



SIGNATURES AND AUTHENTICATION FOR EVERYONE

## **SAFE-BioPharma Certificate Policy SAFECP**

***12 March 2010***

***Version 2.5***

**Copyright ©SAFE-BioPharma Association 2005-2009. All rights reserved. The SAFE-BioPharma Association copyrights this SAFE-BioPharma Standard document. This document is confidential material, and is intended for use only by the SAFE-BioPharma Association and organizations participating in the SAFE-BioPharma System or their authorized agents. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by the SAFE-BioPharma Association.**

## Version 2.5

---

### Document Control

Area	Description
Author(s)	SAFE Core Team and SAFE Operations & Technology Working Group
Change Control	SAFE-BioPharma Association Change Management Council
Approver(s)	SAFE-BioPharma Policy Approval Authority (PAA)
Issue Date	12 March 2010
Version	2.5
Source File	SAFE-BioPharma Certificate Policy v2.4 4 Mar 2009.doc
Security	SAFE-BioPharma Association confidential
Distribution	<p>The information contained in this document is intended for personnel charged with the management and operation of the SAFE- BioPharma System. Recipients include the SAFE-BioPharma Association, SAFE- BioPharma Members, SAFE- BioPharma Working Group Participants, SAFE- BioPharma Partners, and Regulatory Agencies.</p> <p>This document is controlled and managed under the authority of the SAFE-BioPharma Policy Approval Authority.</p>

### Revision History

Version	Date	Revised By	Summary of Changes/Comments
1.1	06 Aug 2004	T. Zagar	Initial release with SAFE- BioPharma v1.1
1.2	27 Oct 2004	N/A	Distributed with SAFE version 1.2 without any changes

## Version 2.5

Version	Date	Revised By	Summary of Changes/Comments
1.3	31 Mar 2005	T. Zagar	<p>Global change from Policy Authority Committee (PAC) to Policy Approval Authority (PAA) usage</p> <p>Changes to Sections 1.3.5.3, 4.9.10, &amp; 5.7.4 to reflect use of SBCA OCSP Responder</p> <p>Update to Section 6.6.1 to reflect regulatory requirements for SBCA and Issuer PKI qualification</p> <p>Added clarifications to name forms in Section 7.1.4</p> <p>Changes in Section 7.1.5 to reflect current guidance on name constraints</p> <p>Modifications to Sections 1.2, 5.5.3, 6.1.1, 6.2.1, 6.2.7, 6.4.1 &amp; 9.8 to reflect use of SAFE- BioPharma certificates as qualified certificates per EU Directive 1999/93/EC</p> <p>Transfer of new requirements from SAFE- BioPharma Certificate, CRL and OCSP Guidance document to Section 10</p> <p>Change to Section 10.8 to reflect new nonce usage in OCSP requests</p>
2.0	30 Jun 2005	T. Zagar	<p>Updated all references to SAFE- BioPharma OIDs to reflect actual IANA enterprise number</p> <p>Clarified that X.500 chaining is not supported by SBCA directory, only LDAP referrals</p> <p>Updated requirements in Section 10 for use of HTTP and LDAP URIs in authority information access extension and CRL distribution point extension</p> <p>Updated requirements for authority information access extension use of .p7c files for calssuers certificates in Section 10</p> <p>Clarified policy mapping extension options in Section 10.1</p> <p>Deleted inhibitAnyPolicy reference in Section 10.3 certificate profile</p> <p>Updated Section 10.9 to reflect 1 hour or less nextUpdate attribute value</p>

## Version 2.5

Version	Date	Revised By	Summary of Changes/Comments
2.1	01 May 2006	T. Zagar	<p>Updated Section 2.1 to agree with Section 10 certificate profiles on required use of HTTP and LDAP access methods</p> <p>Amended Sections 9.3.3, 9.4.6, and 9.4.7 to allow Member and Issuer rules consistent with the SAFE-BIOPHARMA Operating Policies to also be used</p> <p>Changed Section 10.2 to allow calssuer attribute in AIA extension of root CA certificates</p> <p>Added Basic Subscriber certificate profile to Section 10</p> <p>Permit optional use of nonce in OCSP request profile</p> <p>Changed Sections 10.1 and 10.2 to permit both medium and basic assurance policies in cross certificates as appropriate</p> <p>Added additional user notice examples for OCSP certificates in Section 10.7</p> <p>Modified footnote regarding nextUpdate in Section 10.10 to agree with the Section 4.9.7 requirement for CRLs</p>
2.11	29 Oct 2006	S. Chokhani	<p>Updated to include encryption certificates</p> <p>Updated to include software certificates</p> <p>Updated based on FBCA policy mapping</p>
2.12	20 Nov 2006	S. Chokhani	Incorporate SAFE- BioPharma Members' input
2.13	30 Nov 2006	S. Chokhani	Incorporate additional SAFE Members' input
2.14	12 Dec 2006	S. Chokhani	Incorporate additional SAFE Members' input
2.15	05 Apr 2007	S. Chokhani	Incorporate FBCA Requirements
2.16	17 Sep 2007	S. Chokhani	Permit Root to be 20 years and remove Common Criteria requirement for cryptographic modules
2.17	25 Sep 2007	S. Chokhani	Align profiles in Section 10 for consistency
2.18	08 Jan 2008	S. Chokhani	Added basic assurance level
2.191	27 Feb 2008	S. Chokhani	Added controls for roaming certificates and made editorial changes.
2.2	10 Mar 2008	T. Zagar	Incorporated reviewer comments and clarified definitions for CCS.
2.3	09 April 2008	T. Zagar	Updated OCSP request and response profiles in Section 10 to better align with RFC 2560.
2.4	04 March 2009	S. Chokhani	<p>Updated to address issues and changes based on regular review of the CP</p> <p>Updated to address 2009 FBCA CP mapping recommendations</p>
2.5	12 March 2010	J. Schoonmaker	Section 3.2.3.1: Antecedent, In-Person process definition -- supplemental

## Approval Statements

Once signed by the parties indicated below, this SAFE- BioPharma Certificate Policy document is approved by the SAFE- BioPharma Policy Approval Authority (PAA) and is incorporated into the SAFE- BioPharma Standard Document Set.

---

*SAFE- BioPharma PAA Chairperson*

*Gary Secrest*

---

*Date*

**TABLE OF CONTENTS**

**DOCUMENT CONTROL..... 2**

**APPROVAL STATEMENTS ..... 5**

**1. INTRODUCTION..... 14**

1.1 OVERVIEW ..... 14

1.1.1 *Certificate Policy (CP)*..... 15

1.1.2 *Relationship between the SAFE CP & the SBCA CPS*..... 15

1.1.3 *Relationship between the SAFE CP and the Issuer CP* ..... 15

1.1.4 *Relationship between the SAFE CP and the SAFE Standard* ..... 15

1.1.5 *Scope* ..... 16

1.1.6 *Interaction with PKIs External to SAFE*..... 16

1.2 IDENTIFICATION ..... 16

1.3 PKI ENTITIES ..... 17

1.3.1 *PKI Authorities*..... 17

1.3.2 *Registration Authority (RA)*..... 18

1.3.3 *Subscribers*..... 18

1.3.4 *Relying Parties* ..... 19

1.3.5 *Other Participants*..... 19

1.4 CERTIFICATE USAGE..... 20

1.4.1 *Appropriate Certificate Uses*..... 20

1.4.2 *Prohibited Certificate Uses* ..... 20

1.5 POLICY ADMINISTRATION..... 20

1.5.1 *Issuer Administering the Document*..... 20

1.5.2 *Contact Person*..... 20

1.5.3 *Person Determining CPS Suitability for the Policy*..... 20

1.5.4 *CPS Approval Procedures*..... 21

**2. PUBLICATION & REPOSITORY RESPONSIBILITIES..... 21**

2.1 REPOSITORIES ..... 21

2.1.1 *Repository Obligations*..... 21

2.2 PUBLICATION OF CERTIFICATION INFORMATION ..... 21

2.2.1 *Publication of Certificates and Certificate Status* ..... 21

2.2.2 *Publication of CA Information* ..... 22

2.2.3 *Interoperability* ..... 22

2.3 FREQUENCY OF PUBLICATION ..... 22

2.4 ACCESS CONTROLS ON REPOSITORIES ..... 22

**3. IDENTIFICATION & AUTHENTICATION ..... 23**

3.1 NAMING ..... 23

3.1.1 *Types of Names* ..... 23

3.1.2 *Need for Names to be Meaningful* ..... 23

3.1.3 *Anonymity or Pseudonymity of Subscribers* ..... 23

3.1.4 *Rules for Interpreting Various Name Forms* ..... 23

3.1.5 *Uniqueness of Names* ..... 23

## Version 2.5

---

3.1.6	<i>Recognition, Authentication, &amp; Role of Trademarks</i>	24
3.2	INITIAL IDENTITY-PROOFING	24
3.2.1	<i>Method to Prove Possession of Private Key</i>	24
3.2.2	<i>Authentication of Issuer Identity</i>	24
3.2.3	<i>Identity-Proofing of Individual Identity</i>	24
3.2.4	<i>Non-verified Subscriber Information</i>	26
3.2.5	<i>Validation of Authority</i>	27
3.2.6	<i>Criteria for Interoperation</i>	27
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	27
3.3.1	<i>Identification and Authentication for Routine Re-key</i>	27
3.3.2	<i>Identification and Authentication for Re-key after Revocation</i>	27
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	27
<b>4.</b>	<b>CERTIFICATE LIFE-CYCLE</b>	<b>28</b>
4.1	APPLICATION	28
4.1.1	<i>Submission of Certificate Application</i>	28
4.1.2	<i>Enrollment Process and Responsibilities</i>	29
4.2	CERTIFICATE APPLICATION PROCESSING	29
4.2.1	<i>Performing Identity-proofing Functions</i>	29
4.2.2	<i>Approval or Rejection of Certificate Applications</i>	29
4.2.3	<i>Time to Process Certificate Applications</i>	29
4.3	ISSUANCE	29
4.3.1	<i>CA Actions During Certificate Issuance</i>	29
4.3.2	<i>Notification to Subscriber of Certificate Issuance</i>	30
4.4	ACCEPTANCE	30
4.4.1	<i>Conduct Constituting Certificate Acceptance</i>	30
4.4.2	<i>Publication of the Certificate by the CA</i>	30
4.4.3	<i>Notification of Certificate Issuance by the CA to Other Entities</i>	30
4.5	KEY PAIR AND CERTIFICATE USAGE	30
4.5.1	<i>Subscriber Private Key and Certificate Usage</i>	30
4.5.2	<i>Relying Party Public Key and Certificate Usage</i>	30
4.6	CERTIFICATE RENEWAL	31
4.6.1	<i>Circumstance for Certificate Renewal</i>	31
4.6.2	<i>Who May Request Renewal</i>	31
4.6.3	<i>Processing Certificate Renewal Requests</i>	31
4.6.4	<i>Notification of New Certificate issuance to Subscriber</i>	31
4.6.5	<i>Conduct Constituting Acceptance of a Renewed Certificate</i>	31
4.6.6	<i>Publication of the Renewal Certificate by the CA</i>	31
4.6.7	<i>Notification of Certificate Issuance by the CA to Other Entities</i>	32
4.7	CERTIFICATE RE-KEY	32
4.7.1	<i>Circumstance for Certificate Re-key</i>	32
4.7.2	<i>Who May Request Certification of a New Public Key</i>	32
4.7.3	<i>Processing Certificate Re-keying Requests</i>	32
4.7.4	<i>Notification of New Certificate Issuance to Subscriber</i>	32
4.7.5	<i>Conduct Constituting Acceptance of a Re-keyed Certificate</i>	32
4.7.6	<i>Publication of the Re-keyed Certificate by the CA</i>	32
4.7.7	<i>Notification of Certificate Issuance by the CA to Other Entities</i>	33

## Version 2.5

---

4.8	CERTIFICATE MODIFICATION .....	33
4.8.1	<i>Circumstance for Certificate Modification .....</i>	33
4.8.2	<i>Who May Request Certificate Modification .....</i>	33
4.8.3	<i>Processing Certificate Modification Requests.....</i>	33
4.8.4	<i>Notification of New Certificate Issuance to Subscriber .....</i>	33
4.8.5	<i>Conduct Constituting Acceptance of Modified Certificate .....</i>	34
4.8.6	<i>Publication of the Modified Certificate by the CA.....</i>	34
4.8.7	<i>Notification of Certificate Issuance by the CA to Other Entities .....</i>	34
4.9	REVOCATION & SUSPENSION.....	34
4.9.1	<i>Circumstance for Revocation of a Certificate.....</i>	34
4.9.2	<i>Who Can Request Revocation of a Certificate .....</i>	34
4.9.3	<i>Procedure for Revocation Request.....</i>	35
4.9.4	<i>Revocation Request Grace Period .....</i>	35
4.9.5	<i>Time within which CA must Process the Revocation Request.....</i>	35
4.9.6	<i>Revocation Checking Requirements for Relying Parties .....</i>	36
4.9.7	<i>CRL Issuance Frequency .....</i>	36
4.9.8	<i>Maximum Latency of CRLs.....</i>	36
4.9.9	<i>Online Revocation Checking Availability.....</i>	36
4.9.10	<i>Online Revocation Checking Requirements.....</i>	36
4.9.11	<i>Other Forms of Revocation Advertisements Available .....</i>	36
4.9.12	<i>Special Requirements Related To Key Compromise .....</i>	37
4.9.13	<i>Circumstances for Suspension.....</i>	37
4.9.14	<i>Who can Request Suspension .....</i>	37
4.9.15	<i>Procedure for Suspension Request.....</i>	37
4.9.16	<i>Limits on Suspension Period.....</i>	37
4.10	CERTIFICATE STATUS SERVICES.....	37
4.10.1	<i>Operational Characteristics .....</i>	37
4.10.2	<i>Service Availability .....</i>	37
4.10.3	<i>Optional Features.....</i>	37
4.11	END OF SUBSCRIPTION .....	38
4.12	KEY ESCROW & RECOVERY .....	38
4.12.1	<i>Key Escrow and Recovery Policy and Practices .....</i>	38
4.12.2	<i>Session Key Encapsulation and Recovery Policy and Practices.....</i>	38
<b>5.</b>	<b>FACILITY MANAGEMENT &amp; OPERATIONS CONTROLS .....</b>	<b>39</b>
5.1	PHYSICAL CONTROLS .....	39
5.1.1	<i>Site Location &amp; Construction .....</i>	39
5.1.2	<i>Physical Access.....</i>	39
5.1.3	<i>Power and Air Conditioning .....</i>	40
5.1.4	<i>Water Exposures .....</i>	40
5.1.5	<i>Fire Prevention &amp; Protection.....</i>	40
5.1.6	<i>Media Storage .....</i>	40
5.1.7	<i>Waste Disposal.....</i>	40
5.1.8	<i>Off-Site backup.....</i>	41
5.2	PROCEDURAL CONTROLS.....	41
5.2.1	<i>Trusted Roles .....</i>	41
5.2.2	<i>Number of Persons Required per Task .....</i>	44

## Version 2.5

---

5.2.3	<i>Identity-proofing for Each Role</i> .....	44
5.2.4	<i>Separation of Roles</i> .....	44
5.3	PERSONNEL CONTROLS .....	45
5.3.1	<i>Background, Qualifications, Experience, &amp; Security Clearance Requirements</i> .....	45
5.3.2	<i>Background Check Procedures</i> .....	45
5.3.3	<i>Training Requirements</i> .....	45
5.3.4	<i>Retraining Frequency &amp; Requirements</i> .....	46
5.3.5	<i>Job Rotation Frequency &amp; Sequence</i> .....	46
5.3.6	<i>Sanctions for Unauthorized Actions</i> .....	46
5.3.7	<i>Contracting Personnel Requirements</i> .....	46
5.3.8	<i>Documentation Supplied To Personnel</i> .....	46
5.4	AUDIT .....	46
5.4.1	<i>Types of Events Recorded</i> .....	46
5.4.2	<i>Frequency of Processing Data</i> .....	50
5.4.3	<i>Retention Period for Security Audit Data</i> .....	50
5.4.4	<i>Protection of Security Audit Data</i> .....	50
5.4.5	<i>Security Audit Data Backup Procedures</i> .....	51
5.4.6	<i>Security Audit Collection System (Internal or External)</i> .....	51
5.4.7	<i>Notification to Event-Causing Subject</i> .....	51
5.4.8	<i>Vulnerability Assessments</i> .....	51
5.5	ARCHIVE .....	51
5.5.1	<i>Types of Events Archived</i> .....	51
5.5.2	<i>Retention Period for Archive</i> .....	52
5.5.3	<i>Protection of Archive</i> .....	52
5.5.4	<i>Archive Backup Procedures</i> .....	52
5.5.5	<i>Requirements for Time-Stamping of Records</i> .....	53
5.5.6	<i>Archive Collection System (Internal or External)</i> .....	53
5.5.7	<i>Procedures to Obtain &amp; Verify Archive Information</i> .....	53
5.6	KEY CHANGEOVER .....	53
5.7	COMPROMISE & DISASTER RECOVERY .....	53
5.7.1	<i>Incident and Compromise Handling Procedures</i> .....	53
5.7.2	<i>Computing Resources, Software, and/or Data Are Corrupted</i> .....	54
5.7.3	<i>CA Private Key Compromise Recovery Procedures</i> .....	54
5.7.4	<i>Business Continuity Capabilities after a Disaster</i> .....	54
5.8	CA & RA TERMINATION .....	55
5.8.1	<i>CA Termination</i> .....	55
5.8.2	<i>RA Termination</i> .....	56
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS</b> .....	<b>57</b>
6.1	KEY PAIR GENERATION & INSTALLATION.....	57
6.1.1	<i>Key Pair Generation</i> .....	57
6.1.2	<i>Private Key Delivery to Subscriber</i> .....	57
6.1.3	<i>Public Key Delivery to Certificate Issuer</i> .....	58
6.1.4	<i>CA Public Key Delivery to Relying Parties</i> .....	58
6.1.5	<i>Key Sizes</i> .....	58
6.1.6	<i>Public Key Parameters Generation and Quality Checking</i> .....	59

## Version 2.5

---

6.1.7	Key Usage Purposes (as per X.509 v3 key usage field).....	59
6.2	PRIVATE KEY PROTECTION & CRYPTO-MODULE ENGINEERING CONTROLS .....	59
6.2.1	Cryptographic Module Standards & Controls.....	59
6.2.2	CA Private Key Multi-Person Control.....	60
6.2.3	Private Key Escrow .....	60
6.2.4	Private Key Backup .....	60
6.2.5	Private Key Archival .....	60
6.2.6	Private Key Transfer into or from a Cryptographic Module.....	60
6.2.7	Private Key Storage on Cryptographic Module.....	61
6.2.8	Method of Activating Private Keys.....	61
6.2.9	Methods of Deactivating Private Keys.....	61
6.2.10	Method of Destroying Private Keys .....	61
6.2.11	Cryptographic Module Rating.....	61
6.3	OTHER ASPECTS OF KEY MANAGEMENT.....	61
6.3.1	Public Key Archive.....	61
6.3.2	Certificate Operational Periods and Key Usage Periods .....	62
6.3.3	Subscriber Private Key Usage Environment.....	62
6.4	ACTIVATION DATA.....	62
6.4.1	Activation Data Generation & Installation .....	62
6.4.2	Activation Data Protection .....	62
6.4.3	Other Aspects of Activation Data.....	62
6.5	COMPUTER SECURITY CONTROLS.....	63
6.5.1	Specific Computer Security Technical Requirements.....	63
6.5.2	Computer Security Rating.....	63
6.6	LIFE-CYCLE SECURITY CONTROLS.....	63
6.6.1	System Development Controls .....	63
6.6.2	Security Management Controls .....	64
6.6.3	Life Cycle Security Ratings.....	64
6.7	NETWORK SECURITY CONTROLS .....	65
6.8	TIME STAMPING.....	65
<b>7.</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES.....</b>	<b>66</b>
7.1	CERTIFICATE PROFILE.....	66
7.1.1	Version Numbers.....	66
7.1.2	Certificate Extensions.....	66
7.1.3	Algorithm Object Identifiers.....	66
7.1.4	Name Forms.....	66
7.1.5	Name Constraints.....	68
7.1.6	Certificate Policy Object Identifier.....	69
7.1.7	Usage of Policy Constraints Extension.....	69
7.1.8	Policy Qualifiers Syntax & Semantics.....	70
7.1.9	Processing Semantics for the Critical Certificate Policy Extension.....	70
7.2	CRL PROFILE .....	70
7.2.1	Version Numbers.....	70
7.2.2	CRL & CRL Entry Extensions .....	70
7.3	OCSP PROFILE .....	70
7.3.1	Version Number.....	70

7.3.2 OCSP Extensions..... 70

**8. COMPLIANCE AUDIT & OTHER ASSESSMENTS ..... 71**

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS..... 71

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR..... 71

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY ..... 71

8.4 TOPICS COVERED BY ASSESSMENT ..... 71

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY ..... 71

8.6 COMMUNICATION OF RESULTS ..... 72

**9. OTHER BUSINESS & LEGAL MATTERS..... 73**

9.1 FEES ..... 73

9.1.1 Certificate Issuance/Renewal Fee ..... 73

9.1.2 Certificate Access Fees..... 73

9.1.3 Revocation or Status Information Access Fee..... 73

9.1.4 Fees for Other Services..... 73

9.1.5 Refund Policy ..... 73

9.2 FINANCIAL RESPONSIBILITY ..... 73

9.2.1 Insurance Coverage ..... 74

9.2.2 Other Assets..... 74

9.2.3 Insurance/warranty Coverage for End-Entities ..... 74

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ..... 74

9.3.1 Scope of Confidential Information..... 74

9.3.2 Information not within the Scope of Confidential Information..... 74

9.3.3 Responsibility to Protect Confidential Information ..... 74

9.4 PRIVACY OF PERSONAL INFORMATION ..... 74

9.4.1 Privacy Plan..... 74

9.4.2 Information treated as Private..... 74

9.4.3 Information not deemed Private..... 75

9.4.4 Responsibility to Protect Private Information ..... 75

9.4.5 Notice and Consent to Use Private Information..... 75

9.4.6 Disclosure Pursuant to Judicial/Administrative Process ..... 75

9.4.7 Other Information Disclosure Circumstances ..... 75

9.5 INTELLECTUAL PROPERTY RIGHTS ..... 75

9.6 REPRESENTATIONS & WARRANTIES ..... 75

9.6.1 CA Representations and Warranties ..... 75

9.6.2 RA Representations and Warranties ..... 76

9.6.3 Subscriber Representations and Warranties ..... 76

9.6.4 Relying Parties Representations and Warranties ..... 77

9.6.5 Representations and Warranties of other Participants ..... 77

9.7 DISCLAIMERS OF WARRANTIES..... 77

9.8 LIMITATIONS OF LIABILITY ..... 78

9.9 INDEMNITIES..... 78

9.10 TERM & TERMINATION ..... 78

9.10.1 Term..... 78

9.10.2 Termination ..... 78

9.10.3 Effect of Termination and Survival..... 78

## Version 2.5

---

9.11	INDIVIDUAL NOTICES & COMMUNICATIONS .....	78
9.12	AMENDMENTS .....	78
9.12.1	<i>Procedure for Amendment</i> .....	78
9.12.2	<i>Notification Mechanism and Period</i> .....	78
9.12.3	<i>Circumstances under which OID must be changed</i> .....	79
9.13	DISPUTE RESOLUTION PROVISIONS .....	79
9.14	GOVERNING LAW .....	79
9.15	COMPLIANCE WITH APPLICABLE LAW .....	79
9.16	MISCELLANEOUS PROVISIONS .....	79
9.16.1	<i>Entire agreement</i> .....	79
9.16.2	<i>Assignment</i> .....	79
9.16.3	<i>Severability</i> .....	79
9.16.4	<i>Enforcement (Attorney Fees/Waiver of Rights)</i> .....	79
9.16.5	<i>Force Majeure</i> .....	80
9.17	OTHER PROVISIONS .....	80
9.17.1	<i>Fiduciary relationships</i> .....	80
9.17.2	<i>Administrative processes</i> .....	80
<b>10.</b>	<b>CERTIFICATE, CRL, AND OCSP FORMATS .....</b>	<b>81</b>
10.1	SBCA → PRINCIPAL CA CERTIFICATE .....	82
10.2	PRINCIPAL CA → SBCA CERTIFICATE .....	84
10.3	ISSUER CA CERTIFICATE .....	85
10.4	HUMAN SUBSCRIBER SIGNATURE CERTIFICATE .....	86
10.5	MACHINE CERTIFICATE .....	87
10.6	HUMAN SUBSCRIBER ENCRYPTION CERTIFICATE .....	88
10.7	OCSP RESPONDER CERTIFICATE .....	89
10.8	CRL FORMAT .....	90
10.9	OCSP REQUEST FORMAT .....	91
10.10	OCSP RESPONSE FORMAT .....	91
<b>11.</b>	<b>DIRECTORY INTEROPERABILITY PROFILE .....</b>	<b>93</b>
11.1	PROTOCOL .....	93
11.2	AUTHENTICATION .....	93
11.3	NAMING .....	93
11.4	OBJECT CLASS .....	93
11.5	ATTRIBUTES .....	94
<b>12.</b>	<b>REFERENCES .....</b>	<b>95</b>
<b>13.</b>	<b>ACRONYMS &amp; ABBREVIATIONS .....</b>	<b>96</b>
<b>14.</b>	<b>GLOSSARY .....</b>	<b>98</b>
<b>15.</b>	<b>SAFE STANDARD APPLICABILITY TO THE SAFE CP .....</b>	<b>101</b>



## 1. Introduction

The Signatures and Authentication For Everyone (SAFE) Standard arose from an initiative sponsored by the Pharmaceutical Research and Manufacturers of America (PhRMA). The SAFE- BioPharma Standard provides the framework for assured electronic identity and supports legally binding, regulatory compliant Digital Signatures. The scope of this framework is business-to-business and business-to-regulator transactions across the bio-pharmaceutical community.

SAFE- BioPharma operates as a closed business system model. SAFE- BioPharma utilizes Digital Certificates issued by Certification Authorities (CAs) meeting rules established by the SAFE-BioPharma Association. These Issuers may be internal to a bio-pharmaceutical company, or may be operated by a third-party provider. The intention is that these Digital Certificates will support Digital Signatures on documents and transactions needed to comply with global regulatory and legal requirements. SAFE- BioPharma will also support confidentiality of documents and transactions through the use of encryption certificates. Because SAFE- BioPharma is to support the interoperation of Digital Certificates across these different enterprise Public Key Infrastructures (PKIs), SAFE- BioPharma will employ a SAFE Bridge Certification Authority (SBCA) to cross-certify with each Principal (generally, but not necessarily, the Root) CA of each Issuer in the SAFE- BioPharma network. As required for interoperation with government regulatory authorities, SBCA will also seek to cross-certify with Regional Bridge Certification Authorities (RBCAs) in order to permit others who are also cross-certified with the RBCAs to trust Digital Certificates meeting the SAFE- BioPharma Standard.

This Certificate Policy (CP) complies with the Internet Request for Comment (RFC) 3647 [RFC 3647]. For purposes of this SAFE CP, all terms used shall have the meanings set forth in the SAFE-BioPharma System Documentation Glossary.

### 1.1 Overview

Assurance level, as defined by the U.S. Federal PKI taxonomy, refers to the:

- Strength of the binding between a Public Key and the individual whose Subject name is cited in the Certificate
- Mechanisms used to control the use of the Private Key
- Security provided by the PKI itself.

The SAFE CP defines three assurance levels for use by SAFE- BioPharma participants:

1. The medium hardware assurance level for Digital Certificates issued to Subscribers (also known as End Entities)
2. The medium software assurance level for Digital Certificates issued to Subscribers
3. The basic assurance level for Digital Certificates issued to Subscribers

A SAFE- BioPharma Policy Approval Authority (PAA) has responsibility for directing the development of this CP, and for approving it and any updates to it. SAFE-BioPharma has overall responsibility for the development and operation of the SBCA.

Any use of or reference to this CP outside the context of SAFE-accredited Issuer is completely at the using party's risk. An Issuer shall not assert the object identifiers (OIDs), listed in Section 1.2 of this CP, in any certificates their CAs issue, except in the *policyMappings* extension for certificates issued to the SBCA, and then only upon approval by the PAA.

The terms and provisions of this CP shall be interpreted under and governed by the SAFE-BioPharma Operating Policies.

Where this CP refers to a "CA," that term shall be interpreted to include the SBCA, and any Issuer CA whose PKI is cross-certified with the SBCA. Where a more specific or limited interpretation is required (e.g., just referring to the SBCA, or to an Issuer's Principal CA, Issuer's root CA, or Issuer's signing CA that is neither a Principal CA nor root CA), this CP will so indicate.

### **1.1.1 Certificate Policy (CP)**

X.509 certificates shall contain one or more registered certificate policy OIDs in the certificate policy extension that in turn shall be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. The OIDs correspond to specific levels of assurance established by a CP that should be available to Relying Parties. Certificates issued by a CA shall assert the appropriate assurance level in the *certificatePolicies* extension by including applicable OID(s).

### **1.1.2 Relationship between the SAFE CP & the SBCA CPS**

This CP states what assurance can be placed in a Certificate issued by the SBCA or any Issuer's CA within SAFE- BioPharma that cross-certifies with the SBCA. The SBCA Certification Practices Statement (CPS) shall state how the SBCA meets the requirements of this CP for certificates issued by the SBCA.

### **1.1.3 Relationship between the SAFE CP and the Issuer CP**

The PAA has responsibility for mapping the CPs of the Issuers cross-certifying with the SBCA. The relationship between this CP and the Issuer CP is asserted in CA certificates issued by or to the SBCA in the *policyMappings* extension. This extension shall indicate that the SAFE-BioPharma policy is equivalent to one or more policies of the Issuer. Conflicts between this CP and an Issuer's CP shall be resolved at the time of CP mapping for cross certification. The Issuer shall submit one or more waivers to identify the timeframe for conflict resolution for PAA approval.

### **1.1.4 Relationship between the SAFE CP and the SAFE Standard**

The SAFE CP is one document within the overall SAFE- BioPharma Standard document set. In addition to the requirements indicated in this CP, the requirements of the other documents in the SAFE- BioPharma Standard shall also apply. Section 15 identifies which other SAFE- BioPharma Standard documents apply to specific CP paragraphs. If conflicts arise at a later date concerning any technical elements covered in the SAFE CP and another SAFE- BioPharma Standard document, the SAFE CP shall take precedence.

### 1.1.5 Scope

The SBCA exists to facilitate trusted electronic business activities among SAFE- BioPharma Members, between SAFE- BioPharma Members and their partners, and between SAFE- BioPharma Members and Regional Regulators. The term Issuer applies to any SAFE- BioPharma Issuer permitted by the SAFE- BioPharma PAA to cross-certify its PKI with the SBCA and to issue certificates that map to one or more of the certificate policy OIDs listed in this CP. Thus, within the SAFE- BioPharma context, an Issuer may include a SAFE- BioPharma Member that operates its own PKI, or an external supplier to a SAFE- BioPharma Member that operates a PKI and supplies Certificates as directed by the SAFE- BioPharma Member.

The scope of this CP also includes Bridge CAs with which the SBCA may cross certify.

### 1.1.6 Interaction with PKIs External to SAFE

The SBCA will extend interoperability to non-SAFE- BioPharma Issuers as determined by the SAFE- BioPharma PAA and only when it is beneficial to the SAFE- BioPharma community. For example, as required, the SBCA may choose to interoperate with the Federal Bridge CA (FBCA) to facilitate the ability of the Food and Drug Administration (FDA) to verify Digital Signatures associated with regulatory submissions. SBCA's method for interoperability is cross-certification with CAs of other domains.

## 1.2 Identification

There are three assurance levels expressed in this Certificate Policy. These are defined in subsequent sections. The SBCA policy OID is registered in the Internet Assigned Numbers Authority (IANA) Objects Registry as follows:

sbca OBJECT IDENTIFIER	::= { 1.3.6.1.4.1.23165 }
sbca-cert-policies OBJECT IDENTIFIER	::= { sbca 1 }
id-sbca-cert-policies-basicAssurance	::= { sbca-cert-policies 1 }
id-sbca-cert-policies-mediumSoftwareAssurance	::= { sbca-cert-policies 2 }
id-sbca-cert-policies-mediumHardwareAssurance	::= { sbca-cert-policies 3 }

An Issuer's CA shall assert an OID corresponding to the appropriate assurance level in the *certificatePolicies* extension of the Certificates issued to its Subscribers. To indicate correspondence of these Issuer OIDs with the above defined SBCA policy OIDs, the SBCA's policy OID shall be asserted in the *issuerDomainPolicy* field(s) and the Issuer's policy OID in the *subjectDomainPolicy* field(s) of the *policyMapping* extension of the certificates issued by the SBCA to the Issuer's CA. The SBCA policy OID shall also be asserted in the *subjectDomainPolicy* field(s) and the Issuer's policy OID shall be asserted in the *issuerDomainPolicy* field(s) of the *policyMapping* extension of the certificates issued by Issuer's CAs to the SBCA.

SAFE- BioPharma Subscriber certificates issued at a medium hardware assurance level in accordance with this CP shall serve the purpose of a Qualified Certificate in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC.

### **1.3 PKI Entities**

The SAFE- BioPharma PKI is defined as the SBCA and the cross-certified Issuer PKIs. Note that this CP specifically applies to Certificates issued by the SBCA and to the operation of the SBCA, but also contains provisions relevant to PKIs wishing to cross-certify with the SBCA, apprising them of requirements which they must meet in order to successfully request cross-certification.

CAs, Certificate Status Authorities (CSAs), Registration Authorities (RAs) and Trusted Agents are also called “PKI components” in this CP, or may be referred to simply as “components.”

The following roles are relevant to the SAFE- BioPharma PKI.

#### **1.3.1 PKI Authorities**

##### **1.3.1.1 SAFE Policy Approval Authority (PAA)**

The PAA is a group of individuals chartered by the SAFE- BioPharma Standard and selected by the SAFE-BioPharma Board of Directors. With respect to this CP, the PAA is responsible for:

- Review, maintenance, clarification, approval, and updates to this SAFE CP,
- Approval of the SBCA CPS,
- Review and approval of applications from SAFE- BioPharma Members and other Issuers desiring to cross certify with the SBCA, to include determination of the CP equivalency mapping between the applicant Issuer’s CP and this CP,
- Approval of the contract agreement (or any amended contract agreement) between each Issuer and SAFE-BioPharma setting forth the respective responsibilities and obligations of both parties, and
- After an Issuer is cross certified with the SBCA, confirmation of continued conformance of that Issuer’s PKI with SAFE- BioPharma requirements as a condition for allowing continued cross certification with the SBCA.

##### **1.3.1.2 SBCA Operational Authority (SBCA OA)**

The SBCA Operational Authority is the Issuer that operates and maintains the SBCA on behalf of SAFE-BioPharma and under direction from the PAA.

##### **1.3.1.3 SBCA OA Program Manager**

The Program Manager is the individual within the SBCA OA who has principal responsibility for overseeing the proper operation of the SBCA including the SBCA repository, and selecting the SBCA OA personnel who will have roles in operating the SBCA as set forth in this CP. The Program Manager requires PAA approval.

##### **1.3.1.4 SAFE Bridge Certification Authority (SBCA)**

The SBCA is the CA operated by the SBCA OA and is authorized by the PAA to create, sign, and issue Public Key Certificates to Principal CAs (see Section 1.3.1.5 for definition and

description of Principal CAs). As operated by the SBCA OA, the SBCA is responsible for all aspects of the issuance and management of certificates it issues including:

- Control over the registration process,
- The identification and authentication process,
- The Certificate generation process,
- Publication of Certificates to Issuer CAs and OCSP Responders,
- Revocation of all certificates issued,
- Publication of revocation information,
- Re-key of SBCA signing material,
- Establishment and maintenance of the SBCA CPS in accordance with this SAFE CP, and
- Performance of all aspects of the SBCA services, operations and infrastructure related to Certificates issued under this CP, in accordance with the requirements, representations, and warranties of this CP, and in accordance with the SBCA CPS.

### **1.3.1.5 Issuer Principal Certification Authority (CA)**

A Principal CA is a CA within a PKI that has been designated to cross certify with the SBCA. The Principal CA may issue either end-entity Certificates, or CA certificates to other Issuer or external party CAs, or both. Where the Issuer operates a hierarchical PKI, the Principal CA is typically the Issuer Root CA, but may be a CA subordinate to the Root CA. Where the Issuer operates a mesh PKI, the Principal CA may be any CA designated by the Issuer for cross certification with the SBCA.

It should be noted that an Issuer may request that the SBCA cross certify with more than one CA within the Issuer; that is, an Issuer may have more than one Principal CA.

This CP also applies to CAs that are “subordinate” to the Principal CA.

### **1.3.1.6 Issuer Certification Authority (CA)**

An Issuer CA or “subordinate CA” shall encompass any CA under the control of the Issuer that has a Certificate issued to it by the Issuer Principal CA or any CA subordinate to the Principal CA, whether or not the Issuer employs a hierarchical or other PKI architecture.

### **1.3.2 Registration Authority (RA)**

The RA collects and verifies each Subscriber’s identity and information for inclusion in the Subscriber’s certificate. The SBCA OA acts as the RA for the SBCA, and performs its function in accordance with a CPS prepared by the SBCA OA and approved by the PAA. Issuer Principal CAs and subordinate CAs shall designate their own RAs or delegate that functions to an appropriate third party. The requirements for RAs in the SBCA and Issuer PKIs are set forth elsewhere in this document.

### **1.3.3 Subscribers**

A Subscriber is the SAFE- BioPharma User to whom or to which a Digital Certificate is issued. SAFE- BioPharma Subscribers may include:

- SAFE- BioPharma Users of a SAFE- BioPharma Member requiring a Certificate for use in accordance with SAFE- BioPharma operating rules.

- An Issuer's Users,
- Machine subscribers.
- PKI operations personnel at the SBCA, various Principal CAs, and various CAs

Note that while CAs are sometimes considered "subscribers" in a PKI, for the purposes of this CP, the term "Subscriber" refers only to end-entities.

### **1.3.4 Relying Parties**

A Relying Party uses a Subscriber's Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, to authenticate a subscriber, or to establish confidential communications with the Subscriber.

Only those Relying Parties with an established contractual agreement with SAFE-BioPharma are subject to that agreement's provisions for reliance on a SAFE- BioPharma signature (that is, a signature based on a Certificate issued by an Issuer meeting SAFE- BioPharma requirements). Further, such Relying Party must meet requirements prescribed by the SAFE- BioPharma Standard for signature validation.

The foregoing paragraph does not prevent other relying parties from relying on SAFE-BioPharma PKI issued certificates; however, the SAFE- BioPharma Signature rules and provisions do not apply to relying parties not subject to a contractual agreement with SAFE-BioPharma.

### **1.3.5 Other Participants**

The SBCA and Issuer CAs may require the services of other security, community, and application authorities. If required, the applicable CPS shall identify the parties, define the services, and designate the mechanisms used to support these services. Examples of other participants include compliance auditors, Trusted Agents (TAs), Machine Operators, and Local Registration Authorities (LRA).

#### **1.3.5.1 Local Registration Authority (LRA)**

The LRA duties are similar to the duties of the RA. LRA may service a limited population as authorized by the RA. LRA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's certificate. The requirements for LRAs in the SBCA and Issuer PKIs are set forth in this document.

#### **1.3.5.2 Trusted Agent (TA)**

The TA collects and verifies each Subscriber's identity in support of the Subscriber registration. The TA shall work closely with an RA or LRA to support Subscriber registration. The requirements for TAs in the SBCA and Issuer PKIs are set forth elsewhere in this document.

#### **1.3.5.3 Certificate Status Authority (CSA)**

Server based Certificate Status Authorities (CSAs) such as Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. The SBCA and Issuer PKIs shall make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The SBCA shall also publish status information for the certificates it issues in a Certificate Revocation List (CRL)

### **1.3.5.4 Machine Operator**

The Machine Operator shall serve as the representative of a Machine Subscriber to an RA or LRA in order to register the Machine Subscriber with the PKI. The requirements for Machine Operators in the SBCA and Issuer PKIs are set forth elsewhere in this document.

### **1.3.5.5 Centralized Credential Server (CCS)**

The private keys for multiple subscribers may be stored on a central credential server, or CCS, based on either a hardware security module (HSM) interfaced to a server, or a software-protected set of private keys in a controlled server environment. This permits these subscribers to access their credentials from multiple workstations and locations. For the purposes of this CP, any centralized aggregation of subscriber private keys must comply with the requirements for a CCS as specified in this CP.

## **1.4 Certificate Usage**

### **1.4.1 Appropriate Certificate Uses**

The use of any Certificates issued by Issuers pursuant to a Member relationship with SAFE-BioPharma, and corresponding contractual relationship with that SAFE- BioPharma Member, and meeting SAFE- BioPharma requirements, shall only be as prescribed by SAFE- BioPharma and set forth in the Agreements between SAFE- BioPharma and its Members and Issuers, along with any separate agreements between such entities that do not conflict with the SAFE- BioPharma requirements. Any other uses of such Certificates, while allowed, shall not be considered as uses within the boundaries of SAFE- BioPharma and shall be solely at the risk of the Participant. The Certificates issued by the SBCA are also subject to these requirements.

### **1.4.2 Prohibited Certificate Uses**

No stipulation.

## **1.5 Policy Administration**

### **1.5.1 Issuer Administering the Document**

The SAFE- BioPharma PAA is responsible for all aspects of this CP.

### **1.5.2 Contact Person**

Questions regarding this CP shall be directed to the Chair of the PAA, whose address can be found on the SAFE-BioPharma website at <http://www.safe-biopharma.org>.

### **1.5.3 Person Determining CPS Suitability for the Policy**

The CPS must conform to the corresponding Certificate Policy. The PAA is responsible for approving the SBCA CPS, thereby confirming that the SBCA conforms to the SBCA CP.

Issuers must designate the person or organization responsible for approving their CPS(s) and confirming that the CPS(s) conform to their CP(s).

In each case, the determination of suitability shall be based on an independent compliance analyst's results and recommendations. The compliance analyst shall be from a firm which is independent from the entity being audited. The compliance analyst may not be the author of the subject CPS. The SAFE- BioPharma PAA shall determine whether a compliance analyst meets these requirements.

### **1.5.4 CPS Approval Procedures**

The SBCA OA shall submit the SBCA CPS and the results of a conformance analysis study to the PAA for approval. The PAA shall accept or reject the CPS and accompanying analysis. If rejected, the SBCA OA shall resolve the identified discrepancies and resubmit the revised CPS to the PAA for approval. This process shall continue until the CPS is approved.

## **2. Publication & Repository Responsibilities**

### **2.1 Repositories**

The SBCA OA shall operate repositories to support SBCA operations. Issuer CAs shall operate repositories to support their PKI operations. Issuers shall ensure interoperability with the SBCA repository so that Relying Parties may obtain Issuer trust path Certificates and CRLs from or through that repository. Certificates must be accessible via HTTP. Certificates may also be made available using LDAPv3 queries (including referrals). CRLs in an Issuer repository shall be accessible via both HTTP and LDAP methods. HTTP only access for CRLs is acceptable if the Issuer and its associated Member(s) agree to accept any limitation this may impose on the use of SAFE-BioPharma Certificates for authentication purposes. Note that making CRLs of Issuer CAs available through the SBCA repository is for the convenience of SAFE- BioPharma Members and Issuers and is not a requirement of this CP.

#### **2.1.1 Repository Obligations**

A variety of mechanisms may be used for posting information into a repository. The repository obligations shall include:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3), or Hypertext Transfer Protocol (HTTP),
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository availability and information as described in later sections.

### **2.2 Publication of Certification Information**

#### **2.2.1 Publication of Certificates and Certificate Status**

The SBCA shall publish all CA certificates and CRLs issued by the SBCA in the SBCA repository. The SBCA shall also publish all the certificates issued to the SBCA.

At a minimum, the Issuer repositories shall contain CA certificates issued to the Issuer PKI, CA certificates issued by the Issuer PKI, and CRLs issued by the Issuer PKI.

### **2.2.2 Publication of CA Information**

The SBCA OA shall publish information concerning the SBCA necessary to support its use and operation. This shall be made available publicly; information on how to obtain a copy of this CP shall be posted on the SAFE-BioPharma website (see <http://www.SAFE-biopharma.org>). The complete SBCA CPS shall not be publicly published; a redacted version of the CPS containing information suitable for disclosure shall be available to SAFE- BioPharma participants from the SBCA website.

The Issuer CP shall be made available to all SAFE- BioPharma Participants. The Issuer CP shall identify the CP publication location. Sections of the Issuer CPS relevant to use by a Relying Party shall also be made available to all SAFE- BioPharma Participants. The Issuer CP shall identify the publication location for the Issuer's redacted CPS. The PAA shall specify the minimum required contents of a redacted CPS.

### **2.2.3 Interoperability**

Where Subscriber Certificates, CA certificates, or CRLs are published in repositories, standards-based schemas for directory objects and attributes shall be employed, specifically LDAPv3, and HTTP protocols. Further requirements are set forth later in this CP.

### **2.3 Frequency of Publication**

This CP and any subsequent changes shall be made available publicly as set forth in Section 2.2.2 within one week of approval by the PAA.

CA certificates and CRLs shall be published upon issuance.

### **2.4 Access Controls on Repositories**

The SBCA and Issuer PKIs shall protect their repository information not intended for public dissemination or modification. Certificates and certificate status information in the SBCA repository shall be made available through the Internet to SAFE- BioPharma Participants and other parties as determined by the PAA.

### **3. Identification & Authentication**

#### **3.1 Naming**

##### **3.1.1 Types of Names**

A CA shall only generate and sign Certificates that contain a non-null subject Distinguished Name (DN) complying with the X.500 standard. Certificates may also include other name forms in the subject alternative name forms field. This CP does not restrict the types of names that can be used in the subject alternative name forms field, but does require that the RFC822 e-mail address of the Subject appear in that field. Details on this may be found in the certificate profiles set forth later in this CP.

##### **3.1.2 Need for Names to be Meaningful**

Names used in the certificates shall identify the person or Machine User to which they are assigned.

When DNs are used, the directory information tree shall accurately reflect organizational structures.

When DNs are used, the common name shall observe name space uniqueness requirements.

Names shall never be misleading. This does not preclude the use of pseudonymous Certificates as defined in Section 3.1.3.

##### **3.1.3 Anonymity or Pseudonymity of Subscribers**

A CA shall not issue anonymous certificates. A CA may issue pseudonymous certificates to internal Subscribers to support its operations. CA certificates shall not contain anonymous or pseudonymous identities.

DNs in end entity certificates issued by Issuer CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

##### **3.1.4 Rules for Interpreting Various Name Forms**

The Issuer's CP shall specify rules for interpreting alternative name forms used. (The rules may be simply a pointer to applicable standards.)

The SBCA as described in the Certificate Profiles in this CP shall only use Uniform Resource Indicators (URIs) in accordance with the applicable Internet Engineering Task Force (IETF) standards.

##### **3.1.5 Uniqueness of Names**

The PAA and Issuer PKI shall enforce name uniqueness.

The PAA shall be responsible for ensuring name uniqueness in certificates issued by the SBCA.

### **3.1.6 Recognition, Authentication, & Role of Trademarks**

A CA shall not knowingly use trademarks in names unless the subject has the rights to use that name.

The PAA shall resolve any name collisions or disputes regarding SBCA-issued certificates brought to its attention.

Issuers shall resolve any name collisions or disputes regarding Issuer Certificates brought to their attention. Any dispute resolution shall be in accordance with the SAFE- BioPharma Operating Policies.

## **3.2 Initial Identity-proofing**

### **3.2.1 Method to Prove Possession of Private Key**

In all cases where the Subscriber named in a Certificate generates its own keys, the Subject shall be required to prove possession of the Private Key that corresponds to the Public Key in the certificate request.

For Signing Keys, the Subscriber may use its Private Key to sign a value and provide that value to the CA issuing the Digital Certificate. The CA shall then validate the signature using the Subject's Public Key.

For encryption keys, this may consist of either: (1) the Subscriber decrypting a CA-provided text; (2) the CA performing a pair-wise consistency check (if the CA performs key escrow); or (3) the CA obtaining conformance of pair-wise consistency check from a trusted source.

The PAA may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated by the CA or RA either (1) directly on the party's hardware or software token, or (2) in a key generator that securely transfers the key to the party's token, then proof of possession is not required.

### **3.2.2 Authentication of Issuer Identity**

Requests for CA certificates in the name of an organization (e.g., a SAFE- BioPharma Issuer) shall include the organization name, address, documentation of the existence of the organization, identity-proofing of the requesting Issuer Agent, and proof of the Agent's authorization to act on behalf of the Issuer. The SBCA Operational Authority or Issuer RA shall verify the information, the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

### **3.2.3 Identity-Proofing of Individual Identity**

#### **3.2.3.1 Identity-Proofing of End User Subscribers**

**For Basic Assurance Level:** The identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, Date of Birth (DoB), address and other personal information in records are consistent with the application and sufficient to identify a unique individual.

## Version 2.5

---

Examples of data that may be verified to meet the stated ID number and account number include: currently-valid credit card number; alien registration number; passport number; currently valid state-issued driver's license number or state-issued identification card number; and social security number.

Address confirmation shall be carried out using:

- Issue credentials in a manner that confirms the address of record supplied by the applicant; or
- Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.

**For Basic Assurance Level:** A Registration Agent (either CA, RA, LRA or TA) shall record the information set forth below for issuance of each Certificate:

- The identity of the Registration Agent performing the identification;
- A signed declaration by the Registration Agent that he or she verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under non-US law;
- Unique ID number(s) provided by the Subscriber, or other unique ID number(s) that are linked directly to the Subscriber, and the names of the databases from which the number(s) were verified;
- The date and time of the verification; and
- A declaration of identity signed by the Subscriber using a handwritten signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

**For Medium Software and Medium Hardware Assurance Levels:** Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or National Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. Credentials required are either one National Government-issued Picture I.D., or two Non-National Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License).

**For Medium Software and Medium Hardware Assurance Levels:** A Registration Agent (either CA, RA, LRA or TA) shall record the information set forth below for issuance of each Certificate:

- The identity of the Registration Agent performing the identification;
- A signed declaration by the Registration Agent that he or she verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under local law;
- A unique identifying number(s) from the ID(s) of the Subscriber (or some other trusted source of information on the Subscriber), or a facsimile of the ID(s);
- The date and time of the verification; and

- A declaration of identity signed by the Subscriber using a handwritten signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

**For All Assurance Levels:** Identity shall be established no more than 30 days before initial certificate issuance.

**For All Assurance Levels:** An entity certified by a National or State Government as being authorized to confirm identities may perform person-to-person identity-proofing on behalf of the RA or LRA. The certified entity, TA, or the applicant shall forward the information collected directly to the RA or LRA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such identity-proofing does not relieve the RA and LRA of its responsibility to verify the presented data. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement.

**[added] Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event can be found in the “SBCA Supplemental Antecedent, In-Person Definition” document.**

### **3.2.3.2 Identity-Proofing of Machine Subscribers**

Machine Users (e.g., routers, firewalls, servers, etc.) may be named as Certificate Subjects. In such cases, the Machine Subscriber shall have a designated human representative called the Machine Operator. The representative shall be responsible for providing the following registration information for the Machine Subscriber:

- Its identification (e.g., serial number) or service name (e.g., DNS name)
- Its public keys
- How it will generate and protect its Private Key (in hardware or software)
- His or her contact information to enable the CA or RA to communicate with the representative as required.

Acceptable methods for performing this authentication and integrity checking are:

- Verification of a digitally signed message sent from the representative (using certificates of medium hardware assurance or greater).
- In person registration by the representative, with the identity of the representative confirmed in accordance with the requirements of Section 3.2.3.1 for Medium Software and Medium Hardware Assurance Levels.

Alternative methods for identity-proofing that provide assurance of identity that is at least as strong as that above may also be employed. If other methods are to be employed, they shall be documented and submitted to the PAA for approval prior to use, and shall only be utilized with approval from the PAA.

### **3.2.4 Non-verified Subscriber Information**

Information that is not verified shall not be included in Certificates.

### **3.2.5 Validation of Authority**

For cross certification, the SBCA OA shall validate (1) an Issuer agent's authorization to act in the name of the Issuer and (2) the PAA approval for the Issuer to cross certify with the SBCA. This cross certification shall be based on successful mapping of the Issuer CP with this CP.

Certificates that contain explicit or implicit Issuer affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the Issuer in the asserted capacity.

### **3.2.6 Criteria for Interoperation**

The Interoperating PKI shall adhere to the following requirements:

- Have a CP mapped to, and determined by the PAA to be in conformance with, the SAFE CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8 of this CP;
- Issue certificates compliant with the profiles described in this CP, and make certificate status information available in accordance with this CP; and
- Provide a publicly accessible directory that interoperates with the SBCA repository

If the Interoperating PKI is a SAFE- BioPharma Issuer, it shall make its CRL (or archived CRL) available within the SAFE- BioPharma community as needed either to support resolution of a future SAFE- BioPharma dispute, or to support a future SAFE- BioPharma centralized OCSP functionality.

## **3.3 Identification and Authentication for Re-key Requests**

### **3.3.1 Identification and Authentication for Routine Re-key**

The SBCA and Principal CAs shall identify themselves through use of their current Signing Key or by using the initial identity-proofing process as described above. Identity shall be established through the initial identity-proofing process at least once every three years.

Subscribers and CAs shall identify themselves through use of their current Signing Key or by using the initial identity-proofing process described above. Identity shall be established through the initial identity-proofing process at least once every nine years.

### **3.3.2 Identification and Authentication for Re-key after Revocation**

If a Certificate is revoked, the Subscriber or Issuer shall go through the initial identity-proofing process described in Section 3.2 to obtain a new certificate.

## **3.4 Identification and Authentication for Revocation Requests**

Revocation requests shall be authenticated. Requests to revoke a Digital Certificate may be authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key is compromised.

## 4. Certificate life-cycle

### 4.1 Application

This section specifies requirements for initial application for certificate issuance.

An Issuer seeking to cross-certify with the SBCA shall complete the Issuer application process specified by the PAA, and which will include submitting a copy of the Issuer's CP and CPS to the PAA for review. If the Issuer's CP and/or CPS is in a format other than that specified in RFC 3647, the Issuer shall also supply a cross reference index between its CP and/or CPS format and the format specified in RFC 3647. The PAA will review the information provided by the Issuer and determine whether to approve the application. If approved, the PAA shall enter into an Agreement with the Issuer (or amend an existing Agreement with that Issuer), and shall authorize the SBCA OA to issue the cross certificate to the Issuer's Principal CA.

Once the PAA approves issuance of an SBCA cross-certificate, the Issuer and the SBCA RA or LRA shall perform the following steps:

- Establish and record CA information per Section 3.2.3;
- Generate a Public/Private Key pair for each certificate required;
- Establish that the Public Key forms a functioning key pair with the Private Key held by the CA (per Section 3.2.1); and
- Provide points of contact for verification of any agent roles or authorizations requested.

These steps may be performed in any order that is convenient for the RA/LRA and Issuer that meets the requirements of this CP; but all must be completed prior to certificate issuance. All communications among CA, RA, LRA, TA, and Subscribers supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued (i.e., communications supporting the issuance of medium hardware assurance certificates shall be protected using medium hardware assurance certificates, or some other mechanism of equal or greater strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

SBCA shall issue end entity certificates to trusted roles where necessary for the SBCA internal operations. SBCA shall not issue end entity certificates to anyone else or for any other purpose.

#### 4.1.1 Submission of Certificate Application

For cross certification with the SBCA, an authorized representative of the Issuer shall submit the application to the PAA.

For submission of certificate applications to an Issuer, the Issuer CP shall describe the submission process for its CAs and Subscribers.

### **4.1.2 Enrollment Process and Responsibilities**

The process for enrollment of an Issuer Principal CA with the SBCA is specified in the SBCA *Technical Guidance for Cross Certification*, available at <<http://www.safe-biopharma.org>>. Issuers applying for cross certification shall be responsible for providing accurate information in their applications for cross certification. Upon creation, each certificate issued by the SBCA shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Issuer.

Issuers shall follow the same process as above to issue a certificate to the SBCA, i.e., check the SBCA certificate manually for accuracy prior to its delivery and publication.

For enrollment with an Issuer, the Issuer CP shall describe the enrollment process for its CAs and Subscribers.

### **4.2 Certificate Application Processing**

It is the responsibility of the CA and RA to verify that the information in certificate applications is accurate. Issuer CPs shall specify procedures to verify information in certificate applications.

#### **4.2.1 Performing Identity-proofing Functions**

For the SBCA, the SBCA OA, in accordance with the requirements of Sections 3.2.2, 3.2.3, 3.2.5, and 3.2.6, shall perform the identity-proofing of Issuers or PAA-approved Subscribers.

For Issuer CAs, the identity-proofing of subordinate CAs and Subscribers shall meet the requirements specified in their respective CPs. To allow cross certification, those requirements shall also meet the provisions of this CP for Subscriber identity-proofing and authentication as specified in Sections 3.2 and 3.3. The Issuer CP shall identify the components of the Issuer PKI (e.g., RA, LRA, TA, etc.) that are responsible for proofing or authenticating the Subscriber's identity in each case.

#### **4.2.2 Approval or Rejection of Certificate Applications**

For the SBCA, the PAA may approve or reject a certificate application.

The Issuer CP shall identify the person or an organizational body that may accept or reject a Certificate application.

#### **4.2.3 Time to Process Certificate Applications**

No stipulation.

### **4.3 Issuance**

#### **4.3.1 CA Actions During Certificate Issuance**

A CA verifies the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA shall post the certificate as set forth in its respective CP.

### **4.3.2 Notification to Subscriber of Certificate Issuance**

For the SBCA, when issuing a certificate to an Issuer for cross certification, the SBCA OA shall notify the Issuer upon issuance.

For an Issuer, its CA shall notify a Subscriber of Certificate issuance in accordance with the Issuer's CP. When issuing a certificate to the SBCA for cross certification, the Issuer shall notify the PAA and SBCA OA upon issuance.

## **4.4 Acceptance**

### **4.4.1 Conduct Constituting Certificate Acceptance**

Failure to object to the certificate or its contents shall constitute acceptance of the certificate.

### **4.4.2 Publication of the Certificate by the CA**

As specified in Section 2.2, all CA certificates shall be published in a publicly accessible repository.

This CP makes no stipulation regarding publication of Subscriber certificates.

### **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

For the SBCA, notification of CA certificate issuance shall be provided to all cross-certified entities.

For all other CAs, the PAA shall be notified upon issuance of all CA certificates. The process for notifying the PAA shall be included in the associated SAFE- BioPharma Issuer Agreement or Memorandum Of Agreement (MOA).

## **4.5 Key Pair and Certificate Usage**

### **4.5.1 Subscriber Private Key and Certificate Usage**

Subscribers shall protect their Private Keys from access by any other party. Subscriber and CA Private Keys shall be protected in accordance with the SAFE- BioPharma Standard specifications. When employed for purposes covered under the SAFE- BioPharma operating rules, Subscriber Private Keys shall be used in accordance with the SAFE- BioPharma Standard specifications and functional process guidelines.

### **4.5.2 Relying Party Public Key and Certificate Usage**

Certificates may specify restrictions on use through certificate extensions. Certificates shall conform to the profiles provided in this CP. A CA shall issue information specifying the current status of all unexpired certificates. Relying Parties must process and comply with this information in accordance with their obligations as SAFE- BioPharma Members or contracted parties of SAFE- BioPharma Members, whenever using Certificates in accordance with SAFE- BioPharma operating rules.

### **4.6 Certificate Renewal**

Certificate renewal, which consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the Public Key, is permitted. Short certificate validity period coupled with frequent renewal of certificates is likely to reduce the size of CRLs.

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

#### **4.6.1 Circumstance for Certificate Renewal**

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the Private Key, as specified in Section 6.3.2.

Certificates may also be renewed when a CA re-keys.

#### **4.6.2 Who May Request Renewal**

A CA may request renewal of its certificate.

For Subscribers, the Subscriber itself, Machine Operator for the Machine Subscriber (as applicable), and LRAs/RAs may request renewal of Subscriber Certificates.

#### **4.6.3 Processing Certificate Renewal Requests**

For the SBCA, the PAA shall approve certificate renewal for reasons other than re-key of the SBCA.

For an Issuer PKI, the issuing CA system or Issuer Agent shall approve certificate renewal.

In all cases, the certificate renewal identity-proofing shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

#### **4.6.4 Notification of New Certificate issuance to Subscriber**

See Section 4.3.2.

#### **4.6.5 Conduct Constituting Acceptance of a Renewed Certificate**

See Section 4.4.1

#### **4.6.6 Publication of the Renewal Certificate by the CA**

See Section 4.4.2.

#### **4.6.7 Notification of Certificate Issuance by the CA to Other Entities**

The SBCA OA shall inform the PAA of any certificate issuance to an Issuer CA or PAA-designated Subscriber.

#### **4.7 Certificate Re-Key**

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

##### **4.7.1 Circumstance for Certificate Re-key**

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate. For Issuer Principal CA certificates, this requires that a valid Agreement exists between the PAA and the Issuer, and the term of the Agreement is beyond the expiry period for the new certificate. For all others, the Subject is entitled to a certificate in accordance with the Issuer CP.

##### **4.7.2 Who May Request Certification of a New Public Key**

A CA may request re-key of its certificate.

For Subscribers, the End-User Subscriber, Machine Operator for the Machine Subscriber (as applicable), and LRAs/RAs may request re-key of Subscriber Certificates.

##### **4.7.3 Processing Certificate Re-keying Requests**

A certificate re-key identity-proofing shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identity-proofing for Re-key as described in Section 3.3.

For cross certificates issued to and by the SBCA, the validity period shall not extend beyond the period of the applicable Issuer Agreement or MOA.

##### **4.7.4 Notification of New Certificate Issuance to Subscriber**

See Section 4.3.2.

##### **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

See Section 4.4.1.

##### **4.7.6 Publication of the Re-keyed Certificate by the CA**

See Section 4.4.2.

### **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

The SBCA OA shall inform the PAA of any certificate issuance to an Issuer CA or PAA-designated Subscriber.

The Issuer CP shall describe how trust anchor re-key information is provided securely to the Subscribers of the Issuer PKI and is made available securely to Relying Parties.

### **4.8 Certificate Modification**

Modifying a certificate means creating a new certificate that has the same or a different subject Public Key and a different serial number, and the new certificate differs in one or more other fields related to the subject (e.g., Subject e-mail address in the subject alternative name field), from the old certificate. The old certificate shall not be further re-keyed, renewed, or updated. The old certificate shall be revoked if the Subscriber no longer holds one or more of any authorizations explicitly stated in the old certificate.

The RA or other designated agent (as set forth previously) shall verify the new updated information in the certificate. For example, if an individual's name changes (e.g., due to marriage), then proof of the name change shall be validated by an LRA/RA or TA. The agent shall securely notify the CA and confirm the validation result prior to the issuance of the certificate.

#### **4.8.1 Circumstance for Certificate Modification**

A CA may issue a new certificate to the Subject when some of the Subject information has changed, e.g., name change due to change in marital status, change in subject attributes, etc., and the Subject continues to be entitled to a certificate. For Principal CA certificates, a valid and unexpired Agreement must exist between the PAA and the Issuer, and the term of the Agreement must be beyond the expiry period of the certificate being sought. For all others, the Subject is entitled to a certificate in accordance with the Issuer CP.

#### **4.8.2 Who May Request Certificate Modification**

A CA may request issuance of a modified certificate.

For Subscribers, the End-User Subscriber, Machine Operator for the Machine Subscriber (as applicable), and LRAs/RAs may request issuance of modified certificates.

#### **4.8.3 Processing Certificate Modification Requests**

A certificate modification request identity-proofing shall be achieved using one of the following processes:

- Initial identity-proofing process as described in Section 3.2; or
- Identity-proofing for Re-key as described in Section 3.3, except the old key can be used as the new key also. In addition, the validation of subject changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

#### **4.8.4 Notification of New Certificate Issuance to Subscriber**

See Section 4.3.2.

### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

See Section 4.4.1.

### **4.8.6 Publication of the Modified Certificate by the CA**

See Section 4.4.2.

### **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

The SBCA OA shall inform the PAA any time it issues a certificate, and shall only undertake certificate issuance when directed to do so by the PAA.

The Issuer CP shall describe how trust anchor re-key information is provided securely to the Subscribers of the Issuer PKI and is made available securely to Relying Parties.

## **4.9 Revocation & Suspension**

### **4.9.1 Circumstance for Revocation of a Certificate**

A certificate shall be revoked when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Subject can be shown to have violated the stipulations of its respective Subscriber, Issuer or Member Agreement, or the stipulations of this CP;
- Private Key is compromised or is suspected of compromise;
- The PAA, CA, or SAFE-BioPharma suspects or determines that revocation of a certificate is in the best interest of the integrity of the SAFE- BioPharma PKI;
- Certification of the Subject is no longer in the interest of the Issuer; or
- Subscriber or other authorized agent (as defined in the Issuer CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. Revoked certificates shall appear on at least one CRL.

### **4.9.2 Who Can Request Revocation of a Certificate**

The PAA, or the SBCA can request the revocation of the certificate issued by the SBCA.

For a certificate issued by the SBCA to an Issuer Principal CA, an authenticated request for certificate revocation can come from a previously designated agent of the Issuer responsible for the Principal CA. Such agent or agents shall be identified in the current SAFE- BioPharma Issuer Agreement as authorized to make such a request.

Only the PAA can direct the revocation of an SBCA certificate.

A subscriber can request revocation of its own certificate.

The Subscriber Certificate issued by an Issuer CA can be revoked as set forth in the Issuer's CP.

A SAFE- BioPharma Member or Issuer can request the revocation of a specific Subscriber Certificate, but the Issuer that issued the Certificate shall process such requests. If such a request cannot be resolved consistent with the Issuer's CP, the request is subject to the SAFE- BioPharma dispute resolution process.

### **4.9.3 Procedure for Revocation Request**

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester per Section 4.9.2.

If an RA performs this function on behalf of the CA, the RA shall send a message to the CA requesting revocation of the certificate. The RA shall digitally or manually sign the message. The message shall be in a format known to the CA.

Upon receipt of a revocation request from an Issuer Principal CA asking that a certificate issued by the SBCA be revoked, the SBCA OA shall authenticate the request and apprise the PAA, and then take whatever action the PAA directs. Separate from the publication of the revocation information, prompt oral or electronic notification of a Principal CA revocation shall be given by the SBCA OA to previously designated agents in all organizations having a Principal CA to which the SBCA has issued a cross-certificate.

A Subscriber ceasing its relationship with an Issuer PKI that sponsored the Certificate shall be required, prior to departure, to surrender to the agents specified in the Issuer CP (through any accountable mechanism) all cryptographic hardware tokens that were issued to the Subscriber by the Issuer PKI. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction. If the hardware tokens cannot be obtained from the Subscriber, then all Subscribers' certificates associated with the un-retrieved tokens shall be immediately revoked, expressing reason code "key compromise."

### **4.9.4 Revocation Request Grace Period**

There is no revocation grace period. Authorized parties, including subscribers are required to request the revocation of a certificate immediately after the need for revocation comes to their attention.

### **4.9.5 Time within which CA must Process the Revocation Request**

The SBCA OA shall: (a) apprise the PAA promptly when it receives a certificate revocation request from an Issuer Principal CA; and (b) revoke a certificate within one hour of receiving the direction to revoke from the PAA.

A CA shall process a certificate revocation request within eighteen (18) hours of the receipt of the request.

### **4.9.6 Revocation Checking Requirements for Relying Parties**

Relying Parties are required to comply with the SAFE- BioPharma requirements for signature validation, which prescribe how certificate status information is to be obtained and used.

### **4.9.7 CRL Issuance Frequency**

The SBCA shall publish a CRL no less frequently than once every 31 days.

The Issuer Principal CAs shall publish CRLs no less frequently than once every 31 days if the Principal CA only issues certificates to other CAs and the Principal CA is operated in an offline manner, and no less than once every 24 hours otherwise. If the CRL is issued every 31 days, such CAs must meet the requirements specified below for issuing Emergency CRLs. Such CAs shall also notify the SBCA Operational Authority upon Emergency CRL issuance. This requirement shall be included in the Issuer Agreement or MOA between SAFE-BioPharma and the Entity.

Other CAs shall publish CRLs at a frequency of no less than once every 24 hours.

In the case of CA compromise or Key compromise, all CAs shall be able to issue emergency CRL within 18 hours of notification.

### **4.9.8 Maximum Latency of CRLs**

The maximum delay between the time that a SAFE- BioPharma Subscriber's certificate is revoked by a CA and the time that this revocation information is available to SAFE- BioPharma Relying Parties shall be no greater than 24 hours. A SAFE- BioPharma Member is free to impose a requirement for a maximum delay that is less than 24 hours upon its Issuer as part of its Member-Issuer Agreement based on the Member's assessment of the acceptable liability risk associated with this delay value relative to its business operations. CRLs shall be published within 4 hours of generation.

### **4.9.9 Online Revocation Checking Availability**

The SBCA is required to operate an OCSP Responder covering the certificates it issues. The SBCA directory shall contain and publish a list of all OCSP Responders operated by Issuer PKIs cross-certified with the SBCA.

### **4.9.10 Online Revocation Checking Requirements**

The SAFE- BioPharma standards require the use of OCSP to obtain certificate status information for any certificates in a trust chain when validating digital signatures made pursuant to the SAFE- BioPharma standards. The timeliness of certificate status information supplied by the OCSP Responder shall be as specified in Section 4.9.8 of this CP. OCSP requests and responses shall comply with the profiles specified later in this CP.

### **4.9.11 Other Forms of Revocation Advertisements Available**

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking. The alternative method(s) shall be described in the CA's approved CPS.

**4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements**

No stipulation.

**4.9.12 Special Requirements Related To Key Compromise**

In the event of a CA private key compromise or loss, a CRL shall be published at the earliest feasible time. Also see Section 4.9.7.

**4.9.13 Circumstances for Suspension**

Not required. If an Issuer supports suspension, that Issuer shall comply with the requirements of SAFE- BioPharma Registration and Certificate Management Technical Specification.

**4.9.14 Who can Request Suspension**

See Section 4.9.2.

**4.9.15 Procedure for Suspension Request**

See Section 4.9.3.

**4.9.16 Limits on Suspension Period**

Suspension shall be resolved as soon as practical. Until that time, the certificate shall be treated as revoked. [Remove from hold \(i.e., suspension\) shall not be authenticated using the certificate that is on hold, revoked, expired or is otherwise invalid.](#)

**4.10 Certificate Status Services**

No stipulation beyond Section 4.9.9.

**4.10.1 Operational Characteristics**

Relying Parties are bound to their obligations as set forth in the SAFE- BioPharma operating rules and the stipulations of this CP irrespective of the operational characteristics of certificate status service.

**4.10.2 Service Availability**

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the certificate status service.

**4.10.3 Optional Features**

No stipulation.

### **4.11 End of Subscription**

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA certificates shall always be revoked at the end of subscription. The Issuer CP shall stipulate that an unexpired Subscriber certificate is revoked upon end of subscription.

### **4.12 Key Escrow & Recovery**

This CP neither requires nor prohibits the capability of recovering Subscriber decryption private keys. This CP prohibits third party escrow or recovery of CA, RA, LRA, and Subscriber signing keys used for purposes set forth in the SAFE- BioPharma standards.

#### **4.12.1 Key Escrow and Recovery Policy and Practices**

CAs that support key recovery shall identify the document describing the key escrow and recovery policy in the applicable CP.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

CAs that support key recovery shall identify the document describing the key encapsulation and recovery policy in the applicable CP.

## 5. Facility Management & Operations Controls

### 5.1 Physical Controls

All CA and CSA equipment including their cryptographic modules shall be protected from unauthorized access at all times.

A CA and CSA shall impose physical security requirements specified in Section 5.1.2.

RA and LRA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA and LRA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the LRA/RA environment.

#### 5.1.1 Site Location & Construction

The location and construction of the facility housing the CA and CSA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA and CSA equipment and records.

#### 5.1.2 Physical Access

The CA, CSA, and CCS equipment shall always be protected from unauthorized access. The equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

These security mechanisms shall be commensurate with the level of threat in the equipment environment.

The physical security mechanisms for CAs, CSAs, and CCS shall be in place to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times;
- Maintain and periodically inspect an access log; and
- Require two person physical access control to both the cryptographic module and computer system.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules and activation information used to access or enable cryptographic modules used by CAs, CSAs, and CCS shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate

with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA, CSA, or CCS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the SBCA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

### **5.1.3 Power and Air Conditioning**

CAs shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any SBCA on-line servers (e.g., those hosting directories) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support a smooth shutdown of the SBCA operations.

### **5.1.4 Water Exposures**

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

### **5.1.5 Fire Prevention & Protection**

No stipulation.

### **5.1.6 Media Storage**

CA media shall be stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CAs and shall be protected from unauthorized access.

### **5.1.7 Waste Disposal**

Sensitive waste material shall be disposed of in a secure fashion.

### 5.1.8 Off-Site backup

Full system backups of CAs, sufficient to recover from system failure, shall be made on a periodic schedule as described in the respective CPS. Backups shall be performed and stored off-site no less than once per week. At least one full backup copy shall be stored at an offsite location. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

(Note: The following requirements apply specifically to the SBCA and are consistent with those developed and published by the U.S. National Institute of Standards and Technology. The requirements also apply to Issuer PKIs but may be implemented by those Issuers in a fashion they deem appropriate to provide a level of security and protection comparable to that which would be obtained by directly meeting the requirements below. In all cases, the method of implementation shall be set forth in the Issuer PKI CP and CPS, and shall be submitted to the PAA for review when the Issuer seeks cross-certification with the SBCA.)

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the SAFE- BioPharma PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion, and any one individual cannot cause much damage. The following are the trusted roles for a CA:

- *CA Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys. This is an Agent role per the SAFE- BioPharma Functional Specification.
- *CA Agent* – authorized to request or approve certificates, or certificate revocations. This is a Registration Agent role per the SAFE- BioPharma Functional Specification.
- *CA Auditor* – authorized to view and maintain CA audit logs. This is an Agent role per the SAFE- BioPharma Functional Specification.
- *CA Operator* – authorized to perform system backup and recovery. This is a Machine Operator role per the SAFE- BioPharma Functional Specification.

In addition to the above CA roles, the SAFE- BioPharma PKI may have the following additional roles:

- *CSA Administrator* – authorized to configure and operate the CSA. This is a Machine Operator role per the SAFE- BioPharma Functional Specification.
- *CSA Auditor* – authorized to view and manage CSA audit logs. This is an Agent role per the SAFE- BioPharma Functional Specification.
- *CCS Administrator* – authorized to configure and operate the CCS. This is a Machine Operator role per the SAFE- BioPharma Functional Specification.

- *CCS Auditor* – authorized to view and manage CCS audit logs. This is an Agent role per the SAFE- BioPharma Functional Specification.
- *RA* – authorized to validate the identity of the subscribers and communicate approval of certificate issuance and revocation requests to the CA. This is a Registration Agent role per the SAFE- BioPharma Functional Specification.
- *LRA* – authorized to validate the identity of the subscribers and communicate approval of certificate issuance and revocation requests to RA. This is a Registration Agent role per the SAFE- BioPharma Functional Specification.
- *Trusted Agent* – authorized to validate the identity of the subscribers on behalf of the RA or LRA. This is a Registration Agent role per the SAFE- BioPharma Functional Specification.
- *Machine Operator* – authorized to obtain a certificate on behalf of a Machine Subscriber. This is a Machine Operator role per the SAFE- BioPharma Functional Specification, and is also referred to as a “representative” for the Machine Subscriber in this CP.

The following sections contain a detailed description of these roles.

### **5.2.1.1 CA Administrator**

The CA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

CA Administrators are not permitted to issue certificates.

### **5.2.1.2 CA Agent**

The CA Agent role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

### **5.2.1.3 CA Auditor**

The CA Auditor role is responsible for:

- Reviewing, maintaining, and archiving CA audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

### **5.2.1.4 CA Operator**

The CA Operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

### **5.2.1.5 CSA Administrator**

The CSA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CSA;
- Establishing and maintaining CSA system accounts;
- Configuring audit parameters, and;
- Generating and backing up CSA keys.
- Operation of the CSA equipment; and
- System backups and recovery.

### **5.2.1.6 CSA Auditor**

The CSA Auditor role is responsible for:

- Reviewing, maintaining, and archiving CSA audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CSA is operating in accordance with its CPS.

### **5.2.1.7 CCS Administrator**

The CCS Administrator role is responsible for:

- Installation, configuration, and maintenance of the CCS;
- Establishing and maintaining CCS system accounts;
- Configuring audit parameters, and;
- Generating and backing up CCS keys.
- Operation of the CCS equipment; and
- System backups and recovery.

### **5.2.1.8 CCS Auditor**

The CCS Auditor role is responsible for:

- Reviewing, maintaining, and archiving CCS audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CCS is operating in accordance with its CPS.

### **5.2.1.9 Registration Authority (RA)**

The RA responsibilities are:

- Verifying identity, either through personal contact, or via LRA or Trusted Agents;
- Entering Subscriber information, and verifying its correctness;
- Securely communicating requests to and responses from the CA; and
- Receiving and distributing Subscriber certificates.

### **5.2.1.10 Local Registration Authority (LRA)**

The LRA responsibilities are:

- Verifying identity, either through personal contact, or via Trusted Agents;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA and RA; and
- Receiving and distributing Subscriber certificates.

While the LRA performs functions similar to RA, an LRA generally is authorized to serve a limited population of Subscribers, based on logical or geographical organization.

### **5.2.1.11 Trusted Agent (TA)**

A Trusted Agent is a person authorized to act as a representative of an LRA or RA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with CAs; they act on the behalf of the LRA/RA only to verify the identity of the Subscriber.

### **5.2.1.12 Machine Operator**

A Machine Operator represents a Machine Subscriber that is named as Certificate subject. The Machine Operator works with the LRA, RA or TA to register Machine Subscribers in accordance with Section 3.2.3.2.

## **5.2.2 Number of Persons Required per Task**

A single person may be sufficient to perform tasks associated with a role, except for the activation of the CA certificate signing Private Key. Generation, backup, and activation of the CA certificate signing Private Key shall require actions by at least two individuals.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access does not constitute a task as defined in this section. Therefore, two-person physical access control as required in Section 5.1.2.1 may be attained using any two individuals in trusted roles.

## **5.2.3 Identity-proofing for Each Role**

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

## **5.2.4 Separation of Roles**

Role shall be enforced either by the CA, CSA, or CCS system.

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume a CA Agent role may not assume an CA Administrator or CA Auditor role.

An individual assigned a CA, CSA, and/or CCS Auditor role shall not perform any other trusted role except CA, CSA and/or CCS Auditor.

No individual shall be assigned more than one identity.

Under no circumstances shall any PKI entity perform its own compliance auditor function.

### **5.3 Personnel Controls**

#### **5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements**

Each PKI shall identify at least one individual or group responsible and accountable for the operation of each CA in the PKI. For the SBCA, these are the PAA and the SBCA Operational Authority.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA and CSA shall be set forth in the CA and CSA CPS.

#### **5.3.2 Background Check Procedures**

CA personnel shall, at a minimum, pass a background investigation covering the following areas:

---

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

---

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with U.S. Executive Order 12968 August 1995, or equivalent.

#### **5.3.3 Training Requirements**

All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms
- Use and operation of all PKI associated equipment
- All PKI software versions in use on the CA system
- All PKI duties an individual is expected to perform

- Disaster recovery and business continuity procedures.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

### **5.3.4 Retraining Frequency & Requirements**

Individuals responsible for PKI roles shall be aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

### **5.3.5 Job Rotation Frequency & Sequence**

No stipulation.

### **5.3.6 Sanctions for Unauthorized Actions**

The CA, CSA, CCS, Issuer, PAA and SAFE-BioPharma shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the SAFE- BioPharma, SBCA or applicable CP or CPS) involving the CA, its repository, or CSA.

### **5.3.7 Contracting Personnel Requirements**

Contractor personnel employed to perform functions pertaining to the CA and CSA shall be subject to the requirements of this CP.

### **5.3.8 Documentation Supplied To Personnel**

The SBCA and Issuer shall make available to its CA, CSA, CCS, RA, and LRA personnel its CP, applicable CPS, applicable system operations documents, operations procedures documents and any relevant statutes, policies or contracts required to perform their jobs.

## **5.4 Audit**

Audit log files shall be generated for all events relating to the security of the CA, CSA, CCS, RA and LRA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive*, Section 5.5.2.

### **5.4.1 Types of Events Recorded**

All security auditing capabilities of the CA, CSA, CCS, RA, LRA operating system and application Components required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. An "X" in a table cell indicates that the respective Component (CA, CSA, CCS, RA or LRA) shall record the indicated type of auditable

## Version 2.5

event. A “-” in a table cell indicates that the respective Component need not record the indicated type of auditable event. An “N/A” in a table cell indicates the event is not applicable. (Note: the table below may be adjusted in future releases of this CP with a reference to the Certificate Issuing and Management Components (CIMC) Protection Profile being developed by NIST.) At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- A success or failure indicator for the event, and
- The identity of the entity that caused the event.

Auditable Event	CA	CSA	CCS	RA	LRA
<b>SECURITY AUDIT</b>					
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X	X
Obtaining a third-party time-stamp	X	X	X	X	X
<b>IDENTITY-PROOFING</b>					
Successful and unsuccessful attempts to assume a role	X	X	X	X	X
The value of <i>maximum number of authentication attempts</i> is changed	X	X	X	X	X
<i>Maximum number of authentication attempts</i> occur during user login	X	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X	X
<b>LOCAL DATA ENTRY</b>					
All security-relevant data that is entered in the system	X	X	X	X	X
<b>REMOTE DATA ENTRY</b>					
All security-relevant messages that are received by the system	X	X	X	X	X
<b>DATA EXPORT AND OUTPUT</b>					
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X	X
<b>KEY GENERATION</b>					
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X
<b>PRIVATE KEY LOAD AND STORAGE</b>					

## Version 2.5

Auditable Event	CA	CSA	CCS	RA	LRA
The loading of Component private keys	X	X	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	N/A	X <sup>1</sup>	N/A	N/A
<b>TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE</b>					
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X	X
<b>SECRET KEY STORAGE</b>					
The manual entry of secret keys used for authentication	X	X	X	X	X
<b>PRIVATE AND SECRET KEY EXPORT</b>					
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X
<b>CERTIFICATE REGISTRATION</b>					
All certificate requests	X	N/A	N/A	X	X
<b>CERTIFICATE REVOCATION</b>					
All certificate revocation requests	X	N/A	N/A	X	X
<b>CERTIFICATE STATUS CHANGE APPROVAL</b>					
The approval or rejection of a certificate status change request	X	N/A	N/A	N/A	N/A
<b>CA CONFIGURATION</b>					
Any security-relevant changes to the configuration of the Component	X	X	X	X	X
<b>ACCOUNT ADMINISTRATION</b>					
Roles and users are added or deleted	X	-	-	-	-
The access control privileges of a user account or a role are modified	X	-	-	-	-
<b>CERTIFICATE PROFILE MANAGEMENT</b>					
All changes to the certificate profile	X	N/A	N/A	N/A	N/A
<b>REVOCATION PROFILE MANAGEMENT</b>					
All changes to the revocation profile	X	N/A	N/A	N/A	N/A
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>					
All changes to the certificate revocation list profile	X	N/A	N/A	N/A	N/A
<b>MISCELLANEOUS</b>					
Appointment of an individual to a Trusted Role	X	X	X	X	X

<sup>1</sup> In the CCS context, all access and use of subscriber private keys shall be auditable.

## Version 2.5

Auditable Event	CA	CSA	CCS	RA	LRA
Designation of personnel for multiparty control	X	X	-	-	-
Installation of the Operating System	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	X
Installation of hardware cryptographic modules	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X
System Startup	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X
Back up of the internal CA database	X	-	N/A	-	-
Restoration from back up of the internal CA database	X	-	N/A	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-	-	-
Posting of any material to a repository	X	-	N/A	-	-
Access to the internal CA database	X	X	N/A	-	-
All certificate compromise notification requests	X	N/A	N/A	X	X
Loading tokens with certificates	X	N/A	X	X	X
Shipment of Tokens	X	N/A	N/A	X	X
Zeroizing Tokens	X	N/A	N/A	X	X
Re-key of the Component	X	X	X	X	X
<b>CONFIGURATION CHANGES</b>					
Hardware	X	X	X	-	-
Software	X	X	X	X	X
Operating System	X	X	X	X	X
Patches	X	X	X	-	-
Security Profiles	X	X	X	X	X
<b>PHYSICAL ACCESS / SITE SECURITY</b>					
Personnel Access to room housing Component	X	-	X	-	-
Access to the Component	X	X	X	-	-
Known or suspected violations of physical security	X	X	X	X	X
<b>ANOMALIES</b>					
Software error conditions	X	X	X	X	X
Software check integrity failures	X	X	X	X	X

## Version 2.5

Auditable Event	CA	CSA	CCS	RA	LRA
Receipt of improper messages	X	X	X	X	X
Misrouted messages	X	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X	X
Equipment failure	X	-	-	-	-
Electrical power outages	X	-	-	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-	-	-
Obvious and significant network service or access failures	X	-	-	-	-
Violations of Certificate Policy	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X

In addition, a message from any source requesting an action by the CA is an auditable event. The message must include message date and time, source, and destination.

### 5.4.2 Frequency of Processing Data

Audit logs from the CA, CSA, CCS, RA, and LRA shall be reviewed at least once every two months. At a minimum, a statistically significant set of security audit data generated by the Component since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. For SBCA audit logs, 100% of the audit data shall be examined.

The analysis shall document and explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

### 5.4.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the component shall comply with the role separation requirements of Section 5.2.4.

### 5.4.4 Protection of Security Audit Data

Component system configuration and operating procedures shall ensure that:

- Only authorized people (i.e., Auditor role) have read access to the logs;
- Only authorized people (i.e., Auditor role) may archive audit logs; and
- Audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention

period (note that deletion may require modification access). Audit logs shall be moved to a safe, secure storage location separate from the component equipment.

### **5.4.5 Security Audit Data Backup Procedures**

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

### **5.4.6 Security Audit Collection System (Internal or External)**

The audit log collection system may or may not be external to a component. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the PAA (or comparable Issuer PKI entity) shall be notified, and a determination shall be made by the SBCA OA (or comparable Issuer PKI entity) whether to suspend the Component operation until the problem is remedied.

### **5.4.7 Notification to Event-Causing Subject**

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the auditable event.

### **5.4.8 Vulnerability Assessments**

The Auditor shall perform vulnerability self-assessments of security controls.

## **5.5 Archive**

### **5.5.1 Types of Events Archived**

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level (requirements for Test Assurance shall be set forth in the Issuer Agreement):

Data To Be Archived	CA	CSA	CCS	RA	LRA
Certification Practice Statement	X	X	X	X	X
Contractual obligations	X	X	X	X	X
System and equipment configuration	X	X	X	-	-
Modifications and updates to system or configuration	X	X	X	-	-
Certificate requests	X	-	N/A	-	-
Revocation requests	X	-	N/A	-	-
Subscriber identity authentication data as per Section 3.2.3	X	N/A	N/A	X	X
Documentation of receipt and acceptance of certificates	X	N/A	N/A	X	X

## Version 2.5

---

Data To Be Archived	CA	CSA	CCS	RA	LRA
Documentation of receipt of Tokens	X	N/A	N/A	X	X
All certificates issued or published	X	N/A	N/A	N/A	N/A
Record of Component Re-key	X	X	X	X	X
All CRLs issued and/or published	X	N/A	N/A	N/A	N/A
All Audit Logs	X	X	X	X	X
Other data or applications to verify archive contents	X	X	X	X	X
Documentation required by compliance auditors	X	X	X	X	X

### **5.5.2 Retention Period for Archive**

The minimum retention periods for archive data shall be established in accordance with applicable regulatory guidance and law as negotiated and agreed between the Issuer and relevant Members, and as specified by the PAA to the SBCA OA. This period shall be no less than 10 years and 6 months.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications needed to process the archive data shall also be maintained for the archival retention period.

Prior to the end of the archive retention period, the SBCA shall provide archived data and the applications necessary to read the archives to a PAA approved archival facility, which shall retain the applications necessary to read this archived data.

The Issuer CP shall state whether and how the archive data is retained beyond the retention period. This CP does not restrict longer retention.

### **5.5.3 Protection of Archive**

Only authorized individuals shall be permitted to add to or delete from the archive. The archived records may be moved to another medium when authorized by the Auditor. The contents of the archive shall not be released except as determined by the PAA, Issuer, or as required by law. Records and material information relevant to use of, and reliance on, a SAFE- BioPharma certificate shall be archived. Archived information of individual SAFE- BioPharma Transactions shall be made available upon request to any Subscribers involved in the transaction or their legally recognized agents. Such information shall be available beyond the end of the validity period of the associated SAFE- BioPharma Subscriber's certificate, up to the retention period indicated in Section 5.5.2. Archive media shall be stored in a safe, secure storage facility separate from the component itself.

### **5.5.4 Archive Backup Procedures**

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

**5.5.5 Requirements for Time-Stamping of Records**

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

**5.5.6 Archive Collection System (Internal or External)**

No stipulation.

**5.5.7 Procedures to Obtain & Verify Archive Information**

Procedures detailing how to create, verify, package, transmit, and store the archive information, shall be published in the component CPS.

**5.6 Key Changeover**

To minimize risk from compromise of a CA's signing Private Key, that key shall be changed often. Once changed, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs that contain certificates signed with that key, only then the old key may be retained. If the old key is retained, it shall be protected just as the new key.

The validity period for certificates issued to and by the SBCA shall be six years or less.

Depending on the key size, CAs shall use the following maximum key usage periods. An Issuer PKI may use a shorter CA private key and/or CA certificate validity period.

Key Size	CA Private Key Usage Period	CA Certificate Validity Period
1024 bit RSA	CA and Subscriber Certificate Validity Period	Not Beyond 12/31/2010
2048 bit RSA	Root CA Self-Signed Certificate Validity Period CA Certificate Validity Period Subscriber Certificate Validity Period	<= 25 years <= 10 Years <= 3 Years

**5.7 Compromise & Disaster Recovery**

**5.7.1 Incident and Compromise Handling Procedures**

The SBCA OA shall notify the PAA and all member entities if any of the following cases occur:

- suspected or detected compromise of the SBCA systems;
- physical or electronic attempts to penetrate SBCA systems;
- denial of service attacks on SBCA components;
- any incident preventing the SBCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow member entities to protect their interests as Relying Parties.

The SBCA Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the SBCA CPS.

All other CAs shall provide notice as required by the applicable Issuer Agreement or MOA.

If the SBCA OA (or comparable Issuer PKI entity) detects a potential hacking attempt or other form of compromise to a CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

If CCS is compromised or suspected of being compromised, the incident shall be investigated. All certificates associated with the subscriber private keys held in the CCS shall be revoked unless a definitive determination is made that the CCS is not compromised.

### **5.7.2 Computing Resources, Software, and/or Data Are Corrupted**

CAs shall maintain backup copies of hardware, system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption.

When computing resources, software, and/or data are corrupted, the CAs shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

### **5.7.3 CA Private Key Compromise Recovery Procedures**

In case of a CA key compromise, the CA shall request revocation of its certificates from all other CAs who have issued it a certificate. The CAs shall immediately publish the revocation information in the most expedient manner. Subsequently, the CA installation shall be re-established as above. If the CA is a trust anchor for an Issuer's subscribers, the trusted self-signed certificate shall be removed from each subscriber, and a new one distributed via secure out-of-band mechanisms. A Trust Anchor CA shall describe its approach to reacting to the key compromise in their CPS. Secure techniques to distribute the new trust anchor shall be described in each applicable CPS.

The CA Operational Authority or CA governing body (e.g., PAA in the case of SBCA) shall also investigate and report to the SAFE- BioPharma PAA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

### **5.7.4 Business Continuity Capabilities after a Disaster**

The SBCA OA (or comparable Issuer agent for a CA) shall promptly and securely advise the PAA and all entities cross-certified with the SBCA in the event of a disaster where the CA installation is physically damaged and all copies of the CA Signing Keys are destroyed.

If CA equipment is damaged or rendered inoperative, but the CA Signing Keys are not destroyed, the CA operation shall be reestablished as quickly as possible and in a secure fashion, giving priority to the ability to generate the CRL.

If an OCSP Responder associated with the SBCA or an Issuer CA is not available for any reason, then the PAA and all entities cross-certified with the SBCA shall be securely and promptly notified in a fashion set forth in the respective Agreements. This will allow Issuers and those contracted with the Issuers to protect their interests as Relying Parties. The PAA shall also determine whether to revoke the Issuer's Principal CA certificate.

In the case of a disaster whereby the SBCA or an Issuer's Principal CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its certificates be revoked, and shall apprise the SBCA OA and PAA of actions they intend to take to reestablish the CA and request a new cross-certificate with the SBCA, and will follow whatever processes have been set forth in the respective Agreement for that purpose. The CA Operational Authority shall at the earliest feasible time securely advise the PAA and all of its member entities in the event of a disaster where the SBCA or Principal CA installation is physically damaged and all copies of the SBCA or Principal CA signature keys are destroyed.

In the case of a disaster whereby a CA (other than a Principal CA and the SBCA) installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new Private and Public Keys, being re-certified, and re-issuing all cross certificates. Finally, Subscriber Certificates shall be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed Private Key do so at their own risk and the risk of others to whom they forward data.

The SBCA and Issuer directories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. The SBCA OA and Issuer PKI shall implement features to provide high levels of directory reliability (99.9% availability or better). The SBCA operations shall be designed to restore full service within 18 hours of failure.

## **5.8 CA & RA Termination**

### **5.8.1 CA Termination**

In the event of termination of the SBCA operation, certificates signed by the SBCA shall be revoked and the PAA shall advise cross-certified PKIs that have entered into Issuer Agreements and/or MOAs with SAFE-BioPharma that SBCA operation has terminated so they may revoke certificates they have issued to the SBCA. Prior to SBCA termination, the PAA shall provide all archived data to an archival facility. Cross certified PKIs shall be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the SBCA is terminated.

In the event that a CA terminates operation, the CA shall provide notice to the SBCA prior to termination. If the Issuer Principal CA (or any CA subordinate to that Principal CA that issues Subscriber Certificates for SAFE- BioPharma purposes) terminates operation for convenience, contract expiration, re-organization, or other non-security related reason, the Agreement between the Principal CA and SAFE-BioPharma shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the Issuer Principal CA that are needed for use within SAFE- BioPharma. At a minimum, such actions shall include preservation of the Principal CA information archive described in the Principal CA CP and CPS.

### **5.8.2 RA Termination**

Upon termination, the RA certificate shall be revoked and the RA shall provide archived data to the respective Issuer PKI approved archival facility.

## **6. Technical Security Controls**

When FIPS 140-1/2 module is used, the module shall be validated and shall be used in FIPS approved mode.

### **6.1 Key Pair Generation & Installation**

#### **6.1.1 Key Pair Generation**

Cryptographic keying material for basic assurance CAs (Issuer Principal CA and Issuer CA) and associated CSA signing keys shall be generated in FIPS 140-1/2 Level 2 (or higher) validated hardware cryptographic modules.

Cryptographic keying material for all medium software and medium hardware assurance CAs (SBCA, Issuer Principal CA, and Issuer CA) and associated CSA signing keys shall be generated in FIPS 140-1/2 Level 3 (or higher) validated hardware cryptographic modules.

At all assurance levels, CA and CSA key generation procedures shall be documented in the respective CPS, and generate auditable evidence that the documented procedures were followed, and were witnessed and attested to by an independent third party. The documented procedures shall be detailed enough to demonstrate that appropriate multi-person control and role separation were used.

Cryptographic keying material for RA and LRA keys shall be generated in FIPS 140-1/2 Level 2 (or higher) validated hardware cryptographic modules.

Cryptographic keying material for End Entities for medium hardware assurance shall be generated in FIPS 140-1/2 Level 2 (or higher) validated hardware cryptographic modules

Cryptographic keying material for End Entities for basic and medium software assurance shall be generated in FIPS 140-1/2 Level 1 software (or higher) in an operating environment that provides private key protections comparable to FIPS 140-1/2 Level 2 (or higher).

Cryptographic keying material for End Entities using a CCS for medium software and basic assurance shall be generated in FIPS 140-1/2 Level 2 (or higher) validated hardware and software cryptographic modules and shall remain in the CCS.

Subscriber keys shall be generated by the subscriber, RA, LRA, CCS, or CA.

#### **6.1.2 Private Key Delivery to Subscriber**

In most cases, Private Keys will be generated and remain within the cryptographic boundary of the cryptographic module. If the owner of the module generates the key, then there is no need to deliver the private key. If the key is generated elsewhere, then the module shall be delivered to the Subscriber by the Issuer. The Issuer shall maintain accountability for the location and state of the module until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. The private key shall be protected from activation, compromise, or modification during the delivery process. Under no circumstances shall anyone other than the Subscriber have substantive knowledge of or control over signing Private Keys after generation of the key. Anyone who generates a signing Private Key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber.

When keyed Hardware Tokens are delivered to subscribers, the delivery shall be accomplished in a way that ensures that the correct Tokens and activation data are provided to the correct Subscribers. The Issuer shall maintain a record of validation for receipt of the Token by the Subscriber.

CAs shall generate their own key pairs in hardware.

### **6.1.3 Public Key Delivery to Certificate Issuer**

Applicant public keys must be delivered securely for certificate issuance in a way that binds the applicant's verified identity to the Public Key. The strength of binding and assurance level shall be commensurate with that of the Public Key being submitted for certificate issuance.

### **6.1.4 CA Public Key Delivery to Relying Parties**

The Issuer PKI shall ensure that its Subscribers receive and maintain its trust anchor(s) in a trustworthy fashion. Acceptable methods for trust anchor delivery include but are not limited to:

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers via secure mechanisms;
- Distribution of trust anchor through secure out-of-band mechanisms;
- Calculation and comparison of trust anchor hash or fingerprint against the hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); or
- Downloading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloaded and the site trust anchor already on the Subscriber system via secure means.

### **6.1.5 Key Sizes**

All FIPS-approved signature algorithms shall be considered acceptable. If the PAA determines that the security of a particular algorithm may be compromised, it shall direct the SBCA OA to revoke the affected certificates.

All trust anchor certificates shall be at least 2048 bit RSA.

All certificates issued shall use at least 1024 bit RSA, with Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2 or equivalent. However, all certificates that last beyond 12/31/2010 shall be at least 2048 bit RSA. In addition, all certificates that are issued after 12/31/2010 shall use SHA-256.

CSAs shall sign certificate status responses using the same signature algorithm, key size, and hash algorithm as used by the CA to sign CRLs.

TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall use SHA-1, triple-DES or AES (minimum 128 bit key strength) for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys. These protocols shall require at least 2048 bit RSA and at least 128 bit AES after 12/31/2010.

**6.1.6 Public Key Parameters Generation and Quality Checking**

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2 or equivalent.

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the PAA.

**6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)**

Public keys that are bound into certificates shall be certified for use in signing or encrypting. This restriction is not intended to prohibit use of protocols (like the TLS or SSL) that provide authenticated connections using key encryption certificates. Such dual-use certificates shall not assert *nonRepudiation*.

The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, Subscriber Certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and *nonRepudiation* bits. Subscriber Certificates to be used for encryption shall set the *keyEncipherment* bit.

Issuer CA certificates must set the following key usage bits: *cRLSign* and *keyCertSign*.

**6.2 Private Key Protection & Crypto-Module Engineering Controls**

**6.2.1 Cryptographic Module Standards & Controls**

The relevant standards for cryptographic modules is FIPS PUB 140-1/2, *Security Requirements for Cryptographic Modules*

The PAA may determine that other comparable qualification, certification, or verification standards are sufficient. The PAA shall identify these standards. Cryptographic modules shall be certified to the levels identified in this section, or certified or qualified to requirements published by the PAA. Additionally, the PAA reserves the right to review technical documentation associated with any crypto-modules under consideration for use by any CA.

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

<b>FIPS 140-1/2</b>	<b>CA</b>	<b>CSA</b>	<b>CCS</b>	<b>RA</b>	<b>LRA</b>	<b>Subscriber</b>
Required	Level 2 (Hardware) for basic Level 3 (Hardware) for medium software and medium hardware	Level 2 (Hardware) for basic Level 3 (Hardware) for medium software and medium hardware	Level 2 (Hardware or Software) for basic and medium software	Level 2 (Hardware)	Level 2 (Hardware)	For medium hardware: Level 2 (Hardware) For basic and medium software: Level 1 (Software)

### **6.2.2 CA Private Key Multi-Person Control**

Use of CA private signing key shall require action by multiple persons in accordance with requirements of Section 5.2.2.

### **6.2.3 Private Key Escrow**

Under no circumstances shall a third party escrow any Signing Keys used to support non-repudiation services. Subscriber private dual-use keys shall not be escrowed.

### **6.2.4 Private Key Backup**

#### **6.2.4.1 Backup of CA Signing Private Key**

The CA signing Private Keys shall be backed up under the same multi-person control as the original Signing Key. A single copy of the signing key shall be stored at the CA location. A second copy shall be kept at the CA backup location. Procedures for CA signing Private Key backup shall be identified in the CA CPS.

CSA Private Keys may be backed up on a hardware cryptographic module approved for CSA. The backup shall be performed under the same control as the CSA key activation.

All copies of the CA and CSA private signature keys shall be accounted for and protected in the same manner as the original ones.

#### **6.2.4.2 Backup of Subscriber Private Keys**

RA and LRA signing Private Keys shall not be backed up. Subscriber medium hardware assurance Private Keys shall not be backed up.

Subscriber basic and medium software assurance private keys may be backed up as long as they remain under the subscriber's control and meet all the protection and usage requirements for the subscriber private keys.

Subscriber private keys held in a CCS may be backed up to a device providing comparable protection levels and approved for CCS use. The CCS backup shall be performed under two-person control.

Backed up subscriber private keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

### **6.2.5 Private Key Archival**

Signing Private Keys shall not be escrowed or archived.

### **6.2.6 Private Key Transfer into or from a Cryptographic Module**

CA Private Keys and all hardware signing keys shall be generated in and remain in the same hardware cryptographic module. The CA and CSA private keys may be backed up in accordance with Section 6.2.4.1. The CA and CSA private keys may be exported from the cryptographic module only to perform key backup procedures as described in Section 6.2.4.1. At no time shall the CA or CSA private key exist in plain text outside the cryptographic module.

RA and LRA Signing Keys shall not be transferred from the module they are generated in. Subscriber medium hardware assurance Signing Keys shall not be transferred from the module they are generated in.

If a private key is transported from one cryptographic module to another, the private key shall be encrypted during transport; private keys shall never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport shall be protected from disclosure.

### **6.2.7 Private Key Storage on Cryptographic Module**

The hardware cryptographic module may store Private Keys in any form as long as the keys are not accessible without a FIPS 140-1/2, Level 2 authentication mechanism. .

### **6.2.8 Method of Activating Private Keys**

The Private Key user (e.g. CA, RA, Subscriber, etc.) shall be authenticated to the cryptographic module before the activation of any Private Key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data such as passwords and PINs shall be protected from disclosure (i.e., the data shall not be displayed while it is entered). Biometrics, if used, shall provide liveness property to ensure that the user is present.

### **6.2.9 Methods of Deactivating Private Keys**

Cryptographic modules that have been activated shall not be available to unauthorized access.

If cryptographic modules are used to store Subscriber Private Keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CP (for Subscribers) or CPS (for CAs). Hardware cryptographic modules shall be removed and stored in a secure container or environment when not in use.

### **6.2.10 Method of Destroying Private Keys**

Signing Private Keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. This may be achieved by executing a “zeroize” command. Physical destruction of module is not required. CA, CSA, and RA private key shall be destroyed by individuals in trusted roles.

### **6.2.11 Cryptographic Module Rating**

See table in Section 6.2.1.

## **6.3 Other Aspects of Key Management**

### **6.3.1 Public Key Archive**

The Public Key is archived as part of the certificate archive process.

### **6.3.2 Certificate Operational Periods and Key Usage Periods**

See table in Section 5.6 for CAs.

The following table provides the maximum private key certificate validity periods for CSA, RA, LRA and Subscribers certificates.

Key Size	CSA Private Key	CSA Certificate	RA, LRA and Subscriber Private Key	RA, LRA and Subscriber Certificate
1024 bit RSA	Up to 3 Years	3 Years	Up to 3 years	3 Years
2048 bit RSA	Up to 3 years	3 Years	Up to 3 years	3 Years

Note: Private keys used for decryption do not have a life time. They may be used at any time for decryption.

CAs shall not issue certificates that extend beyond the expiration date of their own certificates and public keys.

### **6.3.3 Subscriber Private Key Usage Environment**

The subscribers shall use their private keys only from the machines that are protected and managed using commercial best practices for computer security and network security controls.

## **6.4 Activation Data**

### **6.4.1 Activation Data Generation & Installation**

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected. Activation data shall meet the requirements of FIPS 140-2 Level 2. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

Where a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

### **6.4.2 Activation Data Protection**

Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

Subscriber activation data presented to CCS to use the subscriber keys shall be protected from disclosure to unauthorized parties, from eavesdropping, and from replay.

### **6.4.3 Other Aspects of Activation Data**

No stipulation.

### **6.5 Computer Security Controls**

#### **6.5.1 Specific Computer Security Technical Requirements**

The following computer security functions shall be provided by the operating system used by the CA, CSA, CCS, RA and LRA:

- Authenticated logins
- Discretionary Access Control
- Security audit capability
- Access control restrictions to CA services based on authenticated identity
- Residual information protection
- Trusted path for user identification and authentication
- Domain separation enforcement
- Operating system self-protection.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

#### **6.5.2 Computer Security Rating**

No Stipulation.

### **6.6 Life-Cycle Security Controls**

#### **6.6.1 System Development Controls**

The SBCA and Issuer PKIs are infrastructure components that support a range of SAFE-BioPharma community applications, some of which may manage regulated data. The SBCA's design, installation, and operation shall be documented by qualified personnel in a qualified manner to support SAFE- BioPharma Member regulated application compliance activities associated with U.S. Food and Drug Administration computer systems validation (CSV) requirements, especially those prescribed to meet 21 Code of Federal Regulations Part 11 regarding electronic records and electronic signatures. The SBCA OA shall develop and produce appropriate qualification documentation establishing that SBCA components are properly installed and configured, and operate in accordance with SAFE- BioPharma technical specifications and the SBCA design. This documentation shall include:

- Installation Qualification plans, procedures/scripts/data, acceptance criteria, and results.
- Operational Qualification plans, procedures/scripts/data, acceptance criteria, certifications, and test results.

Issuer PKIs shall prepare and maintain similar documentation.

The following specific requirements shall be met as part of the system development process:

- CA shall use software, whether off-the-shelf or custom-built, that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software that is developed specifically for the CA, CSA, or CCS shall be developed in a controlled environment, and the development process shall be defined and documented. The PKI owner shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment. This requirement does not apply to off-the-shelf hardware or software.
- Where open source software has been utilized, the PKI owner shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- All hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The PKI platform (server hardware, operating system software, and PKI application software) shall be dedicated to performing PKI functions. There shall be no non-PKI applications installed on the PKI platform. Connected or associated hardware devices, network connections, or component software that are not part of the PKI platform are exempt from this requirement.
- Proper care shall be taken to prevent malicious software from being loaded. Applications required to perform the PKI operation shall be obtained from sources authorized by local policy.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

CA, CSA, CCS, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

### **6.6.2 Security Management Controls**

The configuration of the CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of CA system. The CA, CSA, and CCS software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. CA software integrity shall be verified at least weekly.

### **6.6.3 Life Cycle Security Ratings**

No stipulation.

### **6.7 Network Security Controls**

The SBCA shall not be connected to any network. Information to be transferred from the SBCA to directories or databases shall be done through “out of band” means (e.g., removable media).

CAs, CSAs, CCS, RAs, and LRAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA, CSA, or CCS.

RAs and LRAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers.

All Directories connected to the Internet shall provide continuous service to SAFE- BioPharma Participants and any entities authorized to rely upon Digital Signatures made meeting SAFE- BioPharma standards. Redundancy shall be employed to ensure continuity of service even during periods of maintenance or backup. All Directories shall use a network guard, firewall or filtering router to protect against denial of service and intrusion attacks.

The applicable CPS shall define the network protocols and mechanisms required for the operation of the PKI Component. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

### **6.8 Time Stamping**

SAFE- BioPharma requires that the system clock time for all CA, CSA, CCS components be derived from a trusted third party time service in accordance with the SAFE- BioPharma Registration and Certificate Management System Technical Specification. SAFE- BioPharma further requires that time derived from the trusted time service be used for establishing the time of:

- Initial validity time of a Subscriber’s Certificate
- Revocation of a Subscriber’s Certificate
- Posting of CRL updates
- OCSP or other CSA responses.

Asserted times shall be accurate to within three minutes.

## 7. Certificate, CRL, and OCSP Profiles

### 7.1 Certificate Profile

#### 7.1.1 Version Numbers

The CAs shall issue X.509 v3 certificates (populate version field with integer "2").

#### 7.1.2 Certificate Extensions

SAFE- BioPharma certificates shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof].

Critical private extensions shall be interoperable in their intended community of use.

Issuer CA and Subscriber certificates may include any extensions as specified by RFC 3280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP. SAFE- BioPharma conforming certificates must include all required extensions. Subject to PAA approval, an Issuer CA may request a waiver from providing certificates in conformance with recommended extensions, but such waiver request shall identify the date by which all certificates issued by that CA shall be in conformance.

Section 10 contains the certificate formats.

#### 7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CP shall use the following OID for identifying the subject public key algorithm:

rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
---------------	--

#### 7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC3280. Subject and issuer fields shall include attributes as detailed in the table below.

## Version 2.5

### CA Name Form

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0...1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc"
	Required	C	1	Country name, e.g., "C=US"
2	Recommended	CN	0...1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Certification Authorities" or similar text
	Optional	O	0...1	Issuer name, e.g., "O=XYZ Inc"
	Optional	C	0...1	Country name, e.g., "C=US"
	Required	DC	1	Domain name, e.g., "DC=xyzinc"
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc.

### Subject Name Form (Non-CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See right	1...N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0...N	As needed
	Required	O	1	Subject organization name, e.g., "O=ABC Ltd"
	Required	C	1	Country name, e.g., "C=GB"
2	Required	See right	1...N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0...N	As needed
	Optional	O	0...1	Subject organization name, e.g., "O=ABC Ltd"
	Required	DC	1	Subject organization domain name, e.g., "DC=abcld"

## Version 2.5

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc.

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

SAFE- BioPharma selected the above name forms for CA and Subject name to provide controlled uniqueness so that a given SAFE- BioPharma Member or Issuer's identifier does not conflict with that of another SAFE- BioPharma entity. To ensure that conflicts do not occur as SAFE- BioPharma grows and evolves:

- Each SAFE- BioPharma Issuer must register the O, C, and/or DC, attribute values it will use in the Issuer field of any certificates issued in accordance with this CP with SAFE-BioPharma.
- Each SAFE- BioPharma Issuer must register the O, C, and/or DC, attribute values it will require in the Subject field of CA certificates issued in accordance with this CP SAFE-BioPharma.
- Each SAFE- BioPharma Member must register the O, C, and/or DC, attribute values it will require in the Subject field of Subscriber certificates issued in accordance with this CP with SAFE-BioPharma.

The Organizational Unit (OU) attribute is optional in the above name forms, however, Subscriber certificates issued at the behest of SAFE-BioPharma(e.g., to independent investigators), must include an OU attribute populated with a unique identifier for the Subject. This unique identifier must associate to a specific Subscriber and must not change when issuing a new certificate to that Subscriber.

### 7.1.5 Name Constraints

The SBCA shall assert critical name constraints in certificates issued to Principal CAs appropriate for the PKI being certified and in accordance with the requirements listed below. SAFE- BioPharma PKIs may also use the excluded sub-tree feature of the Name Constraints extension in accordance with the requirements list below to assert what name spaces they do not trust and the name spaces they own.

The use of name constraints shall be employed in accordance with the following requirements:

- Use of Name Constraints shall not impact SAFE- BioPharma System operation (i.e., trust may not be broken at the signature level)
- SAFE-BioPharma must permit all SAFE- BioPharma Members in good standing via Name Constraints in SBCA issued certificates, but may permit or exclude non-SAFE-BioPharma Members as deemed appropriate by the SAFE- BioPharma Policy Approval Authority (PAA) for SAFE- BioPharma operations
- The SBCA shall utilize the permitted sub-tree feature in the Name Constraints extension within its cross-certificates to limit SAFE- BioPharma use to SAFE- BioPharma Members and Issuers, and to those non-SAFE- BioPharma entities (e.g., Regulators) that the PAA decides to explicitly allow

- Name Constraints expressed in a certificate issued to the SAFE- BioPharma Bridge CA shall not exclude an entire CA namespace (unless the Member first engages in a dispute resolution process) but may exclude any subtree within that CA's namespace
- Only a SAFE- BioPharma Member may request a Name Constraint relative to another SAFE- BioPharma Member or Subscriber in its Issuer's CA cross-certificate; an Issuer or SAFE-BioPharma shall never initiate such a request
- Upon initiating a request for use of a Name Constraint in a cross-certificate issued to the SBCA restricting all certificates issued by a SAFE- BioPharma Issuer or all certificates associated with a SAFE- BioPharma Member, the requesting Member shall file a formal dispute with SAFE-BioPharma in accordance with the SAFE- BioPharma Dispute Resolution Process; pending resolution of the dispute, such Name Constraints may be temporarily implemented by the associated Issuer
- A SAFE- BioPharma Issuer may apply Name Constraints within its own PKI, as long as it is not a cross-certificate with the SBCA as above, in accordance with Member guidance and Issuer policy
- SBCA shall not cross certify with an Issuer root CA whose cross-certificates include Name Constraints if the Issuer CA supports multiple Members from a common root. Alternately stated, unless an Issuer PKI instance supports one, and only one, Member, the SBCA shall not accept a name constrained cross-certificate from that Issuer CA.
- When an Issuer's cross-certificate includes a Name Constraints extension excluding a SAFE- BioPharma Issuer, Member or Subscriber, the SBCA shall protect each cross-certificate so it will not be visible to SAFE- BioPharma Community at large (that is, such cross-certificates shall not be published in a public or SAFE- BioPharma community accessible directory or .p7c file); each such cross-certificate shall be visible only to SAFE-BioPharma, the SBCA, the specific Issuer, and the associated Member

Principal CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in Section 10 subject to the requirements above.

The Issuer CA may obscure a Subscriber Subject name to meet local privacy regulations as long as such name is unique and traceable to a corresponding unobscured name. Issuer names may be obscured as well, but only if the Issuer provides the corresponding unobscured names to SAFE-BioPharma for name space management purposes. Issuer CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

### **7.1.6 Certificate Policy Object Identifier**

CA and Subscriber Certificates issued under this CP shall assert one or more of the OIDs listed in Section 1.2 as appropriate for the Issuer PKI.

### **7.1.7 Usage of Policy Constraints Extension**

The SBCA shall assert the policy constraints extension to inhibit policy mapping in Principal CA certificates. The SBCA shall not inhibit policy mapping in the certificates issued to the other Bridges (e.g., FBCA). The Issuer Principal CAs are required to adhere to the Certificate Formats described in this CP since inhibiting policy mapping may limit interoperability.

### **7.1.8 Policy Qualifiers Syntax & Semantics**

Certificates issued under the SAFE CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers.

### **7.1.9 Processing Semantics for the Critical Certificate Policy Extension**

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

## **7.2 CRL Profile**

### **7.2.1 Version Numbers**

CAs shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

### **7.2.2 CRL & CRL Entry Extensions**

CRLs shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof].

Critical private extensions shall be interoperable in their intended community of use.

Section 10 contains the CRL formats.

## **7.3 OCSP Profile**

OCSP requests and responses shall be in accordance with RFC 2560. Section 10 contains the OCSP request and response formats.

### **7.3.1 Version Number**

The version number for request and responses shall be v1.

### **7.3.2 OCSP Extensions**

Responses shall support the nonce extension.

## **8. Compliance Audit & Other Assessments**

CAs must have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of their Agreement with SAFE-BioPharma are being implemented and enforced.

### **8.1 Frequency Of Audit Or Assessments**

CAs, CSAs, CCS, and RAs shall be subject to a periodic compliance audit, which is no less frequent than once per year.

CAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA, CSA, CCS, or RA operations to validate that the subordinate components are operating in accordance with the security practices and procedures described in their respective CPS. Further, the PAA has the right to require aperiodic compliance audits of Issuer Principal CAs (and, when needed, their subordinate CAs) that interoperate with the SBCA. The PAA shall state the reason for any aperiodic compliance audit and shall bear the cost of the audit unless otherwise specified in the respective Issuer Agreement.

### **8.2 Identity & Qualifications Of Assessor**

The auditor shall demonstrate competence in the field of compliance audits for security and PKIs, and shall be thoroughly familiar with requirements that the PAA imposes on the issuance and management of SAFE- BioPharma PKI certificates. The compliance auditor shall perform such compliance audits as a primary responsibility.

### **8.3 Assessor's Relationship To Assessed Entity**

The compliance auditor either shall be a private firm, which is independent from the component being audited, or it shall be sufficiently organizationally separated from that component to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or CPS.

The PAA shall determine whether a compliance auditor meets this requirement.

### **8.4 Topics Covered By Assessment**

The purpose of a compliance audit shall be to verify that a PKI component is complying with the requirements of the applicable CP and CPS as well as the SAFE- BioPharma Standard and any applicable MOAs. Thus all applicable aspects of this CP, the Issuer CP, the component CPS and the SAFE- BioPharma Standard shall be covered by a compliance audit.

### **8.5 Actions Taken As A Result Of Deficiency**

The PAA may determine that a CA or CSA is not complying with its obligations set forth in this CP and any applicable MOAs. When such a determination is made, the PAA may suspend operation of the SBCA, or may direct the SBCA OA to cease interoperating with the affected Issuer Principal CA (e.g., by revoking the certificate that the SBCA had issued to the Issuer

Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how a component operates, and the requirements of this CP, the Issuer CP, the applicable CPS, any applicable MOAs, or the SAFE- BioPharma Standard, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Issuer responsible for the component of the discrepancy. If the component is a Principal CA, the Principal CA shall also notify the SBCA promptly; and
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the Issuer Agreement, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PAA may decide to halt temporarily operation of the SBCA, to revoke a certificate issued by the SBCA, or take other actions it deems appropriate.

### **8.6 Communication Of Results**

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Component, shall be provided to the PAA. The report shall identify the CP and CPS used in the assessment, including their dates and version numbers. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

## **9. Other Business & Legal Matters**

### **9.1 Fees**

#### **9.1.1 Certificate Issuance/Renewal Fee**

SBCA certificate issuance and renewal fees shall be in accordance with the SAFE- BioPharma Issuer Agreement.

Issuer CA certificate issuance and renewal fees shall be in accordance with the respective Agreement between the SAFE- BioPharma Member and Issuer.

#### **9.1.2 Certificate Access Fees**

SBCA certificate access fees shall be in accordance with the SAFE- BioPharma Issuer Agreement.

Issuer CA certificate access fees shall be in accordance with the respective Agreement between the SAFE- BioPharma Member and Issuer.

#### **9.1.3 Revocation or Status Information Access Fee**

SBCA certificate revocation or status information access fees shall be in accordance with the SAFE- BioPharma Issuer Agreement.

Issuer CA certificate revocation or status information access fees shall be in accordance with the respective Agreement between the SAFE- BioPharma Member and Issuer.

#### **9.1.4 Fees for Other Services**

Fees for other SBCA services shall be in accordance with the SAFE- BioPharma Issuer Agreement.

Fees for other Issuer CA services shall be in accordance with the respective Agreement between the SAFE- BioPharma Member and Issuer.

#### **9.1.5 Refund Policy**

Refunds from the SBCA shall be in accordance with the SAFE- BioPharma Issuer Agreement.

Refunds from an Issuer CA shall be in accordance with the respective Agreement between the SAFE- BioPharma Member and Issuer.

### **9.2 Financial Responsibility**

TBD.

### **9.2.1 Insurance Coverage**

TBD.

### **9.2.2 Other Assets**

TBD

### **9.2.3 Insurance/warranty Coverage for End-Entities**

TBD

## **9.3 Confidentiality of Business Information**

Information pertaining to the SBCA and not requiring protection may be made publicly available at the discretion of the PAA. Specific confidentiality requirements for business information are defined in the SAFE- BioPharma Operating Policies, the SAFE- BioPharma Standard, and associated Member and Issuer agreements.

### **9.3.1 Scope of Confidential Information**

Confidential information concerning the SBCA shall include any information provided by an Issuer PKI for purposes of cross-certifying with the SBCA, and of establishing and maintaining the provisions of its SAFE- BioPharma Issuer Agreement.

### **9.3.2 Information not within the Scope of Confidential Information**

As specified by the PAA and by the SAFE- BioPharma Operating Policies and Issuer Agreements.

### **9.3.3 Responsibility to Protect Confidential Information**

All PKI components shall be responsible for protecting the confidential information it possesses in accordance with the SAFE- BioPharma Operating Policies, and any applicable SAFE- BioPharma Member and Issuer internal rules.

## **9.4 Privacy of Personal Information**

### **9.4.1 Privacy Plan**

All Subscriber identifying information as defined by local privacy regulations shall be protected from unauthorized disclosure.

### **9.4.2 Information treated as Private**

Information to be treated as private shall be defined in the respective SAFE- BioPharma Member and Issuer Agreements, and SBCA and Issuer CA CPSs.

#### **9.4.3 Information not deemed Private**

Shall include any information not specifically identified under Section 9.4.2. Information included in the certificates shall be deemed not to be private.

#### **9.4.4 Responsibility to Protect Private Information**

Any sensitive information shall be explicitly identified in a CPS. All information stored electronically on the component equipment and not in the repository, and all physical records shall be handled as sensitive and shall be in accordance with SAFE- BioPharma Operating Policies. Access to this information shall be restricted to those with an official need-to-know in order to perform their official duties. Sensitive information may be released in accordance with other stipulations in Section 9.4.

#### **9.4.5 Notice and Consent to Use Private Information**

Requirements for notice and consent to use private information shall be defined in the respective SAFE- BioPharma Member and Issuer Agreements, and the Issuer CPs.

#### **9.4.6 Disclosure Pursuant to Judicial/Administrative Process**

Any disclosure shall be handled in accordance with SAFE- BioPharma Operating Policies, and any applicable SAFE- BioPharma Member and Issuer internal rules.

#### **9.4.7 Other Information Disclosure Circumstances**

Any disclosure shall be handled in accordance with SAFE- BioPharma Operating Policies, and any applicable SAFE- BioPharma Member and Issuer internal rules.

### **9.5 Intellectual Property Rights**

The PAA retains exclusive rights to any products or information developed by SAFE-BioPharma under or pursuant to this CP.

A CA Operational Authority shall not knowingly violate intellectual property rights held by others.

### **9.6 Representations & Warranties**

#### **9.6.1 CA Representations and Warranties**

In addition to the representation and warranties contained in the SAFE- BioPharma Operating Policies, the SBCA and Issuer PKI CAs represent and warrant that they shall conform to the stipulations of this document, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming their practices and procedures to the stipulations of the approved CPS;
- Ensuring that registration information is accepted only from RAs or LRAs who understand and are obligated to comply with this policy;

- Including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and the Subscribers are informed of the consequences of not complying with those obligations,
- Revoking the certificates of Subscribers found to have acted in a manner counter to those obligations; and
- Operating or providing for the services of an on-line repository that satisfies the obligations under Section 9.6.5, and informing the repository service provider of those obligations if applicable.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

### **9.6.2 RA Representations and Warranties**

An RA who performs registration functions as described in this policy represents and warrants that it shall comply with the stipulations of this policy, and comply with a CPS approved by appropriate authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

LRAs and TAs shall be bound to the RA obligations.

### **9.6.3 Subscriber Representations and Warranties**

Before being issued certificates, subscribers shall be required to sign a document containing the requirements the Subscriber shall meet in order to satisfy their obligations respecting protection of the private key and use of the certificate.

Subscribers shall represent and warrant that they:

- Accurately represent themselves in all communications with the PKI;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- Notify, in a timely manner, the CA, RA or LRA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- Use certificates in accordance with the Issuer CP and, when used to make or verify digital signatures on SAFE- BioPharma documents or transactions, the SAFE- BioPharma requirements governing such use.

Machine Operators assume the obligations of Subscribers for the certificates associated with their Machine Subscribers.

### **9.6.4 Relying Parties Representations and Warranties**

Parties who rely upon the certificates issued under the SAFE- BioPharma PKI represent and warrant that they shall be subject to the SAFE- BioPharma Standard governing such use, which include the following provisions:

- Use of the certificate is limited to the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- A check is performed for each certificate in a trust path for validity, using procedures described in the SAFE- BioPharma Standard, prior to reliance;
- Information is preserved as set forth in the SAFE- BioPharma Standard for later verification of signature validation.

### **9.6.5 Representations and Warranties of other Participants**

#### **9.6.5.1 Repository Representations and Warranties**

See Section 2.1.1.

#### **9.6.5.2 CSA Obligations**

A CSA, who provides revocation status and/or complete validation of certificates represents and warrants that it shall conform to the stipulations of this CP, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that certificate and revocation information is accepted only from valid CAs; and
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the certificate status.

A CSA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

#### **9.6.5.3 CCS Obligations**

A CCS that securely stores and uses roaming credentials when requested by the subscribers represents and warrants that it shall conform to the stipulations of this CP, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that subscriber private keys are protected from disclosure, modification and destruction at all times; and
- Subscriber private keys are used only when the subscriber appropriately authenticates to the CCS and requests the use of their key.

A CCS that is found to have operated in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

### **9.7 Disclaimers Of Warranties**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

## **9.8 Limitations of Liability**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements. In conformance with EU Directive 1999/93/EC, the SAFE- BioPharma Operating Policies, Section 5.7.3, specify the liability limits associated with a SAFE- BioPharma signature used for a SAFE- BioPharma System Transaction.

## **9.9 Indemnities**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

## **9.10 Term & Termination**

### **9.10.1 Term**

This CP shall become effective when approved by the PAA. This CP has no specified term.

### **9.10.2 Termination**

Termination of this CP is at the discretion of the PAA.

### **9.10.3 Effect of Termination and Survival**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

## **9.11 Individual Notices & Communications**

All communication between the PAA, SBCA OA, and Issuer PKI authorized agents shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronic, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting the SAFE- BioPharma Standard.

## **9.12 Amendments**

### **9.12.1 Procedure for Amendment**

The PAA shall review this CP at least once every year. The PAA shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to SAFE- BioPharma PKI participants and subscribers as specified in the Certificate Policy Plan. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

### **9.12.2 Notification Mechanism and Period**

This CP and any subsequent changes shall be made publicly available within one week of approval.

All policy changes under consideration by the PAA shall be disseminated to SAFE- BioPharma Participants and other parties designated by the PAA. All SAFE- BioPharma Participants and other parties designated by the PAA shall provide their comments to the PAA in accordance with the SAFE- BioPharma Change Management Process.

### **9.12.3 Circumstances under which OID must be changed**

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties, as determined by the PAA, in its sole discretion.

### **9.13 Dispute Resolution Provisions**

The use of certificates issued by the SBCA, and certificates issued by any entity cross-certified with the SBCA for SAFE- BioPharma purposes, is governed by contracts, agreements, and standards set forth by SAFE- BioPharma. Those contracts, agreements and standards include dispute resolution procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CP and intended for SAFE- BioPharma purposes.

### **9.14 Governing Law**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

### **9.15 Compliance with Applicable Law**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

### **9.16 Miscellaneous Provisions**

#### **9.16.1 Entire agreement**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

#### **9.16.2 Assignment**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

#### **9.16.3 Severability**

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12.

#### **9.16.4 Enforcement (Attorney Fees/Waiver of Rights)**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

**9.16.5 Force Majeure**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

**9.17 Other Provisions**

**9.17.1 Fiduciary relationships**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

**9.17.2 Administrative processes**

As specified in the SAFE- BioPharma Operating Policies and the applicable SAFE- BioPharma Member and Issuer Agreements.

## 10. Certificate, CRL, and OCSP Formats

This section contains the formats for the various PKI objects such as certificates, CRLs, and OCSP requests and responses. Trust anchor profiles are not provided since they are not relevant to interoperability.

## Version 2.5

### 10.1 SBCA → Principal CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	cn = SAFE Bridge CA ou = Certification Authorities o = SAFE-Biopharma Association c = US
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time format
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} 2048 bit if the PCA is a trust anchor; and 2048 in all cases for certificates lasting beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the SBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; {1 3 6 1 4 1 23165 1 3} for medium hardware assurance, {1 3 6 1 4 1 23165 1 2} for medium software assurance, and/or {1 3 6 1 4 1 23165 1 1} for basic assurance as appropriate
Policy Mapping	c=no; may express mappings [ {1.3.6.1.4.1.23165.1.3} { <PCA CP's medium hardware assurance OID> }, {1.3.6.1.4.1.23165.1.2} { <PCA CP's medium software assurance OID> }, and/or {1.3.6.1.4.1.23165.1.1} { <PCA CP's basic assurance OID> } ] or be absent as appropriate for each specific cross-certification instance to achieve proper SAFE certificate validation results
Basic Constraints	c=yes; cA=True; path length constraint optional (the path length constraint will typically be absent, but may be used to meet the needs of the specific cross-certification situation)
Name Constraints	c=yes; permitted subtrees: Principal CA DN prefix up to o=<company name>
Policy Constraints <sup>2</sup>	c=yes; requireExplicitPolicy skipCerts = 0; inhibitPolicyMapping skipCerts = 0 [the inhibitPolicyMapping field shall not be used when cross-certifying with another bridge CA]

<sup>2</sup> The SBCA shall not assert the inhibitPolicyMapping field when cross certifying with another Bridge, thus permitting transitive trust through the Bridge. The SBCA shall rely on other Bridges to assert the inhibit policy mapping constraint by setting skipCerts = 0 in the inhibitPolicyMapping field of the policy constraints extension so that a PKI cannot map policies.

## Version 2.5

---

Field	Value
Authority Information Access	c=no; id-ad-calssuers access method entry contains both an HTTP URL for a .p7c file containing certificates issued to SBCA and an LDAP URI. The HTTP URL shall appear first. . The host for calssuers must be different from host for CRL Distribution Points id-ad-ocsp access method entry contains HTTP URL for the SBCA OCSP Responder
CRL Distribution Points <sup>3</sup>	c=no
Inhibit Any-Policy	c=no; skipCerts = 0; host for CRL Distribution Points must be different from host for AIA calssuers

---

<sup>3</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

## Version 2.5

### 10.2 Principal CA → SBCA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time format
Subject Distinguished Name	cn = SAFE Bridge CA ou = Certification Authorities o = SAFE-Biopharma Association c = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request <u>to</u> the SBCA from this PCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request <u>from</u> the SBCA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; { <PCA's SAFE-equivalent CP OID(s)> }
Policy Mapping	c=no; [{ <PCA's SAFE-equivalent medium hardware assurance CP OID> }{1 3 6 1 4 1 23165 1 3}, {PCA's SAFE-equivalent medium software assurance CP OID> }{1 3 6 1 4 1 23165 1 2}, and/or {PCA's SAFE-equivalent basic assurance CP OID> }{1 3 6 1 4 1 23165 1 1},]
Basic Constraints	c=yes; cA=True; it is recommended that the path length constraint be absent
Name Constraints	c=yes; excluded subtrees: Principal CA DN prefix up to o=<company name>
Policy Constraints	Optional; c=yes; requireExplicitPolicy skipCerts=0; inhibitPolicyMapping field absent
Authority Information Access	c=no; id-ad-caIssuers access method entry: if PCA is a trust anchor, id-ad-caIssuers field is optional; id-ad-caIssuers access method entry must contain an HTTP URL for a .p7c file containing certificates issued to the superior CA that issued the PCA's certificate. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file must include every certificate issued to that superior CA; must not include self-signed certificates; and may include any other certificates of utility. id-ad-ocsp access method entry contains HTTP URL for the PCA OCSP Responder
CRL Distribution Points <sup>4</sup>	c = no; optional

<sup>4</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

## Version 2.5

Field	Value
Inhibit Any-Policy	c=no; skipCerts = 0

### 10.3 Issuer CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time format
Subject Distinguished Name	Unique X.500 Subject CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} 2048 bit for certificates lasting beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; if CA is not a trust anchor, include { <Issuer's SAFE Equivalent OID> } otherwise, absent. If CA is not a trust anchor, multiple certificate policies may be asserted as long as at least one policy mapped to a SAFE certificate policy is included.
Basic Constraints	c=yes; cA=True; path length constraint absent or value per Issuer PKI
Policy Constraints	Optional; c=yes; requireExplicitPolicy skipCerts = 0; inhibitPolicyMapping skipCerts = 0
Authority Information Access	c=no; id-ad-calssuers access method entry must contain an HTTP URL for a .p7c file containing certificates issued to Issuing CA. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file must include every certificate issued to that CA; must not include self-signed certificates; and may include any other certificates of utility. id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points <sup>5</sup>	c = no

<sup>5</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP

## Version 2.5

### 10.4 Human Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption 2048 bit for certificate that last beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	Optional; c=no; at least has Client Authentication {1.3.6.1.5.5.7.3.2 and Secure Email {1.3.6.1.5.5.7.3.4}
Certificate Policies	c=no; { <Issuer's SAFE equivalent OID> } Multiple certificate policies may be asserted as long as at least one policy mapped to a SAFE certificate policy is included
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-calssuers access method entry must contain an HTTP URL for either a) .p7c file containing certificates issued to the Issuing CA, or b) the Issuing CA. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file, if used, must include every certificate issued to that CA; must not include self-signed certificates; and may include any other certificates of utility. id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points <sup>6</sup>	c = no

URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

<sup>6</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

## Version 2.5

---

### 10.5 Machine Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption 2048 bit for certificate that last beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature; any additional uses are acceptable, but must not assert nonRepudiation if the certificate is dual-use
Extended Key Usage	Optional; c=no
Certificate Policies	c=no; { <Issuer's SAFE equivalent OID> } Multiple certificate policies may be asserted as long as at least one policy mapped to a SAFE assurance level is included
Subject Alternative Name	c=no; RFC822 email address <u>or</u> DNS address (required); others optional
Authority Information Access	c=no; id-ad-calssuers access method entry must contain an HTTP URL for either a) .p7c file containing certificates issued to the Issuing CA, or b) the Issuing CA. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file, if used, must include every certificate issued to that CA; must not include self-signed certificates; and may include any other certificates of utility. id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points <sup>7</sup>	c = no

---

<sup>7</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

### 10.6 Human Subscriber Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	As specified in Section 5.6 of this CP; expressed in UTC format if date is 12/31/2049 or earlier, else Generalized Time
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption 2048 bit for certificate that last beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Certificate Policies	c=no; { <Issuer's SAFE equivalent OID> } Multiple certificate policies may be asserted as long as at least one policy mapped to a SAFE certificate policy is included
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-calssuers access method entry must contain an HTTP URL for either a) a .p7c file containing certificates issued to the Issuing CA, or b) the Issuing CA. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file, if used, must include every certificate issued to that CA; must not include self-signed certificates; and may include any other certificates of utility. id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points <sup>8</sup>	c = no

<sup>8</sup> The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain two URIs, one for HTTP (i.e., of the form http://...) and one for LDAP (i.e., of the form ldap://...). The HTTP URI shall appear first. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

### 10.7 OCSP Responder Certificate

The following table contains the OCSP Responder certificate profile assuming that the OCSP Responder certificate is issued by the same CA as the Subscriber Certificate. Alternative trust models may be acceptable to the PAA.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than one month from date of issue
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	1024 or 2048 bit RSA key modulus, rsaEncryption; 2048 bit RSA key modulus, rsaEncryption for SBCA-issued OCSP responder certificates 2048 bit for certificate that last beyond 12/31/2010
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies	c=no; shall include all the certificate policy OIDs for which the Issuing CA issues certificates. Policy Qualifier for the SAFE-mapped OID shall be present and express a userNotice. This userNotice shall indicate that SAFE use is subject to limitations and limited liability as indicated in Issuer's CP or other associated trust scheme documentation. Note 1 provides examples of acceptable text for the userNotice.
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check	c=no; value is NULL (OID=id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5})
Authority Information Access	c=no; id-ad-calssuers access method entry must contain an HTTP URL for either a) a .p7c file containing certificates issued to issuing CA, or b) the Issuing CA. If an LDAP URI also appears, the HTTP URL must appear first. The .p7c file, if used, must include every certificate issued to that CA; must not include self-signed certificates; and may include any other certificates of utility.

## Version 2.5

---

Note 1: Examples of acceptable userNotice formats -

userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/for SAFE use see SAFE CP at <http://www.safe-biopharma.org/cp-pdf>; other use see [COMPANY] CP at [URL]/CPs incorporated by reference"

userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/CPs incorporated by reference (SAFE use: CP at [www.safe-biopharma.org/cp-pdf](http://www.safe-biopharma.org/cp-pdf) ; other use: [COMPANY] CP at [URL])"

userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/CPs incorporated by reference (SAFE use: CP at [www.safe-biopharma.org/cp-pdf](http://www.safe-biopharma.org/cp-pdf) ; [COMPANY] use: CP at [URL])"

### 10.8 CRL Format

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN (as specified in Section 7.1.4 of the SAFE CP)
thisUpdate	UTC format if date is 12/31/2049 or earlier, else Generalized time format
nextUpdate	UTC format if date is 12/31/2049 or earlier, else Generalized Time format (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTC format if date is 12/31/2049 or earlier, else Generalized Time format)
Issuer's Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
<b>CRL Extension</b>	<b>Value</b>
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier filed in certificates issued by the CA)
<b>CRL Entry Extension</b>	<b>Value</b>
Invalidity Date	c=no; optional
Reason Code	c=no; optional

### 10.9 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	Value
Version	V1 (0)
Requester Name	Optional; DN of the requestor
Request List	List of certificates as specified in RFC 2560
Signature	Optional; For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
<b>Request Extension</b>	<b>Value</b>
Nonce	c=no; optional
<b>Request Entry Extension</b>	<b>Value</b>
None	None

### 10.10 OCSP Response Format

See RFC2560 for detailed syntax. The following table lists the fields populated by the OCSP Responder.

## Version 2.5

---

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate) or DN of OCSP Responder
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status <sup>9</sup> , thisUpdate, nextUpdate <sup>10</sup>
Responder Signature	For current configurations: sha-1WithRSAEncryption {1 2 840 113549 1 1 5} By January 1, 2011: sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
<b>Response Extension</b>	<b>Value</b>
Nonce	c=no; Value in the nonce field of request (required, if present in request)
<b>Response Entry Extension</b>	<b>Value</b>
None	None

---

<sup>9</sup> If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

<sup>10</sup> The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

### 11. Directory Interoperability Profile

This section provides an overview of the directory interoperability profiles. The following topics are discussed:

- Protocol
- Authentication
- Naming
- Object Class
- Attributes

Each of these items is described below.

#### 11.1 Protocol

Each Issuer shall implement a directory system that provides either Lightweight Directory Access Protocol (LDAP), or HTTP access to certificates and CRLs. For LDAP, LDAP referrals shall be supported.

#### 11.2 Authentication

Each Issuer directory system shall permit “none” authentication to read certificate and CRL information.

Each Issuer shall be free to implement authentication mechanisms of its choice for browse and list operations.

Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc, shall require password over SSL or stronger authentication mechanism.

#### 11.3 Naming

This CP has defined the naming convention. Certificates shall be stored in the directory in the entry that appears in the certificate subject name. `issuedByThisCA` element of `crossCrossCertificatePair` shall contain the certificate(s) issued by a CA who name the entry represents.

CRLs shall be stored in the directory in the entry that appears in the CRL issuer name.

#### 11.4 Object Class

Entries that describe CAs shall be defined by the `organizationUnit` structural object class. These entries shall also be a member of `pkiCA cpCPS` auxiliary object classes.

Entries that describe individuals (human entities) shall be defined by the `inetOrgPerson` class, which inherits from other classes: `person`, and `organizationalPerson`. These entries shall also be a member of `pkiUser` auxiliary object class.

### **11.5 Attributes**

CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cPCPS attributes, as applicable.

User entries shall be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the repository.

## 12. REFERENCES

The following documents were used in part to develop this CP:

ABADSG	Digital Signature Guidelines, 1996-08-01. <a href="http://www.abanet.org/scitech/ec/isc/dsgfree.html">http://www.abanet.org/scitech/ec/isc/dsgfree.html</a> .
Directive 1999/93/EC	European Parliament and of the Council: Community Framework for Electronic Signatures, dated 13 December 1999
FIPS 140-2	Security Requirements for Cryptographic Modules, May 2001 <a href="http://www.csrc.nist.gov/cryptval/">http://www.csrc.nist.gov/cryptval/</a>
FIPS 186-2	Digital Signature Standard, January 2000 <a href="http://www.csrc.nist.gov/cryptval/">http://www.csrc.nist.gov/cryptval/</a>
FPKI-E	Federal PKI Certificate and CRL Extensions Profile, April 2000 <a href="http://www.csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls">http://www.csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls</a>
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. <a href="ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc">ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc</a>
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. <a href="Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html">Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html</a>
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Malpani et. Al., June 1999.
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Housley et. Al., April 2002.
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani et. Al., October 2003.
CIMC PP	Protection Profile for Certificate Issuing Management Components, Version 1, October 2001 <a href="http://www.csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf">http://www.csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf</a>

### 13. ACRONYMS & ABBREVIATIONS

This section addresses acronyms and abbreviations used in this CP and not already defined in the SAFE-BioPharma System Documentation Glossary.

DN	Distinguished Name
DSS	Digital Signature Standard
EU	European Union
FBCA	Federal Bridge Certification Authority
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
IETF	Internet Engineering Task Force
HTTP	Hypertext Transfer Protocol
HTTPS	SSL for HTTP
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKIX	Public Key Infrastructure X.509
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TA	Trusted Agent
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web



## 14. GLOSSARY

This glossary addresses terms used in this CP and not already defined in the SAFE- BioPharma System Documentation Glossary.

Access	Ability to make use of any information system (IS) resource.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
CA Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and that may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Components, PKI Components	Collective name for Certification Authorities, Certificate Status Authorities (CSAs), Registration Authorities (RAs) and Trusted Agents
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Duration	A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue".

## Version 2.5

---

E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Immediately	In accordance with an expedient and well defined process.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding signing Private Key. Legal non-repudiation refers to how well possession or control of the private Signing Key can be established.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Principal CA	The Principal CA is a CA designated by an Issuer to interoperate with the SBCA. An Issuer may designate multiple Principal CAs to interoperate with the SBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Issuer policy.
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Revoke (a Certificate)	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Server	A system entity that provides a service in response to requests from clients.

## Version 2.5

---

Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate Signing Key is certified by another CA, and whose activities are constrained by that other CA (see superior CA).
Superior CA	In a hierarchical PKI, a CA who has certified the certificate Signing Key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trust Anchor	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trust anchors are used to start certification paths.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

## 15. SAFE- BioPharma Standard Applicability to the SAFE CP

The SAFE- BioPharma Standard documents identified in the *SAFE- BioPharma Standard Document Set* are included by reference with this CP. These documents include:

DOCUMENT	IDENTIFIER
<b>Business Documents</b>	
System Documentation Glossary	GLOSSARY
SAFE-BioPharma Operating Policies	POLICIES
<b>Functional Process Guidelines</b>	
Electronic Identity Management Functional Process Guidelines	E-ID MGMT
Digital Signature Use & Verification Functional Process Guidelines	D-SIG USE
<b>System Governance</b>	
SAFE-BioPharma Change Management Process	CHANGE
SAFE-BioPharma Accreditation Process	ACCREDIT
SAFE-BioPharma Transaction Dispute Resolution Process	DISPUTE
<b>Specifications</b>	
SAFE-BioPharma Functional Specifications	FNSPEC
SAFE-BioPharma -Enabled Application Technical Specification	SEASPEC
SAFE-BioPharma End-User Systems Technical Specification	EUSSPEC
SAFE-BioPharma Machine Systems Technical Specification	MSSPEC
SAFE-BioPharma Registration and Certificate Management Technical Specification	RCMSPEC
SAFE-BioPharma Central Systems Technical Specification	CENTECHSPEC

## Version 2.5

In particular, the table below indicates which of these documents shall apply to each section of this CP.

	CP SECTION	GLOSSARY	POLICIES	E-ID MGMT	D-SIG USE	CHANGE	ACCREDIT	DISPUTE	FNSPEC	SEASPEC	EUSSPEC	MSSPEC	RCMSPEC	CENSYSPEC
1.	INTRODUCTION		X	X	X	X			X					
2.	PUBLICATION & REPOSITORY RESPONSIBILITIES			X	X				X				X	X
3.	IDENTIFICATION & AUTHENTICATION		X	X					X					X
4.	CERTIFICATE LIFE-CYCLE		X	X	X				X		X	X	X	
5.	FACILITY MANAGEMENT & OPERATIONS CONTROLS								X		X	X	X	X
6.	TECHNICAL SECURITY CONTROLS			X	X				X		X	X	X	X
7.	CERTIFICATE, CRL, AND OCSP PROFILES				X				X				X	
8.	COMPLIANCE AUDIT & OTHER ASSESSMENTS		X	X	X		X		X	X	X	X	X	X
9.	OTHER BUSINESS & LEGAL MATTERS		X	X	X	X	X	X	X				X	X
10.	CERTIFICATE, CRL, AND OCSP FORMATS				X				X				X	
11.	DIRECTORY INTEROPERABILITY PROFILE				X				X	X	X	X	X	X
12.	REFERENCES			X	X				X	X	X	X	X	X
13.	ACRONYMS & ABBREVIATIONS	X												
14.	GLOSSARY	X												