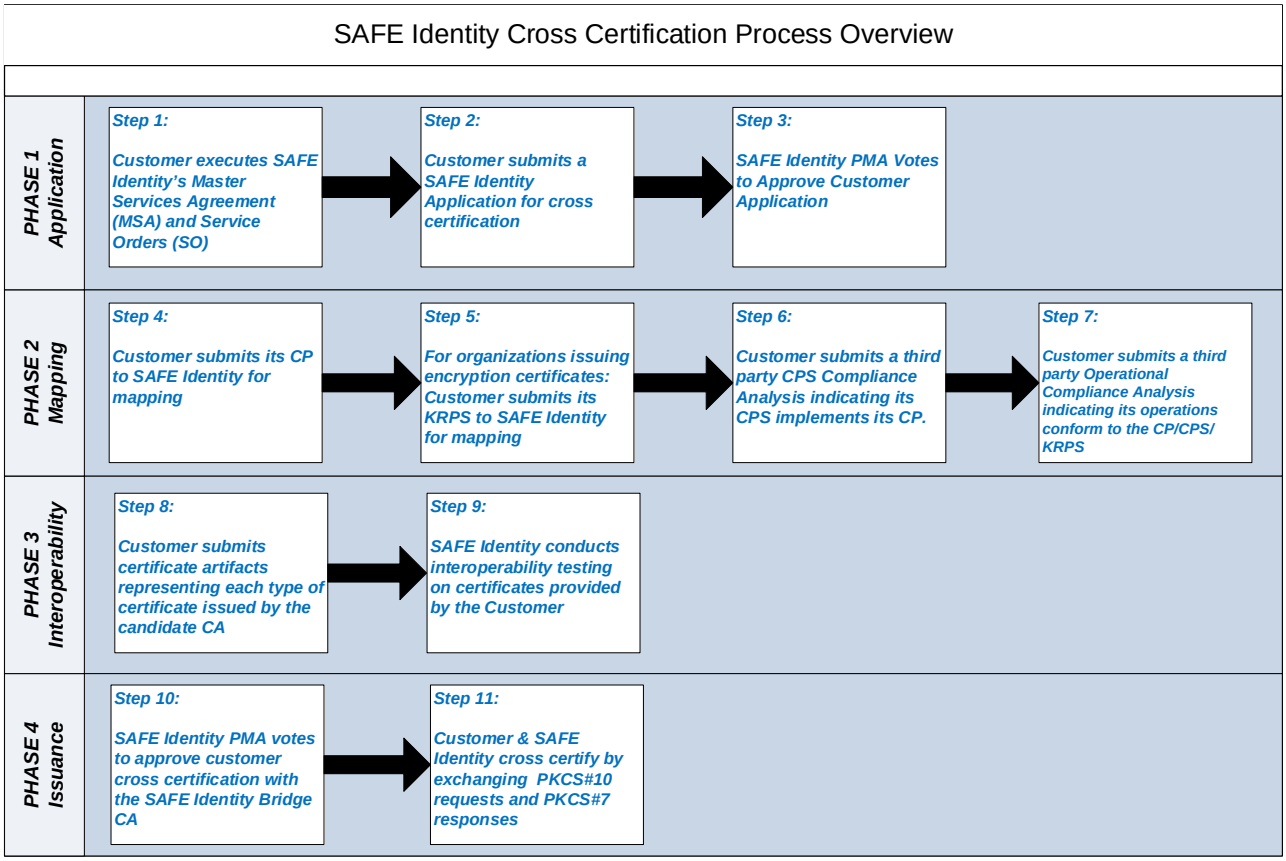
Applicants for cross certification must provide independent third-party attestation to the adherence of the applicant's Certification Practice Statement (CPS) to its CP and the applicant's PKI operations to its CP and CPS.

In addition, applicants for cross certification must successfully complete interoperability testing conducted by SAFE Identity, the results of which are shared with the PMA and used in making the final determination to cross certify.

Finally, all applicants for cross-certification must obtain unique policy Object Identifiers (OIDs) in the standard ISO object identifier registry from the appropriate commercial or national registration authorities.

2 Cross Certification Process

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



2.1 Phase I – Application

2.1.1 Step 1: Master Services Agreement

The SAFE Identity Master Services Agreement (MSA) must be executed by the applicant before the cross-certification process can commence. The MSA includes a one-time obligation of funds for the cross-certification activities (on-boarding) and the first year's (recurring) annual maintenance fee. Fees due under the MSA must be paid before the application is presented to the PMA for a vote.

2.1.2 Step 2: Prepare Application for Cross Certification:

The applicant completes the application and submits it, along with supporting documentation to the SAFE Identity PMA Chair.

The application must contain the following information:

2.1.2.1 Information on the Applicant's Organization

- The organization's legal name
- (Optional) Short description of the organization
- Two organization representatives: name and title, postal address, office phone and office e-mail

address. These representatives should occupy positions in the organization whose primary responsibility relates to PKI and/or Identity Management for the organization. In addition, at least one should be a member of senior management within the organization, with oversight responsibilities for PKI and/or Identity Management activities within the organization and authority to speak to issues pertaining to this subject on behalf of the organization. Upon successful completion of the cross-certification process, it is expected that one of these individuals would be the designated SAFE Identity PMA voting member, while the other would be the alternate PMA voting member.

2.1.2.2 Information on the Applicant's Service Level Request

Organizations must:

- Indicate whether or not this is an Enterprise Cross Certification. That is, the applicant organization issues credentials to its own employees and select contract personnel, and does not provide credential services to other organizations for a fee.
- Declare whether the applicant organization is seeking SAFE Identity Certified Credential Provider certification. That is, does the applicant organization intend to use its relationship with the SIBCA to market credential services to other organizations for a fee.
- Declare whether the applicant organization will issue encryption certificates, and make an assertion concerning escrow functionality compliant with the SAFE Identity Key Recovery Policy (KRP).
    - If yes, the applicant must develop a Key Recovery Practices Statement (KRPS) that implements escrow and recovery functionality that is compliant with SAFE Identity standards as detailed in the SAFE Identity KRP.
    - The KRPS should be submitted to SAFE Identity as part of the application package for review during the mapping process. The submission of this document is covered by the confidentiality agreement between SAFE Identity and the applicant. It will not be shared with the PMA or any other entity outside the SAFE Identity CPWG.
    - The applicant must include KRPS compliance in the third party audit covering PKI operations before final approval will be granted.

  Note: If the applicant is seeking cross certification for a Bridge, it must clearly indicate whether or not the Bridge supports key recovery. In the event it does support key recovery, the Applicant must submit the Bridge's KRP.

2.1.2.3 Information on the Applicant's PKI Architecture

A diagram of the PKI Architecture and an in-depth description should be attached as Appendix B to the application. In addition, at a minimum, the following information should be provided in the application:

- Technical Considerations – An account of the specific technical aspects of the applicant organization's PKI, including:
    - CA software utilized with an overview of the configuration.
    - Hypervisor (if applicable) and Operating System the CA is running on and hardware utilized (including Hardware Security Module (HSM)).
    - Directory product utilized and any relevant configuration information.
    - Online Certificate Status Protocol (OCSP) Responder product utilized and any relevant

configuration information, if applicable.

- Security Considerations – An account of the security architecture protecting the applicant organization's CAs, including:
    - A list of all CAs subordinate to or cross certified with the organization's Principal CA and to what degree the organization has control over these related CAs.
    - A list of all CAs cross certified with the Principal CA and to what degree they are under the applicant organization's direct control.
    - Network services and controls protecting the applicant organization's CAs.

2.1.2.4 Information on the Applicant's Directory Architecture

A diagram of the applicant organization's Directory Architecture should be attached as Appendix C to the application. In addition, at a minimum, the following information should be provided:

- The applicant must describe the organization's directory structure and how interoperability with SAFE Identity's directory requirements will be accomplished.
- The applicant must describe how namespace control will be achieved for ensuring unique distinguished naming within its PKI enterprise.

2.1.2.5 Information on the Applicant's Auditing Practices

Applicants must employ the services of an auditor to provide an independent analysis of the compliance of the applicant's Certification Practices Statement to the governing Certificate Policy and an assessment of whether the PKI operations implement the Certification Practices Statement. The auditor may be either:

- An independent third-party entity with no relationship to the Applicant's organization or
- A Corporate Internal Auditor, provided the organization can demonstrate sufficient separation and independence to ensure no conflict of interest.

In both cases, the auditor must have sufficient experience and training to perform in the function of independent auditor. SAFE Identity will make the determination of auditor suitability based on the responses in Section 5 of the application.

Auditor information must cover the following three major areas:

- Identity and experience of the Lead Auditor.
- Identity and experience of the Staff Auditors.
- Attestation of auditor independence.
    - For Third Party Auditors – Attestation that the compliance auditor works for a separate third- party operating entity, independent of the applicant's organization and any of its affiliates.
    - For Corporate Independent Auditors – An organizational diagram showing points of intersection between the organization administering the PKI and the Corporate Independent

      Auditor and an attestation that the corporate internal auditor is organizationally independent.

2.1.2.6 Information on Applicant's Certificate Policy Mapping

The applicant must select the level(s) of assurance offered by the SIBCA CP to which cross certification is requested. Place a checkmark in all that apply.

The applicant's CP must support the requested level(s) of assurance.

2.1.2.7 Attached Documentation

Applicants must attach the following required documentation to the application:

- Appendix A – Applicant's CP. CP must be in RFC 3647 format.
- Appendix B – A detailed diagram of the applicant's CA architecture with explanation of its operational processes.
- Appendix C – The directory schema of the applicant's PKI.
- Appendix D – Key Recovery Practices Statement (if applicable).
- Appendix E (Bridge applicants only) – the Criteria and Methodology pertaining to the applicant Bridge.

Note: the applicant's CP *must* be provided in electronic form as a Microsoft *WORD* document for SAFE Identity review. The CP will be shared with the PMA membership. The contents of Appendix B will be protected by SAFE Identity and not shared with any parties outside the CPWG.

Organizations may submit additional documentation with the application at their discretion. These additional documents must be identified here and provided as additional Appendices.

2.1.2.8 Authorized Signature

The application must be signed by a senior official from the applicant's organization with the specific authority to bind the company to a contract and who is authorized to commit the organization to SAFE Identity's cross certification process.

2.1.3 Step 3: Application Approval

Once the completed application and associated documents are received by SAFE Identity, the CPWG conducts a review and may request additional information or clarification from the applicant. Once satisfied that the documentation is complete and the interoperability use case is valid, the CPWG prepares a recommendation and submits it along with the application to the PMA for review and approval.

Upon approval/disapproval, the PMA Chair advises the Applicant point of contact (POC). If the decision is to proceed, the CPWG initiates the review and audit activities.

If the decision is not to proceed with the cross-certification process, the PMA Chair 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.

When notified of a decision to proceed, the Applicant cross certification process then continues with Phase II for formal mapping of certificate policies.

2.2 Phase II – Mapping

Once the MSA has been signed, fees have been paid and the SAFE Identity PMA has approved the application, the policy mapping phase can begin. It consists of four activities:

- Certificate Policy Mapping
- KRPS Mapping (when applicable)
- CPS Compliance Analysis Review
- Operational Compliance Analysis Review

2.2.1 Step 4: Certificate Policy Mapping

Purpose: Map the Applicant's CP to the SAFE Identity CP in order to establish equivalency of trust for certificates whose policy OIDs are present in the cross certificate between the Applicant CA and the SIBCA.

Procedures:

- The CPWG will map the applicant's CP to the SAFE Identity CP.
- The resulting Certificate Policy Mapping Report will identify areas where the applicant's CP does not contain the detail necessary to map successfully and which may require modifications to the applicant's CP.
- The CPWG will make itself available to discuss the specific mapping report findings at the applicant's discretion.
- The applicant will submit a revised CP that addresses the CPWG mapping report findings. The CPWG requires a marked-up version showing the revisions made as a result of the findings using Track Changes.
- The above process may repeat several times until both the CPWG and the applicant are satisfied at which time, the CPWG will prepare a final mapping report for consideration by the SAFE Identity PMA indicating the applicant's CP has been mapped successfully to the SAFE Identity CP.

SAFE Identity Certified Credential Provider

When a SAFE Identity cross-certified organization is granted Certified Credential Provider status, the cross certificate issued by the SIBCA to the organization will not contain any name constraints. However, absence of name constraints requires additional diligence on the part of the cross-certified organization to ensure accuracy of organization naming and prevention of name collision within the organization's community of users and with other names assigned by other SAFE Identity participants. Therefore, an applicant whose intent is to act as a credential provider to other organizations must satisfy the provisions associated with SAFE Identity Certified Credential program; specifically, the applicant must describe how name uniqueness will be managed across subscriber enterprises and across SAFE Identity community: both organizational and individual naming.

Name conflicts must be identified and dealt with in a consistent and positive manner that is documented in the CPS or related documentation. At a minimum, the applicant should be prepared to share Section 3.1.5 of its CPS. The SAFE Identity Certified Credential Provider applicant will be required to provide a presentation of the processes employed to the SAFE Identity CPWG, be prepared to answer CPWG questions and revise the process until the CPWG is satisfied that name meaningfulness and name uniqueness are adequately addressed.

2.2.2 Step 5: KRPS Compliance

The applicant's KRPS will be compared to the SAFE Identity KRP for any Applicant that intends to issue encryption certificates to end users. All others will skip Step 5. See Section 2.1.2.2 above to determine applicability of this step.

- The CPWG will review and analyze the applicant's KRPS to determine if the KRPS provides sufficient information in terms of meeting SAFE Identity's KRP requirements.
- The resulting KRPS Compliance Analysis will identify areas where the applicant's KRPS does not meet the requirements of the SAFE Identity KRP or does not contain sufficient details, and require modifications to the applicant's KRPS.
- The CPWG will make itself available to discuss the specific compliance analysis findings, at the applicant's discretion.

The applicant will submit a revised KRPS that addresses the CPWG report findings in a marked up version using *tracked changes*.

The above process may repeat several times until both the CPWG and the applicant are satisfied, at which time, the CPWG will issue a final KRPS Compliance Analysis for consideration by the SAFE Identity PMA, indicating the applicant's KRPS has successfully demonstrated compliance to the SAFE Identity KRP.

Note: SAFE Identity recognizes the sensitive nature of a KRPS. The document will be used internally by the SAFE Identity CPWG to perform the compliance analysis but will not be shared with PMA members or made available beyond the CPWG.

Bridge CAs will undergo KRP mapping instead of KRPS compliance analysis.

2.2.3 Step 6: CPS Compliance Analysis

The applicant must engage the services of a third-party auditor (identified in Section 6 of the application to perform a compliance analysis of the CPS in relation to the applicant's CP (submitted with the application and revised during the CP Mapping process). The compliance auditor must return an opinion indicating that "the CPS complies with the requirements of the CP" in order for the CPS compliance analysis to be accepted by the SAFE Identity PMA. The applicant will provide the auditor opinion to SAFE Identity for consideration by the PMA.

2.2.4 Step 7: PKI Operational Compliance Audit

Related to the CPS Compliance Analysis in Step 6, the third-party auditor must complete an operational compliance audit. This compliance audit assesses whether the credentialing infrastructure is implemented in accordance with the CPS and KRPS (where applicable). The audit may take one of two forms, as follows:

- If the audit is being performed on an existing fully functioning CA, a full operational audit will be performed.
- If the audit is being performed on a new CA that is not yet fully functioning (i.e. production certificates have not been issued in quantity), a pre-operational audit will be performed. The following applies to a pre-operational audit:
    - The pre-operational audit is valid for six months, at which time an operational audit must be performed.
    - In the event an operational audit cannot be completed within the six-month timeframe due to an insufficient number of production certificates, the organization may request one, and

only one, six-month extension.

- The extension request must indicate the reason for the extension with an assertion from the auditor that use of the operational environment is insufficient to perform a meaningful audit.
- The extension is granted at the sole discretion of SAFE Identity.
- In the event an extension is not granted and the organization does not complete an operational audit, the cross certificate issued by the SIBCA will be revoked.

- Regardless of the operational environment, the annual audit, due twelve months following the last successful audit must be completed.

The following applies to all types of audits:

- The applicant will provide the Auditor with a set of management assertions concerning the operations of the PKI in relation to the CP/CPS and KRPS (where applicable).
- The Auditor will prepare an opinion letter summarizing the audit findings.
- The Audit must address all of the requirements identified in the *SAFE Identity Audit Letter Template*.
- The applicant will submit the audit opinion letter, along with the statement of management assertions to SAFE Identity for consideration by the PMA.
- Audit opinion letters pertaining to applicants for SIBCA cross certification must be free of any findings.

2.3 Phase III –Interoperability

The purpose of Interoperability testing is to identify and resolve any incompatibilities between the Applicant's PKI and those of the SIBCA. interoperability testing focuses on the proper construction of certificates, CRLs, OCSP responses, and PKCS-10 requests with respect to the PKI's infrastructure. This testing does not include running PK-enabled applications, such as TLS or secure E Mail.

2.3.1 Step 8: Submission of Certificate Artifacts

The Applicant submits the following for SAFE Identity review:

- All CA certificates, including the self-signed root and cross certificate(s).
- One sample of each type of certificate issued by each CA in the applicant's PKI.
- One sample of each type of CRL issued by each CA in the applicant's PKI.
- All OCSP Responder certificates.

For Bridge CAs, only the PKI objects produced by the Bridge itself including associated CRLs and OCSP Responders, if applicable, are required.

2.3.2 Technical Interoperability Testing

This testing requires examination of the PKI artifacts identified in Step 8 for conformance to certificate profiles and interoperability. In addition, the following are reviewed:

- One sample OCSP request and response for each OCSP Responder.
- All pointers in the certificates and CRLs such as CRL DP and CA Issuers field in AIA.
- Status response of certificates from the OCSP Responders.
- Conformance to Cloud Signature Consortium standards
- Directory interoperability
- The ability of the SIBCA to access the Applicant's OCSP Responder.
- Appropriate validity and/or re-issuance periods for all issued certificates.

Additional examination and testing may be required depending on the complexity of the applicant's PKI.

The OA Administrator documents the results of the test and forwards it to the CPWG. The CPWG reviews the report and determines if there are areas of technical non-compliance with the SIBCA environment. If such areas are identified, the CPWG works with the OA Administrator to perform an assessment of the need to make changes to the SIBCA environment or documentation, the need to request changes to the Applicant's PKI or documentation, or the reasonableness of accepting certain differences. Any accommodation may include a recommended timeframe for resolution of such differences.

2.4 Phase IV –Issuance

Once all Mapping and Interoperability activities have been completed successfully, the issuance phase will be initiated consisting of the PMA Approval Vote and subsequent cross certificate issuance.

2.4.1 Step 10: PMA Approval Vote

Upon satisfactory completion of the mapping, compliance analysis, compliance audit, and interoperability testing, the documentation is gathered and presented to the PMA for final review and vote.

The CPWG prepares a decision brief based on the results of the CP mapping exercise and the technical interoperability report and provides it to the PMA for review and approval.

The following documentation is required:

- SAFE Identity report concerning mapping of applicant CP to SAFE Identity CP.
- Latest version of the applicant CP, with changes resulting from the mapping activity included.
- KRPS compliance analysis, where applicable.
- Compliance auditor's assertion letter concerning the applicant's CPS conformance to the applicant's CP.
- Compliance auditor's opinion letter concerning conformance of applicant operations to the CPS and KRPS, where applicable, with management assertions attached. This may be based on either a pre-operational audit or full operational audit.
- Baseline Interoperability test results summary.

The PMA Chair schedules a vote to approve cross certification based on these results at the next PMA meeting.

The PMA reviews the CPWG recommendation, discusses the results, and asks any questions they have concerning the process. Once all questions have been addressed, the Chair calls for a vote regarding cross certification of the applicant PKI, which requires a 75% majority of the voting member approval to pass.

Upon approval by the PMA for applicant cross certification or subordination, the applicant is welcomed as a full voting member of the PMA. The PMA Chair provides the Letter of Authorization to the Operations Authority Manager to issue a cross certificate to the newly approved CA as described in *Step 11: Cross Certification.*

2.4.2 Step 11: Cross Certification

The first step in issuing a cross certificate is completion of the Naming Application Form. SAFE Identity will assist the applicant with completion of this form which provides details of certificate construction and will be used in generating the certificate. In filling out the Naming Application Form, the policy mappings specified must be per the PMA approved Application (see *Step 3: Application Approval*) and subsequently confirmed by the CP mapping performed by the CPWG in *Phase II: Mapping*.

In addition, both SAFE Identity and the applicant must:

- Securely[1] exchange CSRs in PKCS#10 format with SKID specified (the correct PKCS #10 certificate profile can be found in the SFE Identity CP Section 10). This process exchanges the public keys that are to be signed by the respective CAs. As an alternative to the CSR, the affiliate may securely provide the certificate of the CA that is being cross certified.
- Sign the CSR/CA certificate using the appropriate CA – this generates a certificate.
- Send the certificate to the other party through digitally signed e-mail or on a write-only media such as a CD.
- Install the received certificate in the appropriate CA Directories.

Upon completion of the cross-certification ceremony, the Applicant will be designated officially as a SAFE-Identity Issuer.

[1] Examples of secure submission include hand carrying, FedEx, certified postal mail, and a digitally signed electronic file that can be verified by SAFE Identity.

3 Maintenance of PKI Relationship with SAFE Identity

It is important to ensure that, once in place and for its duration, the cross-certification continues to guarantee the agreed-upon level(s) of trust between SAFE Identity and the cross-certified PKI.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified entities and for terminating the arrangement. The following activities are inherent to the maintenance of SAFE Identity cross certification and subordination relationships:

- Participation in the SAFE Identity PMA.
- Annual recertification of the SAFE Identity relationship.
- Problem resolution.
- Termination.

3.1 Participation in the SAFE Identity PMA

Upon approval of an organization for cross certification, the organization becomes a SAFE Identity Issuer and is invested with full rights as a member of the SAFE Identity PMA. To this end the newly affiliated organization must provide, as part of the MSA, the name and contact information for the primary voting member that will represent the organization at PMA meetings, and the name and contact information for an alternate to represent the organization when the primary voting member is unavailable. These representatives must be employees of the Issuer organization and hold positions with oversight responsibilities for PKI and/or Identity Management activities within the organization. Issuer organizations are required to participate in the monthly PMA meetings or provide a voting proxy when absence is unavoidable. Proxy may be assigned to the Chair or to any other voting member.

In the event an organization wishes to replace its voting member or alternate, this must be communicated to the SAFE Identity PMA Chair in a written notification on company letterhead and duly signed by an individual authorized to act on behalf of the organization.

3.2 Annual Recertification of the SAFE Identity Relationship

Cross certificates issued by the SIBCA expire twelve months from date of issuance. In order to continue as a SAFE Identity Issuer, the cross certified organization must undergo recertification. The following activities are performed *annually* during the recertification process to maintain an organization's cross certification status with the SIBCA:

- Renewal of the *MSA Service Order* between the Issuerand SAFE Identity.
- *Differential Policy Mapping.*
- *Interoperability Testing*.
- *Annual Compliance Audit*.
- Review and vote by the SAFE Identity PMA to continue SIBCA relationship.
- Reissuance of SIBCA cross certificate.

In addition, a *KRPS Differential Compliance Analysis* is conducted biannually, where applicable.

In the event a SAFE Identity Issuer wishes to make changes to the cross-certification relationship (e.g. implement new policy OID mappings), an "Application for Cross-Certificate Modification" must be completed in addition to the above.

3.2.1 Renewal of the MSA Service Order

The Service Order (SO) associated with the MSA must be renewed annually. Recertification activities (mapping, interoperability testing, etc.) will not be undertaken until the SO has been renewed and any outstanding fees have been paid.

Failure to complete the MSA SO renewal in a timely manner to allow completion of recertification activities before the expiration date of the current cross certificate may result in its cross certificate lapsing and suspension of the organization's SAFE Identity PMA voting membership.

3.2.2 Differential Policy Mapping

SAFE Identity Issuers complete a Certificate Policy Differential Policy Mapping each year in order to renew their cross certification with the SIBCA. This mapping reduces the risk of policy drift between the Issuer's CP and the SAFE Identity CP as these documents change over time. This mapping also helps SAFE Identity ensure that any CP change requests the SAFE Identity PMA has approved over the past twelve months were adopted by the Issuer. The Issuer's agreement with SAFE Identity obligates the organization to adopt changes within the timeframe specified in the change request; generally, three months. To assist Issuers in preparing for the differential policy mapping, SAFE Identity will provide a red-lined CP that indicates the changes that have taken place between the SAFE Identity CP version previously used to map the Issuer's CP and the current version of the SAFE Identity CP.

The Differential Policy Mapping is accomplished by reviewing the changes in the Issuer's CP since the last approved policy mapping and mapping these to the current SAFE Identity CP. To this end, the Issuer must supply:

- A current CP in *WORD* document format that highlights (with *Track Changes*) all changes from the last approved policy mapping.

SAFE Identity's CPWG will:

- Verify the submitted CP is consistent with the last cross certified CP, with track changes showing all new modifications.
- Perform a differential policy mapping against the current SAFE Identity CP that examines the changes to the Issuer's CP to ensure changes made to the SAFE Identity CP have been adopted, where appropriate, and no other changes made are detrimental to cross organizational trust.
- Generate a mapping report that identifies areas where the Issuer's CP does not appear to map successfully and which may require additional modifications to the CP.
- Be available to discuss the policy mapping report at the Issuer's discretion.

Based on the report and subsequent discussion, the Issuer will submit a revised CP that addresses the CPWG mapping report findings in a marked-up version using tracked changes, as well as a "clean" version that contains no editorial marks or comments. Each revised document must be assigned a new version number and date of creation to ensure effective version control. This is an iterative process which may repeat several times until both the CPWG and the Issuer are satisfied, at which time the CPWG will issue a final mapping report indicating the Issuer's CP has been mapped successfully to the SIBCA CP.

Once the Issuer's CP is accepted by the CPWG, the Issuer must ensure its CPS is amended as appropriate.

If the modifications to the Issuer's CP as a result of the mapping process are considered "significant", an updated third-party compliance analysis and audit must be supplied by the Issuer. SAFE Identity with notify the Issuer when this is the case.

3.2.3 KRPS Differential Compliance Analysis

Issuers that issue encryption certificates to end users are required to undergo review of their KRPS every two years. To assist in the process, SAFE Identity will provide a red-lined KRP that indicates the changes that have taken place between the SAFE Identity KRP version previously used in review of the Issuer's KRPS and the current version of the SAFE Identity KRP.

Note: SAFE Identity recognizes the sensitive nature of a KRPS. The document will be used internally by the SAFE Identity CPWG to perform the compliance analysis but will not be shared with PMA members or made available beyond the CPWG.

The KRPS compliance review is accomplished by examining the changes in the Issuer's KRPS since the last approved KRPS compliance review with the current SAFE Identity KRP for reference. To this end, the Issuer must supply:

- A current KRPS in *WORD* document format.
- A current KRPS in *WORD* document format that highlights (with *Track Changes*) all changes from the last approved KRPS mapping.

SAFE Identity's CPWG will:

- Examine the Issuer's KRPS for conformance with SAFE Identity KRP.
- Generate a KRPS compliance audit report identifying areas where the Issuer's KRPS does not meet the requirements of the SAFE Identity KRP.
- Determine whether modifications to the Issuer's KRPS are needed.
- Be available to discuss the specific compliance report findings, at the Issuer's discretion.

The Issuer will submit a revised KRPS that addresses the CPWG compliance report findings in a marked-up version using tracked changes. Each revised document must be assigned a new version number and date of creation to ensure effective version control.

The above process may repeat several times until both the CPWG and the Issuer are satisfied, at which time, the CPWG will issue a final KRPS compliance report indicating the Issuer's KRPS has been reviewed successfully for compliance with the SAFE Identity KRP for consideration by the PMA.

3.2.4 Interoperability Testing

The Issuer's PMA representative is responsible for keeping the contact information concerning the technical resource current. The technical resource must have knowledge of the operational environment of the organization's PKI and will act as the liaison between the Issuer and SAFE Identity for the duration of the interoperability testing.

Interoperability testing is required for annual recertification of all Issuers. SAFE Identity's interoperability testing focuses on the proper construction of certificates, CRLs, OCSP responses, and PKCS-10 requests with respect to the Issuer PKI's infrastructure. This testing does not include running PK-enabled applications such as TLS or secure E Mail.

- SAFE Identity will conduct all applicable interoperability testing using the SAFE Identity lab facilities.
- Upon completion, an interoperability report will be prepared identifying areas where the tested artifacts are not conformant and/or interoperability may be affected.
- SAFE Identity will make itself available to discuss the specific interoperability report findings, at the

Issuer's discretion.

- The Issuer will submit revised artifacts that address the interoperability report findings for retesting.

The above process may repeat several times until both SAFE Identity and the Issuer are satisfied, at which time, SAFE Identity will issue a final interoperability report for consideration by the SAFE Identity PMA, indicating the Issuer has successfully demonstrated interoperability in the SAFE Identity Federated PKI environment.

For interoperability findings that cannot be addressed immediately, the Issuer may submit a mitigation plan indicating the modifications that will be made to the certificates it issues in order to address the findings, and the timeframe for accomplishing these modifications. SAFE Identity may accept all or parts of the mitigation plan at its discretion; the affiliate must rectify the remaining issues immediately.

Testing requires examination of PKI artifacts such as the following for conformance to certificate profiles and interoperability:

- All CA certificates, including the self-signed root and cross certificate(s).
- One sample of each type of certificate issued by each CA in the Issuer's PKI.
- One sample of each type of CRL issued by each CA in the Issuer's PKI.
- PKCS#10 cross certificate request.
- All OCSP Responder certificates.
- One sample OCSP request and response from each OCSP Responder.
- All pointers in the certificates and CRLs such as CRL DP and CA Issuers field in AIA.
- Status response of certificates from the OCSP Responders.
- Conformance to Cloud Signature Consortium standards
- Directory interoperability
- The ability of each cross-certified organization to validate the other cross-certified organizations' CA certificates and cross certificates
- The ability of the SIBCA to access the Applicant's OCSP Responder
- Appropriate validity and/or re-issuance periods for all issued certificates.

Additional examination and testing may be required depending on the complexity of the Issuer's PKI.

For Bridge CAs, only the PKI objects produced by the Bridge itself and associated OCSP Responders, if applicable, are examined.

3.2.5 Annual Compliance Audit

All Issuers cross certified with the SIBCA must undergo an annual audit that covers the previous 12 months, and is completed on or before the anniversary date of the previous audit. The Compliance Audit must be conducted by an approved auditor who has demonstrated competence in PKI audits. The auditor may be either an independent third-party entity with no relationship to the Issuer's organization or a Corporate Internal Auditor provided the Issuer can demonstrate sufficient separation and independence to ensure no conflict of interest. When a Corporate Internal Auditor is used, the Issuer must engage the services of an independent third-party auditor every third year, at a minimum.

In the event the Issuer changes audit companies, the individuals conducting the audit on behalf of the third party independent audit company change, elects to use corporate internal auditors, or the corporate internal auditor personnel change, the Issuer must notify SAFE Identity and provide information concerning the new audit company, organizational separation, and/or personnel in accordance with the application template, described in Section 2.1.3.5 above.

The annual compliance audit is comprised of two parts: the CP/CPS compliance analysis and the Operational Compliance assessment.

3.2.5.1 CP/CPS Compliance Analysis

Compliance analysis of the CPS in relation to the Issuer's CP is performed by the third party or corporate internal auditor. The compliance auditor must return an opinion indicating that "the CPS complies with the requirements of the CP" in order for the CPS compliance analysis to be accepted by the SAFE Identity PMA. The affiliate will provide the auditor opinion to SAFE Identity for consideration by the PMA.

3.2.5.2 Operational Compliance Assessment

The operational compliance assessment assesses whether the credentialing infrastructure is operating in accordance with the CPS and KRPS (where applicable).

- The Issuer will provide the Auditor with a set of management assertions concerning the operations of the PKI in relation to the CP/CPS and KRPS (where applicable).
- The Auditor will prepare an opinion letter summarizing the audit findings and identifying the areas of non-compliance, if any.
- The audit opinion must address all of the requirements identified in the *SAFE Identity Audit Letter Template.*
- The Issuer will submit the audit opinion letter, along with the statement of management assertions and a mitigation plan, with milestones, for the identified areas of non-compliance, if any, to SAFE Identity for consideration by the PMA.

3.2.6 PMA Vote on Recertification

Upon satisfactory completion of the mapping/compliance analysis, interoperability testing, and compliance audits, the documentation is gathered and presented to the PMA for final review and vote.

The following documentation is required:

- SAFE Identity CP Mapping Report.
- Latest version of the Issuer's CP, with changes resulting from the mapping activity included.
- Compliance auditor's assertion letter concerning the Issuer's CPS conformance to the its CP.
- Compliance auditor's opinion letter concerning conformance of Issuer PKI operations to the CPS and KRPS, where applicable, with management assertions attached.
- Interoperability test results summary.
- KRPS compliance analysis, where applicable.

The SAFE Identity PMA Chair schedules a vote to approve re-certification based on these results at the next PMA meeting.

Approval by a 75% majority of the voting members (with recusal of the concerned member) are required to pass:

Upon approval of the vote by the SAFE Identity PMA, the PMA Chair will instruct the Operational Authority to issue a new cross certificate to the customer.

3.2.7 Reissuance of Cross Certification Certificate

The first step in reissuing a cross certificate is completion of the Naming Application Form. SAFE Identity will assist the affiliated organization with completion of this form to ensure the details of certificate construction are accurate. In filling out the Naming Application Form, the policy mappings specified must be in accordance with the findings of the CP Mapping Report described in *Section 3.2.2, Differential Policy Mapping* and approved by the PMA as described in *Section 3.2.6 PMA Vote on Recertification*.

For continuation of the cross certified relationship, both SAFE Identity and the Issuer must:

- Securely exchange CSRs in PKCS#10 format with SKID specified. This process exchanges the public keys that are to be signed by the respective CAs. As an alternative to the CSR, the Issuer may securely provide the certificate of the CA that is being cross certified.
- Sign the CSR/CA certificate using the appropriate CA – this generates a certificate.
- Send the certificate to the other party through digitally signed e-mail or on a write-only media such as a CD.
- Install the received certificate in the appropriate CA Directories.

3.3 Problem Resolution

Either SAFE Identity or the Issuer may notify the other of problems and request resolution.

For Technical problems, the Issuer PKI technical resource will work with the SAFE Identity Operations Manager to resolve the issue(s).

For situations where SAFE Identity or the SAFE Identity PMA has reason to believe that the Issuer PKI is not operating in compliance with its MSA or CP, either SAFE Identity or the SAFE Identity PMA may request an aperiodic compliance audit and a compliance audit letter specifically addressing the concern. All such requests will be made for cause, and the cause will be disclosed at the time of the request.

For CA key compromise, the affected organization will take action immediately as required in the CP Section 5.7, to include immediate notification to the SAFE Identity PMA Chair.

SAFE Identity reserves the right to join the Issuer's internal incident response team if deemed necessary.

3.3.1 Notification

3.3.1.1 SAFE Identity Responsibilities

SAFE Identity will promptly advise the PMA membership:

- In the event of any material problem or inability to operate the SIBCA in accordance with the SAFE Identity CP or CPS.
- In the event that SAFE Identity becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the SIBCA and that interoperates with the SIBCA.
- In the event that SAFE Identity takes any action to terminate or limit such other party's interoperability with the SIBCA.
- In the event of a SIBCA private key compromise or loss, or an Issuer's Principal CA private key

compromise or loss. A CRL shall be published at the earliest feasible time by the SAFE Identity Operational Authority.

- In the event of a disaster where the SIBCA or an Issuer Principal CA installation is physically damaged and all copies of the SIBCA or Issuer Principal CA signature keys are destroyed.

Any such notification will occur as follows:

- The SAFE Identity PMA Chair or the SAFE Identity Operations Manager shall notify the PMA Member points of contact.
- Notification will be done by telephone, by digitally signed and encrypted e-mail, or by any other mechanism agreed upon and documented in official correspondence between the PMA Members and SAFE Identity.
- Additional procedures in accordance with SAFE Identity CP Section 5.7 will be followed.

3.3.1.2 Issuer Responsibilities

The Issuer will promptly advise the SAFE Identity PMA Chair and the SAFE Identity Operational Authority:

- In the event of any material problem or inability to operate the Principal CA in accordance with the Issuer CP or CPS .
- In the event that the Issuer becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the SIBCA and that interoperates with the Principal CA.
- In the event that the Issuer takes any action to terminate or limit such other party's interoperability with the SIBCA.
- In the event of a Issuer Principal CA private key compromise or loss. A CRL shall be published at the earliest feasible time by the Issuer CA.
- In the event of a disaster where the Issuer Principal CA installation is physically damaged and all copies of the Issuer Principal CA signature keys are destroyed.

Any such notification will occur as follows:

- The Issuer shall notify the SAFE Identity PMA Chair and the SAFE Identity Operational Authority.
- Notification will be done by telephone, by digitally signed and encrypted e-mail, or by any other mechanism agreed upon and documented in official correspondence between SAFE Identity and the Issuer.
- The Issuer shall follow all procedures specified in SAFE Identity CP Section 5.7, Issuer CP Section 5.7, and Issuer Principal CA CPS Section 5.7.

3.3.2 PMA Problem Resolution

SAFE Identity reserves the right to take necessary immediate action to resolve problems within the SAFE Identity community, followed by appropriate notification to the SAFE Identity PMA as soon as deemed practicable. However, in accordance with the legal provisions provided in the MSSAs between SAFE Identity and its Customers and when circumstances permit, problem resolution may be referred to the SAFE Identity PMA.

Problem resolution within the SAFE Identity community is routinely carried out by the SAFE Identity PMA through PMA votes:

- Approve PMA procedures for actions/remedies to address non- compliance requires a simple majority of the voting membership.
- Directions to the SAFE Identity OA to revoke cross certificates requires a 75% majority of the voting membership exclusive of the concerned party (requires recusal of concerned member).
- Determination of remedies/actions to be taken for unacceptable risk to the SAFE Identity trust fabric requires a 75% Majority of the voting membership.
- Determination to restore SAFE Identity interoperability following cross certificate revocation requires a 75% majority of the voting membership.

3.4 Termination

SAFE Identity has the right to terminate, modify, suspend or discontinue the SIBCA or individual Issuer's agreements due to:

- Government regulation or requirement.
- To avoid material liability to a third party.
- Revocation of an Issuer's certificate
- SAFE Identity's relationships with its service providers or licensors so require
- To avoid violations of the law or regulations

The relationship between SAFE Identity and a Issuer PKI may be terminated by either party.

3.4.1 Notice of Termination

In the event the Issuer PKI initiates termination, the Issuer PKI POC must notify SAFE Identity in writing of its intent to terminate the MSA, the reason(s) for seeking termination, and the desired termination date.

Should SAFE Identity become aware that there has been a failure in the integrity of an Issuer PKI, SAFE Identity will revoke the cross-certificate of the Issuer PKI. SAFE Identity will inform the Issuer PKI POC of the revocation and provide a resolution date after which the MSA will be terminated if the issue is not resolved. SAFE Identity will inform the other PMA members of the issue, the revocation, and the timeframe provided for resolution.

SAFE Identity will inform the Issuer PKI in writing of its intent to terminate the MSA at least 10 days before the effective date of termination.

3.4.2 Revocation of SIBCA -issued Certificates

SAFE Identity will revoke a cross certificate issued by the SIBCA if it can be proven or it is reasonable to believe key compromise has occurred or if the certificate needs modification.

In addition, SAFE Identity will revoke a cross certificate at the request of the organization to which it was issued.

3.4.2.1 Who Can Request Revocation of a Certificate

Any SAFE Identity PMA voting Issuer may request revocation of its own SIBCA-issued certificate at any time.

In addition, any SAFE Identity PMA member may request revocation of any other organization's SIBCA-issued certificate for cause. The SAFE Identity PMA chair will call a SAFE Identity PMA meeting to inform

the PMA membership of the request to revoke a certificate issued by the SIBCA and, upon confirmation of the request by the PMA members, issue a request to the SAFE Identity Operational Authority to revoke the certificate.

In accordance with legal provisions provided in service agreements with Issuers, SAFE Identity may revoke any cross certificate issued by the SIBCA at any time. SAFE Identity may request revocation of a certificate issued by the SIBCA if any of the following are true:

- The Issuer is in default with respect to its financial obligations to SAFE Identity.
- The Issuer has fallen out of compliance with its CP/CPS (or the SAFE Identity KRP, where applicable). This requires proof or must be reasonable to believe is the case before revocation action is taken. The Operational Authority Manager will be responsible for reporting this action and the justification to the SAFE Identity PMA immediately following the action.
- There is a compromise in the trusted roles at a Issuer's CA. This requires proof or must be reasonable to believe is the case before revocation action is taken. The Operational Authority Manager will be responsible for reporting this action and the justification to the SAFE Identity PMA immediately following the action.
- The Issuer's CA key has been compromised.

For additional guidance, see Sections 4.9.1 and 4.9.2 of the SAFE Identity or Affiliate CP.

3.4.2.2 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

3.4.2.3 Certificate Suspension

In accordance with legal provisions provided in service agreements with Issuers, SAFE Identity may suspend any certificate issued by the SIBCA at any time. SAFE Identity will suspend a certificate if it is reasonable to believe key compromise has occurred or the certificate needs modification.

SAFE Identity will remove the suspended certificate from the CRL if investigation findings confirm that a key compromise has not occurred and the certificate does not need modification.

4 Acronyms and Abbreviations

CA	Certification Authority
CP	Certificate Policy
PMA	Policy Management Authority
CPS	Certification Practice Statement
CPWG	Certificate Policy Working Group
CRL	Certificate Revocation List
CSR	Certificate Signing Request
HSM	Hardware Security Module
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
MSA	Master Services Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
SIBCA	SAFE Identity Bridge Certification Authority
SKID	Subject Key Identifier
SO	Service Order