TC TrustCenter GmbH Certificate Policy for SAFE

Version 2.4 of April 25, 2008

Revision History

Version	Date	Revised By	Summary of Changes/Comments
1.0	28 Nov 2007	B. Kirsig	Initial version
1.1 To 1.95	27 Oct 2004 To 03 Mar 2008	B. Kirsig,	Intermediate versions with continuous improvements to include medium software and medium hardware assurance level
2.0	04 Mar 2008	B.Kirsig	Version approved by SAFE
2.1	06 Mar 2008	B. Kirsig	Added improvements required by T. Zagar
2.2	17 Mar 2008	B. Kirsig	Added basic assurance level
2.3	25 Mar 2008	B. Kirsig	Errors corrected
2.3.1	10 Apr 2008	B. Kirsig	Corrected Requestor Name in OCSP Request format
2.4	25 Apr 2008	B. Kirsig	Added roaming certificates and definitions for CCS

TABLE OF CONTENTS

1. Introduction

The SAFE Standard arose from an initiative sponsored by the Pharmaceutical Research and Manufacturers of America (PhRMA). The SAFE 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 operates as a closed business system model. SAFE utilizes Digital Certificates issued by Certification Authorities (CAs) meeting rules established by the SAFE-BioPharma Association.

In general, 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 will also support confidentiality of documents and transactions through the use of encryption certificates.

Because SAFE is to support the interoperation of Digital Certificates across these different enterprise Public Key Infrastructures (PKIs), TC TrustCenter will cross certify with the SAFE Bridge Certification Authority (SBCA).

To further increase the interoperability TC TrustCenter's SAFE CAs certificates will be issued by TC TrustCenter's Root CAs which are pre-configured in most of the current internet browsers and other applications.

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 Standard.

To allow an estimation of the trustworthiness of issued certificates a CA publishes a Certificate Policy (CP) describing the requirements which a Certification Authority (CA) shall employ in issuing certificates to a Subscriber. This includes certificate application, use and revocation or suspension of the certificate.

This Certificate Policy (CP) complies with the Internet Request for Comment (RFC) 3647 [RFC 3647]. It supports only certificates which are compliant with the requirements of the SAFE (Signatures and Authentication for Everyone) medium software assurance level and medium hardware assurance level. Details can be found at http://www.safe.org.

TC TrustCenter also issues other types of certificates using other CAs, among others qualified certificates in compliance with the German Electronic Signature Act and with the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. This CP does not govern other TC TrustCenter CAs or the issuance of qualified certificates under the German Signature Act. In Germany the issuance of qualified certificates is regulated in the German Electronic Signature Act, which does not cover other types of certificates.

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

TC TrustCenter may either issue qualified certificates in compliance with EU Directive 1999/93/EC by itself or make use of a subcontractor who is authorized to issue qualified certificates in a member state of the EU. All qualified certificates shall be consistent with the applicable laws of the issuer country. Qualified certificates may be used to produce electronic signatures which are legally considered in the European Union as being

equivalent to handwritten signatures. As a natural consequence qualified certificates may be issued to individual persons only.

TC TrustCenter's services are provided on the basis of TC TrustCenter's General Terms and Conditions (GTC), which are available from TC TrustCenter's repository.

TC TrustCenter's CPS in combination with TC TrustCenter's organization, processes, and procedures has been assessed by independent auditors to be compliant to the standard „ETSI TS 102 042 – Policy requirements for certification authorities issuing Public Key certificates", Version 1.2.3 of the European Telecommunications Standards Institute (ETSI). All certificates issued under this CP also fulfill at least the requirements of the "Lightweight Certificate Policy" (LCP) of ETSI TS 102 042.

This CP does neither constitute a declaration of self-escrow, nor does it state legally binding warranties. Any legally binding statements by TC TrustCenter are made in the General Terms and Conditions or in specific contracts (e.g. a Subscriber Agreement) between TC TrustCenter and other parties.

This CP makes extensive use of the vocabulary related to the field of digital signatures and certificates, cryptography and Public Key encryption, which is referenced in the GLOSSARY (section 14). The glossary also provides the definition of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

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 standard defines three assurance levels for use by SAFE 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.

This CP supports the all of the above mentioned assurance levels for Digital Certificates.

TC TrustCenter's Policies and Practices Board (PPB) has responsibility for directing the development of this CP, and for approving it and any updates to it.

CAs shall not assert the object identifiers (OIDs), listed below in any certificates their CAs issue, except in the *policyMappings* extension for certificates issued to the SBCA, and then only upon approval by the SAFE PAA.

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}

CAs shall use the OIDs listed in Section 1.2 of this CP.

The terms and provisions of this CP shall be interpreted under and governed by the SAFE Operating Policies and the provisions in section 9.

Where this CP refers to a "CA," that term shall be interpreted as TC TrustCenter's Root CAs, and TC TrustCenter's and its contractors' SAFE CAs. Where this CP refers to a "Root CA," that term shall be interpreted as one of TC TrustCenter's Root CAs.

Where a more specific or more general interpretation is required, this CP will so indicate.

1.1.1 Certificate Policy (CP)

To allow an estimation of the trustworthiness of issued certificates a CA publishes a Certificate Policy (CP) describing the requirements which a Certification Authority (CA) shall employ in issuing certificates to a Subscriber.

X.509 certificates issued under this CP shall contain one of the certificate policy OIDs of this CP (section 1.2) 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. One of the OIDs corresponds to the basic level of assurance, one corresponds to the medium software level of assurance, the third one to the medium hardware level of assurance.

1.1.2 Relationship between this CP and CA CPS

This CP states what assurance can be placed in a Certificate issued by CAs asserting one or more of the policy OIDs listed in Section 1.2. CA's Certification Practices Statement (CPS) shall state how CAs meet the requirements of this CP.

1.1.3 Relationship between the SAFE CP and this CP

The SAFE PAA has responsibility for mapping this CP with the SBCA. The relationship between the SAFE CP and this CP is asserted in CA certificates issued by or to the SBCA in the *policyMappings* extension. This extension shall indicate that the SAFE policy is equivalent to this CP. Conflicts between the SAFE CP and this CP shall be resolved at the time of CP mapping for cross certification.

1.1.4 Scope

CAs exists to issue electronic certificates in compliance with the SAFE standard in order to facilitate trusted electronic business activities among SAFE Members, between SAFE Members and their partners, and between SAFE Members and Regional Regulators. CAs will be cross-certifed with the SBCA and can issue certificates that map to the basic, medium software, and medium hardware certificate policy OIDs listed in the SAFE CP and in this CP (see Section 1.1).

The scope of this CP is limited to the TC TrustCenter Root CAs, TC TrustCenter and its contractors' SAFE CAs, and to the SBCA.

1.1.5 Interaction with PKIs External to SAFE

In order to allow interoperability with other PKIs, CAs shall cross-certify with the SBCA.

CAs shall not cross-certify with other CAs. However, CAs may be certified by TC TrustCenter's Root CAs.

1.2 Identification

The assurance levels expressed in this Certificate Policy are "medium hardware", "medium software", and "basic" as defined in the SAFE CP. The policy OIDs are registered in the Internet Assigned Numbers Authority (IANA) Objects Registry as follows:

> { trustcenter (1.2.276.0.44) policies (1) certificates (1) customerSpecific (6) safe (16) policies (1) mediumHardwareAssurance (1) }
>
> { trustcenter (1.2.276.0.44) policies (1) certificates (1) customerSpecific (6) safe (16) policies (1) mediumSoftwareAssurance (3) }
>
> { trustcenter (1.2.276.0.44) policies (1) certificates (1) customerSpecific (6) safe (16) policies (1) basicAssurance (4) }

CAs shall assert one or more of these OIDs in the *certificatePolicies* extension of the certificates issued to its Subscribers.

The SBCA policy OID 1.3.6.1.4.1.23165.1.1 resp. 1.3.6.1.4.1.23165.1.2 resp. 1.3.6.1.4.1.23165.1.3 shall be asserted in the *subjectDomainPolicy* field(s) and the corresponding policy OIDs of this CP shall be asserted in the *issuerDomainPolicy* field(s) of the *policyMapping* extension of the certificates issued by the CAs to the SBCA.

1.3 Community and Applicability

This CP adheres to the structure laid out in RFC3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", © 1999 by the Internet Society, in order to facilitate comparison with other Certificate Policies and to ease interoperability between the certificates issued by different CAs, thereby promoting electronic commerce.

In general, CAs issue certificates to everyone unless persons or organizations must be excluded due to legal restrictions.

CAs issue qualified certificates in compliance with applicable local law of the EU member state where the qualified CA resides as a legal entity and in compliance with the Directive 1999/93/EC of the European Parliament and of the Council. Qualified certificates may be used to produce electronic signatures which are legally considered by members of the European Union as being equivalent to handwritten signatures. These certificates shall be issued in accordance with the medium hardware assurance policy of this CP.

1.3.1 PKI authorities

1.3.1.1 SAFE Policy Approval Authority (PAA)

The SAFE PAA is a group of individuals chartered by the SAFE 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 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 requirements as a condition for allowing continued cross certification with the SBCA.

1.3.1.2 TC TrustCenter's Policies and Practices Board (PPB)

TC TrustCenter's Policies and Practices Board consists of a group of TC TrustCenter executives and has the responsibility for review, maintenance, clarification, approval, and updates to this CP.

TC TrustCenter's PPB is responsible for the approval of CA CPS for the CAs asserting policy OIDs identified in Section 1.2 of this CP. TC TrustCenter's PPB is also responsible for the approval of the cross-certification of CAs with the SBCA.

1.3.1.3 Certification authorities

A Principal CA is a CA within a PKI that has been designated to cross certify with the SBCA.

Signing CAs that issue end entity certificates shall be the Principal CAs under this CP.

CAs are authorized by the PBB to create, sign, and issue Public Key Certificates to End entities (see Section 1.3.3 for definition and description of End entities). CAs are responsible for all aspects of the issuance and management of certificates they issue including:

- Control over the registration process,
- The identification and authentication process,
- The Certificate generation process,
- Publication of Certificates to End entities and OCSP Responders,
- Revocation of all certificates issued,
- Publication of revocation information,
- Re-key of certificates,
- Establishment and maintenance of the CA CPS in accordance with this CP, and
- Performance of all aspects of the CA's 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 CA CPS.

TC TrustCenter may contract with external organizations to provide CA services only when the contractor agrees to abide by the terms of this CP and the TC TrustCenter CA CPS or submits a CPS for TC TrustCenter PPB approval. This CP shall then be part of the contract.

1.3.2 Registration authorities

A Registration Authority (RA) works on behalf of a CA. TC TrustCenter operates one or more in-house Registration Authorities. TC TrustCenter may contract with external organizations to provide RA services only when the contractor agrees to abide by the terms of this CP and the TC TrustCenter CA CPS. This CP shall then be part of the contract.

An RA collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's certificate.

Personal identification of end users applying for a certificate may take place at a location where the RA or the LRA is located.

Furthermore, face-to-face identification required for certificates issued by CAs can be performed in: (1) TC TrustCenter Ident Points®, or (2) German Post Offices, or (3) authorized Identification Points in organizations.

A TC TrustCenter Ident Point® provides the service of personal identification on behalf of and exclusively for TC TrustCenter. This results in a more efficient handling of registering end users.

The post offices offer the identification service to different companies, most notably banks, and it takes a day or two for the certificate to be issued once the identification process is completed. This service is available in Germany only.

Identification points in organizations may be installed if an organization operates a LRA. A LRA shall implement the functionality of an Identification Point for a limited group of users.

TC TrustCenter and external RA may also authorize individual persons to act as their representatives. These representatives are then authorized to perform the identity verification.

1.3.3 End entities

In the context of this document, end entity (or end user) is a synonym for Subscriber (or person). It refers to both natural and juristic persons which are able to perform legal acts, and who use certificates issued by the CAs.

End entities may include:

- SAFE Users of a SAFE Member requiring a Certificate for use in accordance with SAFE operating rules.
- Technical devices (also called 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.

A technical device needs a human sponsor acting as the representative of the technical device to an RA in order to register the device.

CAs issue qualified certificates in accordance with the applicable law of the country where the CA issuing these qualified certificates resides and in accordance with the Directive 1999/93/EC. Qualified certificates are issued to natural persons only.

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 signature (that is, a signature based on a Certificate issued by an Issuer meeting SAFE requirements). Further,

such Relying Party must meet requirements prescribed by the SAFE Standard for signature validation.

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

1.3.5 Other Participants

A CA 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. The LRA may service a limited population (e.g. an organization) as authorized by the RA. An LRA collects and verifies each End entities' identity and information for inclusion in the certificate. The requirements for LRAs are set forth in this document.

Any LRA shall be contractually bound to its CA. The CA shall register any LRA as local registration service provider. These LRAs shall be equipped with special Registration Officer (RO) certificates. Only data signed by one of the RO certificates shall be accepted by the CA system.

1.3.5.2 Trusted Agent (TA)

The TA collects and verifies 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 are set forth elsewhere in this document.

1.3.5.3 Certificate Status Authority (CSA)

CAs shall operate their own systems to provide status information for SAFE compliant certificates issued under this CP. CAs shall make Certificate status information available through one or more OCSP responders. Additional means to provide status information, e.g. a Certificate Revocation List (CRL) may be employed.

Other Certificate Status Authorities (CSAs) such as Server-based Certificate Validation (SCVP) to provide revocation status information or full certification path validation services shall not be used.

1.3.5.4 Machine Operator

The Machine Operator shall serve as the representative of a technical device to an RA or LRA in order to register the technical device with the PKI. The requirements for Machine Operators 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 certificates issued by a CA pursuant to a member relationship with SAFE, and corresponding contractual relationship with that SAFE member, and meeting SAFE requirements, shall only be as prescribed by SAFE and set forth in the agreements between SAFE and its members and issuers, along with any separate agreements between such entities that do not conflict with the SAFE requirements. Any other uses of such certificates, while allowed, shall not be considered as uses within the boundaries of SAFE 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 Contact details

1.5.1 Specification administration organization

This CP is administered by TC TrustCenter's Policies and Practices Board.

1.5.2 Contact person

TC TrustCenter
Certification Practice Administrator
TC TrustCenter GmbH
Sonninstrasse 24-28
20097 Hamburg
Germany
Phone: +49 (0)40 808026-0
Fax: +49 (0)40 808026-126
E-Mail: certificate@trustcenter.de

1.5.3 Person determining CPS suitability for the Policy

CA CPS must conform to this Certificate Policy.

TC TrustCenter's Policies and Practices Board consisting of TC TrustCenter executives determines the CPS's suitability and is responsible for its approval, thereby confirming that CAs assert one or more of the policy OIDs conform to this CP.

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 respective CPS. TC TrustCenter's Policies and Practices Board shall determine whether a compliance analyst meets these requirements.

2. Publication and Repository

2.1 Repositories

CAs shall operate repositories to support their PKI operations. CAs shall ensure interoperability with the SBCA repository so that Relying Parties may obtain 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 repository shall be accessible via both HTTP and LDAP methods.

2.1.1 Repository Obligations

Repository shall use an X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3), or Hypertext Transfer Protocol (HTTP).

Repository shall be available as required by the certificate information posting and retrieval stipulations of this CP.

Repository shall be subject to access control mechanisms to protect its availability and information as described in later sections.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

CA certificates issued by the SBCA and by the TC TrustCenter Root CA and the SBCA certificate issued by the CAs shall be published in their repository.

CAs shall publish CRLs in their repository.

2.2.2 Publication of CA information

TC TrustCenter shall publish this CP, its CPS, its GTC, and other related documents in its repository at http://www.trustcenter.de/repository.

TC TrustCenter shall publish the trust anchors on its website.

The directory of all certificates issued by the CAs may also be used for on-line certificate status inquiries; it shall be accessible from the repository as well. The Certificate Revocation Lists shall be publicly available.

CAs shall also offer an OCSP service for certificate status requests.

2.2.3 Interoperability

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

2.3 Frequency of publication

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

CRLs are updated at least daily. Details can be found in section 4.9.7. The certificate databases are updated every time a certificate is issued by the respective CA. Any other information listed in section 2.2.2 is updated every time it is modified.

2.4 Access controls on Repositories

Only authorized personnel shall be able to publish or modify any information referred to in section 2.2.2.

The repository shall not contain information not intended for public dissemination.

Repositories shall be made available through the Internet to SAFE Participants and other parties as determined by the respective PPB.

3. Identification and Authentication

In order to obtain a certificate, any Subscriber must apply for a certificate, and identify and authenticate himself to the CA or the RA. This section covers these topics.

3.1 Naming

3.1.1 Types of names

CAs 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 technical device 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

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

DNs in end entity certificates issued 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

Subject Alternative Name forms shall be interpreted in accordance with the applicable Internet Engineering Task Force (IETF) and ITU standards.

Organization and Organizational Unit fields shall be absent in the subject DN of any X.509 certificate issued for private use. If one (or both) of these fields are present in the subject DN, the certificate is either intended for commercial use or sponsored by that organization.

3.1.5 Uniqueness of names

Any Subscriber DN in a X.509 certificate issued must uniquely identify a single entity among all of the Subscribers. If necessary, a CA may append additional numbers or letters to an actual name in order to ensure the name's uniqueness. The same entity may have different certificates all bearing the same subject DN, but no two separate entities may share a common DN (and be issued by the same CA). In any case, there must not be two X.509 certificates having the same issuer DN and serial number.

3.1.6 Recognition, authentication and role of trademarks

CAs shall honor trademark claims that are documented by a Subscriber.

TC TrustCenter shall resolve any name collisions or disputes regarding CA certificates brought to its attention. Any dispute resolution shall be in accordance with the SAFE Operating Policies.

3.1.7 Name claim dispute resolution procedure

CAs shall not be responsible for resolving name claim disputes among Subscribers. CAs may add, at their own discretion, additional information to a name in order to make it unique among the names of certificates issued by the CAs covered under this Policy.

3.2 Initial Identity Proofing

In order to obtain a certificate, any Subscriber must apply for a certificate, and identify and authenticate himself to the relevant CA. This section covers these topics.

3.2.1 Method to prove possession of Private Key

In order to prove a Subscriber's possession of the Private Key corresponding to the Public Key contained in a certificate application, any certificate request submitted for a signature certificate shall be self-signed.

When the encryption key pair is not generated by the CA or the RA, the subscriber shall also prove the possession of decryption private key when applying for encryption certificates. 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.

3.2.2 Authentication of organization identity

Requests for certificates in the name of an organization (i.e., where the O-Field of the certificate is present) shall include the organization name, address, documentation of the existence of the organization, identity-proofing of the requesting organization agent, and proof of the agent's authorization to act on behalf of the organization. The CA or an RA recognized by the CA 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 Authentication of individual identity

For Basic Assurance Level:

The identity may be established by in-person proofing before a Registration Authority, Trusted Agent, or an entity certified by TC TrustCenter as being authorized to confirm identities on behalf of the respective CA. Also 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 identity may also be established remotely by verifying information provided by the applicant including ID number and account number through record checks either

with the applicable agency or institution or through credit bureaus or similar databases.

The identity proofing shall confirm that: name, date of birth, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual.

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:

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

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;
- 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.

For Medium Software and Medium Hardware Assurance Levels:

The identity of an individual shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by TC TrustCenter as being authorized to confirm identities on behalf of the respective CA. Also 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.

All information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may replace the in-person identity proofing requirement. Nevertheless, in this case a facsimile of the applicant's ID(s) shall be provided by the applicant.

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).

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;

- 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 non-US law.

For All Assurance Levels:

Identity shall be established no more than 30 days before initial certificate issuance.

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.

3.2.3.2 Identity-Proofing of Technical devices

Technical devices (e.g., routers, firewalls, servers, etc.) may be named as certificate subjects. In such cases, the technical device shall have a designated human representative called the Machine Operator. The representative shall be responsible for providing the following registration information for the device:

- 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.

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 TC TrustCenter's PPB for approval prior to use, and shall only be utilized with approval from the PPB.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

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

3.3 Identification and Authentication for Re-key Requests

Certificate re-key may be performed in case the existing key can no longer be used.
Examples are:

- The key is comprised and the certificate has to be revoked,
- The existing certificate has expired.

Rekey means changing the Public Key for an existing certificate by issuing a new certificate with a *different* (usually new) Public Key. The certificate name stays the same. It is different from renewal, which means issuing a new certificate, with an extended validity period, for the *same* Public Key.

3.3.1 Identification and Authentication for Routine Re-key

Subscribers shall identify themselves through use of their current Signing Key whose certificate has not yet expired 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.

SBCA shall establish its identity every three years.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked, the Subscriber shall generate a new key pair and reapply for a new certificate by going through the initial identity-proofing process described in Section 3.2 to obtain a new certificate. The revoked key pair is ineligible to sign and authenticate a re-key request.

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 *Certificate Application*

This section specifies requirements for initial application for certificate issuance.

For the purpose of cross-certification with the SBCA, CAs shall issue certificates to the SBCA.

The following application procedure shall apply to the certificate application by the SBCA:

SBCA shall complete the application process specified by the PPB and this CP.

The PPB shall review the information provided by the SBCA and determine whether to approve the application. If approved, the PPB shall enter into an Agreement with the SBCA (or amend an existing Agreement), and shall authorize the SAFE CA to issue the cross certificate to the SBCA.

Once the PPB approves issuance of a cross-certificate to the SBCA, the SBCA and the relevant RA shall perform the following steps:

- Both parties shall provide points of contact for verification of any agent roles or authorizations requested;
- The RA shall establish and record CA information per Section 3.2.3;
- SBCA shall generate a Public/Private Key pair to be cross-certified (if required);
- SBCA shall produce a properly formatted PKCS #10 cross-certificate request. The PKCS #10 request shall contain, at a minimum, the full DN of the SBCA, the SBCA's public key, the SBCA-generated Subject Key Identifier extension, and a signature enveloping certificate request;
- The RA shall verify that the Public Key submitted by SBCA forms a functioning key pair with the Private Key held by the SBCA (per Section 3.2.1).

These steps may be performed in any order that is convenient for the RA and SBCA that meets the requirements of this CP; but all must be completed prior to certificate issuance.

CAs shall be stood up upon written and authenticated approval from TC TrustCenter's PPB.

End entity applicants shall complete the online application form and follow the procedures described in section 4.1.1.

Completed applications for certificates shall then be submitted to a CA for processing, the result being either approval or denial.

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.

In general, the key pair and the certificate request shall be generated by the Subscriber during the process of applying for the certificate. In most cases this is automatically done by

- the Subscriber's internet browser or server software in case of a basic or medium software assurance level certificate or

– the Subscriber's software application in combination with a Secure Signature Creation Device (SSCD) in case of a medium hardware assurance level certificate.

Only on Subscriber's request or in special projects a CA shall generate keys on behalf of the Subscriber. Key generation then shall take place in a secure environment.

Keys for digital signatures shall be created in a cryptographic hardware device such as a smart card or hardware security module.

Keys for medium hardware assurance level certificates intended to serve the purpose of a Qualified Certificate in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC shall be created in cryptographic hardware devices (SSCDs) that are approved to be used for such purposes.

Other keys (e.g. encryption keys) may be created in software.

4.1.1 Submission of Certificate Application

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

Other applicants shall complete the online application form and generate a key pair in accordance with section 6.1.1. The applicant shall submit the certificate application to a CA using his/her internet browser or other application software. Submitting the application form will automatically deliver the Public Key to the CA in accordance with section 6.1.3.

4.1.2 Enrollment Process and Responsibilities

When applying for cross certification SBCA shall be responsible for providing accurate information in their application for cross certification. Upon creation, each cross-certificate and CA certificate shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered and published.

The end-user applicant shall provide all required information by completing and submitting the certificate application.

After receiving the application the CA shall check the application for errors and omissions. Pursuant to section 3.2.1, the CA shall perform the proof of possession of the private key (e.g., verify digital signature on the self-signed signature certificate request).

The CA shall then initiate the identification and authentication process as described in section 3.

4.2 Application Processing

Having received an application a CA shall begin to process the application. This shall include the verification of accuracy and correctness of all relevant data.

4.2.1 Performing Identity-proofing Functions

The identity-proofing for Subscribers shall meet the requirements specified in this CP.

To allow cross certification with the SBCA, 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. Only TC TrustCenter's in-house RA, or an associated LRA, or Trusted Agent as defined in section 1.3.2 shall perform identity-proofing for the SBCA personnel as set forth in section 3 of this CP.

4.2.2 Approval or Rejection of Certificate Applications

A CA shall either approve the application and issue the Subscriber's certificate upon successful completion of the identity-proofing process or reject the application and inform the applicant about any problems or inconsistencies. The application of the SBCA shall be approved or rejected by the relevant PPB.

If in doubt the PPB may accept or reject a certificate application. In case of critical questions the PPB may contact the SAFE PAA.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

CAs shall verify, as set forth in section 3.2.1, that the applicant is in possession of the Private Key and that the certificate request has the proper contents, for example a server certificate request must state the fully qualified server and domain name in the "Common Name" field. CAs shall verify the data contained in the request according to this CP. Because medium hardware assurance level certificates shall serve the purpose of qualified certificates CA or RA shall, in addition to the above, verify the data contained in the request according to the applicable local legislation on Electronic Signatures.

CAs shall generate certificates using the appropriate certificate format, and set validity periods and extension fields in accordance with relevant standards, such as X.509.

Certificates shall be checked to ensure that all fields and extensions are properly populated.

For certificate renewals, a CA shall generate and sign a new instance of the certificate, differing from the previous certificate only by the validity period.

Certificates shall be valid for no more than three years from the date of issuance.

After generation, verification, and acceptance, CAs shall post the certificate as set forth in section 4.4.2 and publish it in the repository.

4.3.2 Notification to Subscriber of Certificate Issuance

A CA shall either issue the Subscriber's certificate upon successful completion of the vetting process and notify the Subscriber about the issuance of the certificate, or inform the Subscriber about any problems or inconsistencies.

After a certificate has been issued the CA shall inform the Subscriber that the certificate is available and notify the Subscriber about the means for obtaining the certificate.

Certificates shall be made available to Subscribers either by allowing them to download the certificates from a web site or via a message containing the certificate. For example, an URL may be sent, describing where the Subscriber can obtain the certificate. The certificate may also be sent to the Subscriber in an e-mail message.

4.4 Acceptance

4.4.1 Certificate Acceptance

Downloading a certificate or installing a certificate from a message (see section 4.3.2) shall constitute the Subscriber's reception of the certificate.

Usage of the Private Key by the Subscriber, corresponding to a certificate issued under this CP, shall be deemed to be acceptance of the certificate.

By accepting a certificate the Subscriber warrants that all of the information provided by the Subscriber (and by its organization, where applicable) and included in the certificate, and all representations made by the Subscriber (and by its organization, where applicable) as part of the application and identification process, are true and not misleading.

4.4.2 Publication of the Certificate by the CA

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

CAs shall make issued certificates available to Subscribers immediately after the certificate has been issued. This includes the CA certificates.

Certificates shall be made available for retrieval from a certificate repository by third parties only if the Subscriber has declared his consent.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

There is no explicit notification to other entities. Certificates shall be published as specified in section 4.4.2.

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 Standard specifications and this CP. When employed for purposes covered under the SAFE operating rules, Subscriber Private Keys shall be used in accordance with the SAFE 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 issued under this CP shall conform to the profiles provided in this CP.

CAs shall issue information specifying the current status of all unexpired certificates. Relying Parties must process and comply with this information (e.g., CRL OCSP responses) in accordance with their obligations as SAFE Members or contracted parties of SAFE Members, whenever using certificates in accordance with SAFE operating rules.

4.6 Certificate Renewal

Certificate renewal 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.

Certificate renewal by re-using Subscribers asymmetric key pair shall only be allowed in case the Subscriber's key is not comprised.

Certificate renewal is not provided for individual certificates issued to natural persons.

Certificate renewal is permitted only for certificates issued to technical devices, e.g. for SSL certificates.

Certificate renewal is also permitted for the CA certificates.

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, the Subject name and attributes are unchanged, and meets the in-person identity proofing requirement specified in Section 3.3.1. In addition, the validity period of the certificate must not exceed the remaining lifetime of the Private Key, as specified in sections 4.3.1 and 6.3.2.

4.6.2 Who May Request Renewal

A CA may request renewal of its certificate.

The Machine Operator for a technical device Subscriber and LRAs/RAs may request renewal of Machine certificates.

4.6.3 Processing Certificate Renewal Requests

A CA or a RA 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 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

See section 4.4.3.

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.

4.7.1 Circumstance for Certificate Re-key

A CA may issue a new certificate to the Subscriber when the Subscriber has generated a new key pair and is entitled to a certificate in accordance with this CP.

A CA may issue a new certificate to a CA when the CA has generated a new key pair and is entitled to a certificate in accordance with this CP.

4.7.2 Who May Request Certification of a New Public Key

A CA may request re-key of its certificate.

The End-User Subscriber, Machine Operator for a technical device Subscriber (as applicable), and LRAs/RAs may request re-key of their respective 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 Agreement or MOA.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 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

See section 4.4.3.

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) must 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 validation process shall be identical to the identity-proofing in section 3.2.

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 Subscribers when some of the information in the certificate has changed, e.g., name change due to change in marital status, change in subject attributes, etc., and the Subscriber continues to be entitled to a certificate in accordance with this CP.

4.8.2 Who May Request Certificate Modification

The End-User Subscriber, Machine Operator for a technical device Subscriber (as applicable), and LRAs/RAs may request issuance of modified certificates.

SBCA may request modification of its certificate.

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 re-used as the new key. In addition, the validation of information that has not been in the old certificate 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 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

See section 4.4.3.

4.9 Certificate Suspension and Revocation

A certificate can either be suspended or revoked. If it is not certain whether the corresponding Private Key has been lost or compromised, the Subscriber must suspend the

certificate until matters have been clarified. If the Private Key has been compromised or lost for sure, or if Subscriber data represented in the certificate has changed substantially, the certificate must be revoked and the Subscriber must reapply.

If the certificate is revoked, it becomes invalid as soon as the CA has processed the revocation request. The certificate's serial number and time of revocation shall be included in the Certificate Revocation List, and subsequent status inquiries to the certificate repository shall result in a response citing the certificate as invalid.

If the certificate is suspended, it shall be placed on the Certificate Revocation List, and any status inquiries to the certificate repository while the suspension is in effect shall result in a response citing the certificate as invalid.

A certificate revocation may be requested at any time; the revocation service shall be available 24 hours a day, 7 days a week.

4.9.1 Circumstances for revocation

A certificate shall be revoked in case:

1. Identifying information or affiliation components of any names in the certificate become invalid;
2. Subject can be shown to have violated the stipulations of its respective Subscriber, Issuer or Member Agreement, or the stipulations of this CP;
3. Private Key is compromised or is suspected of compromise;
4. The SAFE PAA, TC TrustCenter PPB, or SAFE-BioPharma suspects or determines that revocation of a certificate is in the best interest of the integrity of the SAFE PKI;
5. Certification of the Subject is no longer in the interest of the CA that issued the certificate;
6. The Subscriber or his agent has submitted a revocation request as described in section 4.9.3;
7. The CA has learned about false information having been supplied in the certificate application that invalidates the certificate.
8. The Subscriber ends its subscription (see section 4.11).

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

Only the Subscriber or an RA can request revocation, except as noted in section 4.9.1, 7. Any entity or third party that confirmed any information contained in a certification should inform the issuing CA about the fact that this information is not or no longer correct, and request revocation in accordance with section 4.9.1, 7.

If a certificate states that its holder may act on behalf of a third party, this party may also request revocation of the certificate.

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.

There are several ways to submit a revocation request:

1. If the Subscriber is still in possession of his Private Key, he has the option of submitting an authenticated revocation request to the CA which issued the certificate.
2. If the Private Key has been lost or is inaccessible for any reason, the Subscriber may call the issuing CA by phone and authenticate by using the revocation password chosen when submitting the initial certificate application.
3. The Subscriber may request his certificate to be revoked by writing a letter to the issuing CA stating this request. Authentication is then provided by the Subscriber's signature. The Subscriber's signature on the revocation request must match the signature provided during the identity proofing process (e.g. signature on facsimile of ID or the Subscriber's declaration of identity, compare section 3.2.3.1).

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.

A Subscriber ceasing its relationship with TC TrustCenter PKI shall be required, prior to departure, to surrender to the CA, RA, or LRA (through any accountable mechanism) all cryptographic hardware tokens that were issued to the Subscriber by the TC TrustCenter 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

A CA shall process the revocation request, upon confirming that it originated from the Subscriber, as promptly and efficiently as possible. The total time needed to process a revocation request shall not exceed eighteen hours from the receipt of the revocation request.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL issuance frequency (if applicable)

Certificate status information shall be made available to all relevant entities through Certificate Revocation Lists (CRLs) which shall be available from the repository of the CA that issued the certificate.

CRLs may also be available upon request by e-mail.

Each CRL shall be digitally signed so that entities can validate the integrity of the CRL and the date of issuance, and it shall include a monotonically increasing sequence number.

CRLs shall be issued at least once a day.

In the case of CA compromise or Key compromise, a CA shall issue emergency CRL within 18 hours of notification.

4.9.8 Maximum Latency of CRLs

The maximum delay between the time that a SAFE Subscriber's certificate is revoked and the time that this revocation information is available to SAFE Relying Parties shall be no greater than 24 hours.

A SAFE Member may impose a requirement for a maximum delay that is less than 24 hours upon a CA based on the SAFE Member's assessment of the acceptable liability risk associated with this delay value relative to its business operations.

4.9.9 On-line revocation / status checking availability

A CA shall operate one or more OCSP Responders covering the certificates it issues. A list of all OCSP Responders operated by TC TrustCenter's SAFE PKI shall be published.

Any changes committed to the repository shall be immediately available to any Subscriber and / or relying party.

The certificate status can be checked on-line from the relevant certificate repository. Web sites of CAs shall contain information about additional means for validating a certificate's status, if such additional means are available.

4.9.10 On-line revocation checking requirements

It is the responsibility of the relying party to either

- obtain the latest CRL and check the revocation status, or
- check the revocation status on-line.

In order to check an on-line revocation status response a relying party must be in possession of or obtain the appropriate response signing certificate. This certificate may differ from the certificate of the issuer of the certificate being checked, and if so, it shall be available from the web site of the issuing CA or upon request by e-mail.

If the certificate used for revocation status responses differs from the certificate of the issuing CA, the revocation status signer certificate must be signed by the same CA using the same key as the certificate in question.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.11.1 Checking requirements for other forms of revocation advertisements

No stipulation.

4.9.12 Special requirements regarding key compromise

Depending on whether the Subscriber suspects or knows for sure that the Private Key has been compromised, the Subscriber is required to request suspension or revocation, respectively, as soon as possible. A Subscriber is not relieved from his obligations as a Subscriber until he has been notified by the issuing CA of the revocation of the certificate.

4.9.13 Circumstances for suspension

A certificate shall be suspended in case:

1. The Subscriber has informed the issuing CA that its certificate must be suspended, for example because the Private Key might have been compromised or lost;
2. TC TrustCenter or any other entity or third party that confirmed any information contained in a certificate suspects that false information has been supplied in the certificate application that might invalidate the certificate.

4.9.14 Who can request suspension

See section 4.9.2.

4.9.15 Procedure for suspension request

The reason code CRL entry extension shall be populated with "certificateHold". The Hold Instruction Code CRL entry extension shall be either absent or contain the OID for id-holdinstruction-reject per RFC 3280.

Also see section 4.9.3.

4.9.16 Limits on suspension period

The period for suspensions requested by the Subscriber must not exceed six weeks. A certificate may be suspended twice; a third suspension or exceeding the suspension period shall result in the certificate being revoked.

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3.1 before the certificate is removed from hold.

4.10 Certificate Status Service

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 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 Subscriber certificates shall be 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 standards.

Key escrow is prohibited for qualified certificates.

4.12.1 Key Escrow and Recovery Policy and Practices

In general, key escrow is not supported.

However, key recovery for decryption keys can be contractually agreed upon between TC TrustCenter and the Subscriber. Such a contractual agreement must then describe the key escrow and recovery procedures and practices.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Procedures for key encapsulation and recovery must be laid down in the contractual agreement mentioned in section 4.12.1.

5. Facility Management & Operations Controls

5.1 Physical Controls

CAs, OCSP Responders, and CCS shall impose physical security requirements specified in Section 5.1.2.

RA and LRA equipment shall be protected from unauthorized access at any time. The RA and LRA shall implement physical access controls to reduce the risk of equipment tampering even when cryptographic equipment 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 CA equipment and certificate status validation systems (i.e. OCSP responders) 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 status validation equipment and records.

5.1.2 Physical Access

CAs, OCSP, and CCS equipment shall always be protected from unauthorized access. The equipment shall be protected from unauthorized access at any time. Physical access controls shall be implemented to reduce the risk of equipment tampering even when cryptographic equipment 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, OCSP responders, 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 all sensitive computer systems and cryptographic equipment as Hardware Security Modules (HSMs).

Removable HSMs shall be inactivated prior to storage. When not in use, removable cryptographic hardware and activation information used to access or enable HSMs used by the CAs, the OCSP responders, 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 by the HSMs, and shall not be stored with the HSMs.

A security check of the facility housing the CA equipment, OCSP responders, , and CCS 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. cryptographic equipment shall be secured during the night);
- 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 activate all peripheral alarming systems. The alarming system shall be configured in such a way that activating it is possible only if all necessary physical protection mechanisms are in place and activated (e.g. all windows are locked and all sensors are active). The alarming system in combination with the access control system shall automatically log date and time of its activation.

5.1.3 Power and Air Conditioning

All CA systems shall have industry standard power and air conditioning systems to provide a suitable operating environment. 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.

On-line servers (e.g., those hosting directories) shall be provided with uninterruptable power supply sufficient for a minimum of six hours operation in the absence of commercial power, to support either a smooth shutdown of the CA operations or to re-establish commercial power.

5.1.4 Water Exposures

All CA systems shall have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire Prevention & Protection

All CA systems shall have industry standard fire prevention and protection mechanisms in place.

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.

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 CA, sufficient to recover from system failure, shall be made on a periodic schedule as described in the CA's 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 CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

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 entire PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the SAFE 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 SAFE Certificate Policy, Version 2.2, January 10, 2008, SAFE-BioPharma Association (SAFECP) defines the following 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 Functional Specification.
- *CA Agent* – authorized to request or approve certificates, or certificate revocations. This is a Registration Agent role per the SAFE Functional Specification.
- *CA Auditor* – authorized to view and maintain CA audit logs. This is an Agent role per the SAFE Functional Specification.
- *CA Operator* – authorized to perform system backup and recovery. This is a Machine Operator role per the SAFE Functional Specification.

In addition to the above CA roles, the SAFE 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 Functional Specification.
- *CSA Auditor* – authorized to view and manage CSA audit logs. This is an Agent role per the SAFE Functional Specification.
- *CCS Administrator* – authorized to configure and operate the CCS. This is a Machine Operator role per the SAFE Functional Specification.
- *CCS Auditor* – authorized to view and manage CCS audit logs. This is an Agent role per the SAFE 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 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 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 Functional Specification.
- *Machine Operator* – authorized to obtain a certificate on behalf of a Machine Subscriber. This is a Machine Operator role per the SAFE Functional Specification, and is also referred to as a "representative" for the Machine Subscriber in this CP.

CAs shall use a role concept with a denomination of roles different from the names above, but with comparable functions.

The following sections contain a detailed description of these roles.

5.2.1.1 CAM1

The CAM1 role shall be 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.

CAM1 shall not be permitted to issue certificates.

5.2.1.2 RA Officer

The RA Officer role shall be 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 Auditor

The Auditor role shall be responsible for:

- Reviewing, maintaining, and archiving CA, OCSP responder, and CCS audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA, the status validation systems, and the CCS are operating in accordance with its CPS.

5.2.1.4 IT-Security Officer

The IT-Security Officer role shall be responsible for:

- Preparation of key generation and quality control when key generation takes place; and
- Approving access for other Trusted Roles to critical systems (CA and OCSP responders); the actual access shall be changed by CAM1 for the CA and SysAd1 for the OCSP Responder.

5.2.1.5 SysAd2/CAM2

The SysAd2 role and the CAM2 role shall be responsible for:

- Routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.6 SysAd1

The SysAd1 role shall be responsible for:

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

5.2.1.7 Registration Authority (RA)

The RA responsibilities shall be:

- 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.

5.2.1.8 Local Registration Authority (LRA)

The LRA responsibilities shall be:

- 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.

5.2.1.9 Trusted Agent (TA)

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

5.2.1.10 Machine Operator

As specified by [SAFECP] a Machine Operator represents technical device 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.

Machine Operators are not applicable to any CA issuing qualified certificates, because in accordance with EU Directive 1999/93/EC qualified certificates shall be issued to natural persons only.

5.2.2 Number of Persons Required per Task

All activities at the CA system and certificate status validation system shall require (at least) dual control. Backup and activation of the CA certificate signing Private Key shall require dual control. Generation of certificate signing Private Keys shall require at least participation of three individuals.

Where multiparty control is required, at least one of the participants shall be an Administrator (CAM1 or SysAd1). All participants shall serve in a trusted role as defined in Section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Auditor Trusted Role.

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

The role concept shall be enforced by the CA system, the OCSP Responder system and CCS system.

Individual CA personnel shall be specifically designated to the roles defined in Section 5.2.1 above.

Individuals may assume more than one role except for the following restrictions:

- Individuals who assume an RA Officer role may also be assigned to the RA role. They may not assume any of the other roles.
- An individual assigned an IT-Security Officer role shall not perform any other trusted role except Auditor, and vice versa.
- An individual assigned the CAM1 role shall not perform any other trusted role except SysAd1, and vice versa.
- An individual assigned the CAM2 role shall not perform any other trusted role except SysAd2, and vice versa.

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

TC TrustCenter's Policies and Practices Board (PPB) is responsible and accountable for the operation of the CAs.

All persons filling trusted roles and personnel involved in issuing, managing, suspending and revoking certificates and managing related data and information 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 OCSP responders shall be set forth in the CA's 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 extent to which these investigations are performed is restricted by the applicable local legislation. TC TrustCenter shall conduct the investigations as far as permitted by applicable local laws.

Personnel shall present a certificate issued by the police, stating that the individual in question has no criminal record whatsoever. Personnel in positions of trust as defined in Section 5.2.1 shall present such a certificate at least once every five years while in a trust position. Regardless of the date of award, the highest educational degree shall be verified.

The German and the laws of some European counties, especially labour law legislation, allow only those investigations about an employee which are strongly necessary for the particular job. TC TrustCenter shall not make further investigations which may harm the employee's privacy or other human rights.

Background checks covering at least the last five years for each area, excepting the residence check which must cover at least the last three years, as required by the SAFE Certificate Policy (SAFECP), are not permitted by German law and the laws of some other European countries.

Information about the place of residence over the last three years is not deemed strongly necessary by German law and most of the EU member states. An employee can agree on providing this information; but it can not be enforced. Personnel in positions of trust shall provide a notification of any changes in their place of residence.

An employee can provide references voluntarily; but it can not be enforced.

Also the adjudication of the background investigation by a competent adjudication authority using a process consistent with U.S. Executive Order 12968 August 1995, or equivalent, is not permitted in Germany and most of the EU member states.

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 area 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 and area of training completed.

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

TC TrustCenter shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by this CP, applicable CPS, or other policies) involving the CA, its repository, OCSP responders, or CCS.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to CA, OCPS Responder, RA, LRA, and TA shall be subject to the same requirements as TC TrustCenter's staff performing similar functions (c.f. section 5.3 and subsections thereof).

5.3.8 Documentation Supplied To Personnel

CAs shall make available to its CA, CCS, RA, and LRA personnel this 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, OCSP responders, 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, OCSP responders, 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, OCSP responder, CCS, RA, or LRA) shall record the indicated type of auditable 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	OCSP	CCS	RA	LRA
SECURITY AUDIT					
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
IDENTITY-PROOFING					
Successful and unsuccessful attempts to assume a role	X	X	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X	X	X
Maximum number of authentication attempts 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	N/A	N/A	N/A	N/A	N/A
LOCAL DATA ENTRY					
All security-relevant data that is entered in the system	X	X	X	X	X
REMOTE DATA ENTRY					
All security-relevant messages that are received by the system	X	X	X	X	X
DATA EXPORT AND OUTPUT					
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X	X
KEY GENERATION					
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	N/A	N/A
PRIVATE KEY LOAD AND STORAGE					
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[1]	N/A	N/A

[1] In the CCS context, all access and use of subscriber private keys shall be auditable.

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

Auditable Event	CA	OCSP	CCS	RA	LRA
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
CONFIGURATION CHANGES					
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
PHYSICAL ACCESS / SITE SECURITY					
Personnel Access to room housing Component	X	X	X	-	-
Access to the Component	X	X	X	-	-
Known or suspected violations of physical security	X	X	X	X	X
ANOMALIES					
Software error conditions	X	X	X	X	X
Software check integrity failures	X	X	X	X	X
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	X	-	-	-
Electrical power outages	X	X	-	-	-

Auditable Event	CA	OCSP	CCS	RA	LRA
Uninterruptible Power Supply (UPS) failure	X	X	-	-	-
Obvious and significant network service or access failures	X	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, OCSP responders, CCS, RA, and LRA shall be reviewed at least once every month. 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.

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 have read access to the logs;
- Only the Auditor role may archive audit logs; and
- Audit logs are not modified.

The entity performing audit log archive (the Auditor role) 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 from the CA system and from the OCSP responders 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 IT-Security Officer (see section 5.2.1.4) shall be notified, and the IT-Security Officer shall determine 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 (see section 5.2.1.3) 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	X	N/A	N/A	X	X
Documentation of receipt and acceptance of certificates	X	N/A	N/A	X	X
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 CA and relevant Members. 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 CA.

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, CAs shall provide archived data and the applications necessary to read the archives to their respective archival facility, which shall retain the applications necessary to read this archived data.

If a Subscriber needs a longer retention period, this may be contractually agreed upon with the issuer of the certificate. Such an agreement shall specify the length of the extended retention period.

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 PPB, CA, or as required by law. Records and material information relevant to use of, and reliance on, a SAFE certificate shall be archived. Archived information of individual SAFE 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 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 applicable CPS or a referenced document (e.g. Archival Policy) 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 applicable CPS or Time-Stamp Policy 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 applicable 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.

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

CAs shall notify the SBCA and all member entities if any of the following cases occur:

- suspected or detected compromise of a CA;
- physical or electronic attempts to penetrate a CA;
- denial of service attacks on a CA components;
- any incident preventing a CA 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.

Each CA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth its CPS.

If a CA detects a potential hacking attempt or other form of compromise of 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 a 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 CA shall respond as follows:

- 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 key compromise of a CA, the CA shall request revocation of its certificates from all other CAs who have issued it a certificate. These other 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 TC TrustCenter Policies and Practices Board (PPB) shall also investigate and report to the SAFE 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

In the case of a disaster whereby a 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 SAFE PAA of actions they intend to take to reestablish the CA. If there is an agreement between the CA and the SBCA OA and SAFE PAA, the CA shall follow whatever processes have been set forth in this Agreement for that purpose. Preferably, the CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new Private and Public Keys, request a new cross-certificate with the SBCA. Finally, after being re-certified and re-issuing all cross certificates, 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.

If a 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 a CA is not available for any reason, then the SAFE PAA and the SBCA shall be securely and promptly notified in a fashion set forth in the respective Agreements. This will allow other Issuers within the SAFE PKI and those contracted with these Issuers to protect their interests as Relying Parties. The SAFE PAA shall also determine whether to revoke a CA certificate.

Directories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. Features shall be implemented to provide high levels of directory reliability (99.9% availability or better).

5.8 CA & RA Termination

5.8.1 CA Termination

A CA can only be terminated by the Board of Directors of the CA. A CA shall inform Subscribers of valid certificates (i. e., neither revoked nor expired). They shall be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation shall be sought.

Furthermore, TC TrustCenter, shall provide notice to the SBCA prior to any CA termination.

TC TrustCenter shall make a reasonable effort to archive the records of the CA and transfer them to a specified custodian, and to establish an acceptable procedure for Subscribers and relying parties for switching to a different provider of SAFE compliant certification services, in order to minimize the effects of the CA ceasing to provide these services by itself

If no alternative certificate provider continues the CA's services, all certificates that have not expired or have not been revoked by the respective Subscribers shall be revoked by the issuer of the certificates. A final CRL shall be published and made available for at least as long as the validity period of the certificate with the longest validity period indicates. The CRL nextUpdate date of this final CRL shall be past the expiration dates of all certificates issued by the CA. Subscribers shall be notified of such action taken by TC TrustCenter.

5.8.2 RA Termination

Upon termination, the RA certificate(s) shall be revoked and the RA shall provide archived data to the relevant 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 and associated OCSP responder signing keys shall be generated in FIPS 140-1/2 Level 2 (or higher) validated hardware cryptographic modules.

Cryptographic keying material for medium software and medium hardware assurance CAs and associated OCSP responders shall be generated in FIPS 140-1/2 Level 3 (or higher) validated hardware cryptographic modules under three party control.

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.

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 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.

Cryptographic keying material for End Entities for medium hardware assurance shall be generated in FIPS 140-1/2 Level 2 validated hardware Secure Signature Creation Devices (SSCDs) approved by the local Signature Law of the issuing CA for the purpose of qualified signatures. These devices shall be under the physical possession and control of the subscribers.

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 CA that generated the key. The sender 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 CA or RA 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

Each CA 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. Fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism;
- 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's system via secure means.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable. TC TrustCenter's PPB may determine that the security of a particular algorithm is compromised. The PPB shall then direct the CA 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 or better.

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 TC TrustCenter's PPB.

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 keyC*ertSign*.

6.2 Private Key Protection & Crypto-Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

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

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

FIPS 140-1/2	CA	OCSP	CCS	RA	LRA	Subscriber
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 at least two 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

Under no circumstances shall the CA signing Private Keys be backed up in clear. The CA signing private keys shall be backed up under the same multi-person control as the original signing key. A single encrypted backup copy of the signing key shall be stored at the CA location using a FIPS 140-1/2 Level 3 (or higher) HSM. A second encrypted backup copy shall be kept at the CA backup location using a FIPS 140-1/2 Level 3 (or higher) HSM. Procedures for CA signing private key backup shall be identified in the relevant CPS.

Under no circumstances shall the status validation system Private Keys be backed up in clear. The backup shall be performed under the same control as the key activation. A single encrypted copy of the OCSP key shall be stored at the OCSP Responder location using a FIPS 140-1/2 Level 3 (or higher) HSM. A second encrypted copy shall be kept at the OCSP Responder backup location using a FIPS 140-1/2 Level 3 (or higher) HSM.

6.2.4.2 Backup of Subscriber Signing Private Keys

RA and LRA signing private keys shall not be backed up. Subscriber medium hardware assurance signing 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.

Subscriber signing Private Keys shall not be backed up by CAs.

6.2.5 Private Key Archival

Signing private keys shall not be escrowed or archived by CAs.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys and all hardware signing keys shall be generated in FIPS 140-1/2 Level 3 (or equivalent) compliant Hardware Security Modules and remain in the same HSM. The CA and certificate status validation system Private Keys may be backed up in accordance with Section 6.2.4.1.

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.

6.2.7 Private Key Storage on Cryptographic Module

Hardware cryptographic modules 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; if video surveillance is present, cameras shall be positioned in such a way that they do not record PINs and passwords). Biometrics, if used, shall provide liveness property to ensure that the user is present.

6.2.9 Methods of Deactivating Private Keys

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. 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 hardware cryptographic modules is not required.

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

All public keys are 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.

All other certificates and associated Private Keys shall have a maximum validity period of 3 years.

The usage period of a decryption Private Key is determined by the user.

6.3.3 Subscriber Private Key Usage Environment

Subscribers shall use their private keys only from 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.

The activation data for a CA signing key shall be split between at least two disjoint groups of trusted roles. The activation data shall be changed upon CA re-key.

6.4.2 Activation Data Protection

Activation data shall 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.

All activation data for critical Private Keys shall be split among dedicated trusted roles, such that no single person has knowledge of all activation data.

Staff involved in the certificate issuance process may write down activation data on a sheet of paper, which the owner of the activation data shall then keep at all times (e.g. in his briefcase) or, alternatively, activation data may be stored electronically. If stored electronically, the activation data shall be encrypted using appropriate algorithms, parameters, and passwords.

For Subscribers it is required that the protection mechanism for activation shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts. CAs shall inform the Subscriber about this requirement.

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, status validation systems, 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.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

TC TrustCenter's SAFE PKI as well as the SBCA and other Issuer PKIs are infrastructure components that support a range of SAFE community applications, some of which may manage regulated data. TC Trustcenter's design, installation, and operation shall be documented by qualified personnel in a qualified manner to support SAFE 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.

CAs shall develop and produce appropriate qualification documentation establishing that all relevant systems are properly installed and configured, and operate in accordance with their own technical specifications and the technical requirements Imposed by SAFE. This documentation shall include:

- Installation manuals, procedures/scripts/data, acceptance criteria, and results.
- Operation manuals, procedures/scripts/data, acceptance criteria, certifications, and test results.

CA system development process shall meet the following requirements:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- All hardware and software 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 or the vendor uses tamper-evident packaging).
- If a CA develops its own software for the CA system, certificate status validation system, or CCS, this development shall take place in a controlled environment, and the entire development process shall defined and documented.
- Whenever possible CAs shall use tamper-evident packaging in combination with courier services for shipping or delivery of hardware and software in order to obtain a continuous chain of accountability, from the purchase location to the operations location.
- CA platform (server hardware, operating system software, and CA application software) shall be dedicated to performing CA functions. There shall be no non-CA applications installed on the CA platform.
- Certificate checking system platform (server hardware, operating system software, and certificate validation application software) shall be dedicated to performing certificate validation functions. There shall be no non-CSA applications installed on the certificate validation system platform.
- RA system platform (server hardware, operating system software, and RA application software) shall be dedicated to performing RA functions. There shall be no non-RA applications installed on the RA platform.
- CAs shall use centralized as well as host based firewalls in combination with local virus scanning software and intrusion detection/prevention systems to prevent malicious software from being loaded. Applications required to perform PKI relevant

operations shall either have been developed in-house or shall have been obtained from reliable sources authorized by TC TrustCenter's policies.

- Hardware and software updates shall be purchased or developed in the same manner as original equipment. Installation of hardware and software shall be performed by trusted and trained personnel in a defined manner.
- Before CA, certificate validation system, CCS, and RA hardware and software is used for the first time it shall be scanned for malicious code and periodically thereafter.
- CAs and certificate status validation systems shall use integrity protection software and automated alarming systems to detect all deviations from a defined state in system configurations and software applications. These mechanisms shall be activated permanently on the CA system and on the certificate status validation system. On all other systems these mechanisms shall be used periodically.

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, certificate status verification, and CCS software, when first loaded, shall be verified as being that supplied from the vendor, manufacturer, or developer, 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

CAs, certificate status verification systems, and CCS shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of 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, the certificate status verification system, or the CCS.

RA 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 firewalls and filtering routers.

All directories connected to the Internet shall provide continuous service to SAFE Participants and any entities authorized to rely upon Digital Signatures made meeting SAFE 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 routers to protect against denial of service and intrusion attacks.

The CA's 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

The system clock time for all CA, certificate status verification systems, and CCS components shall be derived from a trusted third party time service in accordance with the SAFE Registration and Certificate Management System Technical Specification. CAs shall use the German Legal Time provided via radio transmission by Germany's official time source, the Physikalisch Technische Bundesanstalt (PTB, http://www.ptb.de). CAs shall use this time source 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 certificate status verification 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 CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

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.

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 conforming certificates must include all required extensions.

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 (DN) 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.

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

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	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	Name of organization that object in the CN is affiliated to, e.g., "O=XYZ Inc" exactly as it appears in the documents provided for I+A
	Required	C	1	Country name, e.g., "C=US" exactly as it appears in the documents provided for I+A
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	Name of organization that object in the CN is affiliated to, e.g., "O=XYZ Inc"
	Required	DC	1	Domain name, e.g., "DC=xyzinc" exactly as documents provided for I+A
	Required	DC	1…N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as documents provided for I+A

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

- The CA 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.
- The CA 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 with SAFE-BioPharma.
- Each SAFE 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 the CA.

The Organizational Unit (OU) attribute is optional in the above name forms. As needed to support specific requirements, an OU attribute may be populated with a unique identifier for the Subject; when used, this unique identifier must associate to a specific Subject and must not change when issuing a new certificate to that Subject.

7.1.5 Name Constraints

A CA may assert critical or non-critical Name Constraints beyond those specified in the Certificate Formats in Section 10 subject to the requirements below.

The use of Name Constraints shall be employed in accordance with the following requirements from the SAFE CP (SAFECP):

- Use of Name Constraints shall not impact SAFE System operation (i.e., trust may not be broken at the signature level)
- SAFE-BioPharma must permit all SAFE Members in good standing via Name Constraints in SBCA issued certificates, but may permit or exclude non-SAFE Members as deemed appropriate by the SAFE Policy Approval Authority (PAA) for SAFE operations
- The SBCA shall utilize the permitted sub-tree feature in the Name Constraints extension within its cross-certificates to limit SAFE use to SAFE Members and Issuers, and to those non-SAFE entities (e.g., Regulators) that the PAA decides to explicitly allow
- Name Constraints expressed in a certificate issued to the SAFE 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 Member may request a Name Constraint relative to another SAFE 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 Issuer or all certificates associated with a SAFE Member, the requesting Member shall file a formal dispute with SAFE-BioPharma in accordance with the SAFE Dispute Resolution Process; pending resolution of the dispute, such Name Constraints may be temporarily implemented by the associated Issuer

- A SAFE 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 Issuer, Member or Subscriber, the SBCA shall protect each cross-certificate so it will not be visible to SAFE Community at large (that is, such cross-certificates shall not be published in a public or SAFE 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

CAs 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.

7.1.6 Certificate Policy Object Identifier

Certificates issued by CAs under this CP shall assert one or more of the OIDs listed in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

A CA is required to adhere to the certificate formats described in this CP.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued under this 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

A CA must have a compliance audit mechanism in place to ensure that the requirements of this CP and the applicable CPS and the provisions of TC TrustCenter's agreement with SAFE-BioPharma are being implemented and enforced.

8.1 Frequency of Audit or Assessments

CAs, status verification systems, CCS, and RA 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 SAFE PAA has the right to require aperiodic compliance audits of CAs. The SAFE 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 responsible PPB imposes on the issuance and management of 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.

The responsible PPB 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 this CP and the applicable CPS as well as the SAFE Standard. Thus all applicable aspects of this CP, applicable CPS, and the SAFE Standard shall be covered by a compliance audit.

8.5 Actions Taken as a Result of Deficiency

TC TrustCenter's PPB may determine that a PKI component is not complying with its obligations set forth in this CP. When such a determination is made, the PPB may suspend operation of the affected PKI component (e.g., CA, OCSP Responder, or RA, etc.), or may request the SBCA OA to cease interoperating with the affected CA (e.g., by revoking the certificate that the SBCA had issued to the affected 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 applicable CPS, or the SAFE Standard, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;

- The compliance auditor shall notify TC TrustCenter,
- TC TrustCenter shall notify the SBCA promptly; and
- TC TrustCenter 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 PPB may decide to halt temporarily operation of a CA, to revoke or request the revocation of the corresponding CA certificate, 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, shall be provided to the relevant PPB and SAFE 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

Certificate issuance and renewal fees shall be in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors, and the Subscriber.

9.1.2 Certificate Access Fees

Certificate access fees shall be in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors and the SAFE Member.

9.1.3 Revocation or Status Information Access Fee

Certificate revocation or status information access fees shall be in accordance with the agreement between the SAFE Member and TC TrustCenter and TC TrustCenter external CA and RA contractors.

9.1.4 Fees for Other Services

Fees for other CA services shall be in accordance with the respective agreement between the SAFE Member and TC TrustCenter.

9.1.5 Refund Policy

Refunds from a CA shall be in accordance with the respective Agreement between the SAFE Member and TC TrustCenter.

9.2 Financial Responsibility

For both kinds of relying parties, contractual and non-contractual relying parties,

- the regulations of indemnification of German or local law of the issuing CA, as applicable, shall be binding

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

To cover all financial expenses in case of termination TC TrustCenter shall make appropriate provisions.

9.3 Confidentiality of Business Information

Information pertaining to TC TrustCenter and not requiring protection may be made publicly available at the discretion of TC TrustCenter.

Specific confidentiality requirements for business information are defined in TC TrustCenter's Policies, the SAFE Standard, and associated Member and Issuer agreements.

9.3.1 Scope of Confidential Information

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

Furthermore, confidential information shall include any information provided by Subscribers for purposes of obtaining certificates from CAs, and of establishing and maintaining the provisions of its Subscriber agreement.

9.3.2 Information not within the Scope of Confidential Information

As specified by Subscriber agreements.

Certificates issued to Subscribers shall not be considered as confidential.

9.3.3 Responsibility to Protect Confidential Information

All of TC TrustCenter's PKI components and external CAs and RAs shall be responsible for protecting the confidential information in their possession in accordance with the SAFE Operating Policies, and any applicable SAFE Member and Issuer internal rules.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All Subscriber identifying information as defined by German privacy regulations, respectively local privacy regulations of the issuing CA, shall be protected from unauthorized disclosure.

9.4.2 Information treated as Private

German Law or the applicable local Law of the issuing CA, as applicable, define which information must be treated as private.

Further information to be treated as private shall be defined in the respective SAFE Member and Issuer Agreements, the respective CA's CPS, and in the respective Subscriber agreements.

9.4.3 Information not deemed Private

Any information not specifically identified under Section 9.4.2 shall be treated as not private. 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 the applicable 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 TC TrustCenter's Operating Policies and SAFE 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 Member and Subscriber agreements.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with SAFE Operating Policies and in accordance with German or local law of the issuing CA, as applicable.

9.4.7 Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with SAFE Operating Policies and in accordance with German or local law of the issuing CA, as applicable.

9.5 Intellectual Property Rights

Key pairs corresponding to certificates of CAs are the property of the issuing CA.

Key pairs corresponding to certificates of Subscribers are the property of the Subscribers that are named in these certificates.

This CP, TC TrustCenter's CPS, and TC TrustCenter's GTC are © 2008 by TC TrustCenter GmbH, Germany.

(See section 1.2 for full identification information.)

TC TrustCenter will 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 Operating Policies, 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 its 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 CP;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in certificates;

- 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.

If a CA is found to have acted in a manner inconsistent with these obligations, it shall be subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

RAs perform registration functions as described in this CP. The RAs represent and warrant that they shall comply with the stipulations of this CP, and comply with the associated CPS approved by TC TrustCenter's PPB.

If an RA is found to have acted in a manner inconsistent with these obligations, it is subject to revocation of RA certificate and RA responsibilities in the relevant SAFE PKI.

LRAs and Trusted Agents 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 CP, 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 issuing 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 this CP and, when used to make or verify digital signatures on SAFE documents or transactions, the SAFE 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 PKI represent and warrant that they shall be subject to the SAFE 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 Standard, prior to reliance;
- Information is preserved as set forth in the SAFE 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 Certificate Status Validation System Obligations

TC TrustCenter and CAs represent and warrant that their Status Validation Systems, who provide revocation status and/or complete validation of certificates, shall conform to the stipulations of this CP, including:

- Conforming to the stipulations of this CP and the applicable, 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.

TC TrustCenter or CA shall provide a CPS, as well as any subsequent changes, for conformance assessment.

If the Status Validation System is found to have acted in a manner inconsistent with these obligations shall be 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 Operating Policies and the applicable SAFE Member and Issuer Agreements.

9.8 Limitations of Liability

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

TC TrustCenter shall not be liable for failures which are not within their respective scope of responsibility, especially for technical failures or non availability of the certificate directory or specific certificates.

9.9 Indemnities

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

9.10 Term & Termination

9.10.1 Term

This CP shall become effective when approved by the SAFE PAA and TC TrustCenter's PPB. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of TC TrustCenter's PPB.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices & Communications

All communication between the SAFE PAA, SBCA OA, and TC TrustCenter's 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 associated Public Key is certified using a Certificate meeting the SAFE Standard.

9.12 Amendments

9.12.1 Procedure for Amendment

TC TrustCenter's PPB shall review this CP at least once every year. The PPB 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 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 PPB shall be disseminated to SAFE Participants and other parties designated by the PPB. All SAFE Participants and other parties designated by the PPB shall provide their comments to the PPB in accordance with TC TrustCenter's Change Management Process.

9.12.3 Circumstances under which OID must be changed

A 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 PPB being responsible for the affected OID, 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 purposes, including CAs is governed by contracts, agreements, and standards set forth by SAFE. 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 purposes.

9.14 Governing Law

As specified in the respective CA's General Terms and Conditions. The place of jurisdiction is described in the respective GTC. The GTCs are available at

- TC TrustCenter: http://www.trustcenter.de/en/about/repository.htm

9.15 Compliance with Applicable Law

As specified in TC TrustCenter's General Terms and Conditions.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

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

9.16.3 Severability

If parts of any of the provisions in this CP are incorrect or invalid, this shall not affect the validity of the remaining provisions 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 Operating Policies and the applicable SAFE Member and Issuer Agreements.

9.16.5 Force Majeure

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

9.17 Other Provisions

9.17.1 Fiduciary relationships

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

9.17.2 Administrative processes

As specified in the SAFE Operating Policies and the applicable SAFE 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.

CA Certificates can be downloaded from the issuing CA's website or from http://www.trustcenter.de/infocenter/root_certificates.htm.

10.1 TC TrustCenter Root CAs

TC TrustCenter's Root CAs use the following profile:

Data Field	**Value**		
Version	v3		
Serial Number	[Automatic no. according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption		
Issuer	**Attribute**	**Value**	**Encoding**
	CN	<Common Name of Root CA>	PrintableString
	OU	<Organisational Unit of Root CA>	PrintableString
	O	TC TrustCenter GmbH	PrintableString
	C	DE	PrintableString
Validity	25 years or less		
Subject	**Attribute**	**Value**	**Encoding**
	CN	<Common Name of Root CA>	PrintableString
	OU	<Organisational Unit of Root CA>	PrintableString
	O	TC TrustCenter GmbH	PrintableString
	C	DE	PrintableString
Subject Public Key	2048 bit RSA key modulus		
Extension	**Crit.**	**Value**	
basicConstraints	yes	cA: TRUE; pathlength absent	
keyUsage	yes	keyCertSign cRLSign	
subjectKeyIdentifier	no	[Key-ID: 160 Bit SHA-1-Hash of PubKey]	

10.2 SBCA → Principal CA Certificates

Must be defined by SBCA.

10.3 Certificates issued to SBCA

Field	Value
Version	V3 (2)
Serial Number	[Automatic unique no. according to TC TrustCenter standard]
Issuer Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption
Issuer Distinguished Name	CA DN encoded as printablestring; one attribute value per RDN
Validity Period	Six years or less
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	sha1withRSAEncryption or sha256 WithRSAEncryption
Extension	**Value**
Authority Key Identifier	c=no; [subject Key-ID in Issuer Certificate]
Subject Key Identifier	c=no; [from PKCS 10 request from the SBCA]
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; 1.2.276.0.44.1.1.6.16.1.4 and/or 1.2.276.0.44.1.1.6.16.1.3 and/or 1.2.276.0.44.1.1.6.16.1.1 cPSuri = http://www.trustcenter.de/guidelines
Policy Mapping	c=no; [{1.2.276.0.44.1.1.6.16.1.4}{1 3 6 1 4 1 23165 1 1}] and/or [{1.2.276.0.44.1.1.6.16.1.3}{1 3 6 1 4 1 23165 1 2}] and/or [{1.2.276.0.44.1.1.6.16.1.1}{1 3 6 1 4 1 23165 1 3}]
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	Absent
Policy Constraints	Absent
Authority Information Access	c=no; i accessMethod: caIssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this field shall be absent accessMethod: ocsp accessLocation: HTTP pointer to OCSP Responder
CRL Distribution Points	c = no; HTTP pointer to full and complete CRL
Inhibit Any-Policy	c=no; skipCerts = 0

10.4 Issuer CA Certificates

Data Field	**Value**		
Version	v3		
Serial Number	[Automatic no. according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption		
Issuer	**Attribute**	**Value**	**Encoding**
	CN	Common Name of Root CA	PrintableString
	OU	Organisational Unit of Root CA	PrintableString
	O	TC TrustCenter GmbH	PrintableString
	C	DE	PrintableString
Validity	10 years or less		
Subject	CA DN encoded as printablestring; one attribute value per RDN		
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}		
Issuer Signature	sha1withRSAEncryption or sha256 WithRSAEncryption		
Extension	**Crit.**	**Value**	
basicConstraints	yes	cA: TRUE; path length constraint absent	
keyUsage	yes	keyCertSign cRLSign	
certificatePolicies	no	1.2.276.0.44.1.1.6.16.1.4 and/or 1.2.276.0.44.1.1.6.16.1.3 and/or 1.2.276.0.44.1.1.6.16.1.1 Policy OIDs other than from this CP may be present cPSuri = http://www.trustcenter.de/guidelines	
subjectKeyIdentifier	no	[Key-ID: 160 Bit SHA-1-Hash of PubKey]	
authorityKeyIdentifier	no	[subjectKeyIdentifier from Issuer Certificate]	
authorityInfoAccess	no	accessMethod: calssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this field shall be absent accessMethod: ocsp accessLocation: HTTP pointer to OCSP Responder	
cRLDistributionPoints	no	HTTP pointer to full and complete CRL	

10.5 Human Subscriber Signature Certificates

10.5.1 Human Subscriber Certificate Basic Assurance Level

Data Field	**Value**		
Version	v3		
Serial Number	[Automatic unique no. according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption		
Issuer	CA DN encoded as printablestring; one attribute value per RDN		
Validity	[Date of Issuance] + 3 years		
Subject	**Attribute**	**Value**	**Encoding**
	CN	<First name + Last name>	PrintableString
	OU	<Organizational Unit> **optional**	PrintableString
	OU	<Organizational Unit for User ID> **optional**	PrintableString
	O	<Organization> **optional**	PrintableString
	Email	<Email address> **optional**	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}		
Issuer Signature	sha1withRSAEncryption or sha256withRSAEncryption		

Extension	**Crit.**	**Value**
basicConstraints	yes	cA: FALSE
keyUsage	yes	digitalSignature nonRepudiation
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) IPSecUser (1.3.6.1.5.5.7.3.7)
certificatePolicies	no	1.2.276.0.44.1.1.6.16.1.4 cPSuri = http://www.trustcenter.de/guidelines
subjectAltNames	no	rfc822-Name = <Email Address>
subjectKeyIdentifier	no	[Key-ID: 160 Bit SHA-1-Hash of PubKey]
authorityKeyIdentifier	no	[subject Key-ID in Issuer Certificate]
authorityInfoAccess	no	accessMethod: caIssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this field shall be absent accessMethod: ocsp accessLocation: HTTP pointer to OCSP Responder
cRLDistributionPoints	no	HTTP pointer to full and complete CRL

10.5.2 Human Subscriber Certificate Medium Software Assurance Level

Data Field	**Value**		
Version	v3		
Serial Number	[Automatic unique no. according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption		
Issuer	CA DN encoded as printablestring; one attribute value per RDN		
Validity	[Date of Issuance] + 3 years		
Subject	**Attribute**	**Value**	**Encoding**
	CN	<First name + Last name>	PrintableString
	OU	<Organizational Unit> **optional**	PrintableString
	OU	<Organizational Unit for User ID> **optional**	PrintableString
	O	<Organization> **optional**	PrintableString
	Email	<Email address> **optional**	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}		
Issuer Signature	sha1withRSAEncryption or sha256withRSAEncryption		
Extension	**Crit.**	**Value**	
basicConstraints	yes	cA: FALSE	
keyUsage	yes	digitalSignature nonRepudiation	
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) IPSecUser (1.3.6.1.5.5.7.3.7)	
certificatePolicies	no	1.2.276.0.44.1.1.6.16.1.3 cPSuri = http://www.trustcenter.de/guidelines	
subjectAltNames	no	rfc822-Name = <Email Address>	
subjectKeyIdentifier	no	[Key-ID: 160 Bit SHA-1-Hash of PubKey]	
authorityKeyIdentifier	no	[subject Key-ID in Issuer Certificate]	
authorityInfoAccess	no	accessMethod: caIssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this field shall be absent accessMethod: ocsp accessLocation: HTTP pointer to OCSP Responder	
cRLDistributionPoints	no	HTTP pointer to full and complete CRL	

10.5.3 Human Subscriber Certificate Medium Hardware Assurance Level

Data Field	**Value**		
Version	v3		
Serial Number	[Automatic no. according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption or sha256withRSAEncryption		
Issuer	CA DN encoded as printablestring; one attribute value per RDN		
Validity	One year or less		
Subject	**Attribute**	**Value**	**Encoding**
	CN	<First name + Last name>	PrintableString
	OU	<Organizational Unit> **optional**	PrintableString
	OU	<Organizational Unit for User ID> **optional**	PrintableString
	O	<Organization> **optional**	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	RSA Key, 1024 Bit, SHA-1 From January 1, 2011: RSA Key, 2048 Bit, SHA-256		
Issuer Signature	sha1withRSAEncryption or sha256withRSAEncryption		

Extension	Crit.	Value
keyUsage	yes	digitalSignature nonRepudiation
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
certificatePolicies	no	1.2.276.0.44.1.1.6.16.1.1 cPSuri = http://www.trustcenter.de/guidelines Policy OIDs other than from this CP may be present
Private CertExtensions	no	QcStatement: QcCompliance = Compliance (0.4.0.1862.1.1) id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod
subjectAltNames	no	rfc822-Name = <Email Address>
authorityKeyIdentifier	no	[Key-ID of Issuer Certificate]
authorityInfoAccess	no	accessMethod: caIssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this field shall be absent accessMethod: ocsp accessLocation: HTTP pointer to OCSP Responder
cRLDistributionPoints	no	HTTP pointer to full and complete CRL
subjectKeyIdentifier	no	[Key-ID: 160 Bit SHA-1-Hash of PubKey]

10.6 Machine Certificate

Currently not supported.

10.7 Human Subscriber Encryption Certificate

Currently not supported.

10.8 OCSP Responder Certificates

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	CA DN encoded as printablestring; one attribute value per RDN
Validity Period	No longer than one month from date of issue
Subject Distinguished Name	OCSP Responder DN encoded as printablestring; one attribute value per RDN
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption; From January 1, 2011: RSA Key, 2048 Bit, SHA-256
Issuer's Signature	sha-1WithRSAEncryption or 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; 1.2.276.0.44.1.1.6.16.1.4 and/or 1.2.276.0.44.1.1.6.16.1.3 and/or 1.2.276.0.44.1.1.6.16.1.1 cPSuri = http://www.trustcenter.de/guidelines userNotice. Note 1 provides examples of acceptable text for the userNotice.
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check (OID=id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5})	c=no; value is NULL
Authority Information Access	c=no; accessMethod: caIssuers accessLocation: HTTP pointer to p7c file containing Issuing CA certificates; single certificate shall be in a .cer file; if the issuing CA only has self-signed certificate, this extension shall be absent.

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; TC CP at http://www.trustcenter.de/guidelines"

10.9 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	CA DN encoded as printablestring; one attribute value per RDN
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	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
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)
CRL Entry Extension	**Value**
Invalidity Date	c=no; optional
Reason Code	c=no;
Hold Instruction	c=no, optional Only present if reasonCode = certificateHold (6) only id-holdinstruction-reject is permitted OID

10.10 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}
Request Extension	**Value**
Nonce	c=no; optional
Request Entry Extension	**Value**
None	None

10.11 OCSP Response Format

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

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	DN of OCSP Responder or Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[2], thisUpdate, nextUpdate[3]
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
Response Extension	**Value**
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**

[2] If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

[3] The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

Field	Value
None	None

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

CAs shall implement a directory system that provides HTTP access to certificates and CRLs. In addition, directory systems may provide Lightweight Directory Access Protocol (LDAP). For LDAP, LDAP referrals shall be supported.

11.2 Authentication

Authentication to read certificate and CRL information shall not be required.

Authentication mechanisms for browse and list operations may be implemented, but are not mandatory.

Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc, shall require password over SSL or stronger authentication mechanism. Such actions shall be allowed for authorized personnel only.

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.

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. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
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 http://www.csrc.nist.gov/cryptval/
FIPS 186-2	Digital Signature Standard, January 2000 http://www.csrc.nist.gov/cryptval/
FPKI-E	Federal PKI Certificate and CRL Extensions Profile, April 2000 http://www.csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html
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.
CIMC PP	Protection Profile for Certificate Issuing Management Components, Version 1, October 2001 http://www.csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf
RFC3280	Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile ftp://ftp.isi.edu/in-notes/rfc3280.txt
RFC3647	Internet X.509 Public Key Infrastructure, Certificate Policy and Certificate Practices Framework ftp://ftp.isi.edu/in-notes/rfc3647.txt
SAFECP	SAFE Certificate Policy, Version 2.3, April 15, 2008, SAFE-BioPharma Association http:/safe-biopharma.org

13. ACRONYMS & ABBREVIATIONS

This section addresses acronyms and abbreviations used in this CP and not already defined in the SAFE 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 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".
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.
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]

I. Addendum for SISAC Users

Some certificates issued by TC TrustCenter's SAFE CAs are intended to be used within the Mortgage Industry and in accordance with the Secure Identity Services Accreditation Corporation ("SISAC") standards.

The SISAC Accredited Certificate Management Service ("Mortgage Industry CMS") is a service designed to meet the requirements of the mortgage industry as defined in Certificate Policy Requirements Document, Version 2.0 dated December 10, 2007 ("CPRD") issued by Secure Identity Services Accreditation Corporation ("SISAC"), a subsidiary of the Mortgage Bankers Association of America ("MBA").

The purpose of this "Addendum" to TC TrustCenter's CP for SAFE is to define the requirements on issuing certificates fulfilling two sets of requirements simultaneously:

- the SISAC standard;
- the SAFE BioPharma standard.

The requirements defined by these two standards are similar but not identical. In some areas the SISAC CPRD imposes additional requirements on the issuance and management of certificates. This Addendum to TC TrustCenter's "Certificate Policy for SAFE" addresses the additional requirements for the usage of SAFE compliant certificates issued by TC TrustCenter under the SAFE medium hardware assurance level in the SISAC environment.

Because certificates have to be in conformance with both standards, and the requirements are similar but not identical, the sum of the requirements exceeds each individual standard.

SISAC distinguishes the following levels for certificates:

1. **Basic:** This level is relevant to environments where the risks and consequences of data compromise are not considered by the Certificate Holder/Subscriber to be of major significance. This may include access to private information where the likelihood of malicious access is not high.
2. **Medium**: This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. [Note: There are two types of Medium assurance certificates: Medium-Hardware where the private key is stored within a hardware token; Medium-Software where the private key is stored within a software token.]
3. **High**: This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are severe. This may include very high value transactions or high levels of fraud risk. User Organizational certificates are not permitted to be issued at the High assurance level.
4. **Device** certificates are issued at a single assurance level. Device certificates identify a particular device within an organization and the application of that device. Examples of Device certificates include SSL Server and IPSEC VPN certificates. [Note: There are two types of Device certificates: Device-Hardware where the private key is stored within a hardware token; Device-Software where the private key is stored within a software token.]

Within the SISAC environment this CP supports only the SAFE medium hardware assurance level for Digital Certificates. Such certificates may also serve as SISAC Medium-Hardware level certificates. All certificates used by SISAC users for SISAC purposes have to fulfill both requirements simultaneously.

All Subscriber certificates issued in accordance with this CP and in accordance with [SISAC CPRD] and [SAFECP] shall –additionally- serve the purpose of Qualified Certificates in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC.

I.1.1.3.1.1 Relationship between the SAFE CP and this CP

The SAFE PAA has responsibility for mapping this CP with the SBCA. The relationship between the SAFE CP and this CP is asserted in CA certificates issued by or to the SBCA in the *policyMappings* extension. This extension shall indicate that the SAFE policy is equivalent to this CP. Conflicts between the SAFE CP and this CP shall be resolved at the time of CP mapping for cross certification.

I.1.1.3.2 Relationship between the SISAC CPRD and this CP

The SISAC Policy Management Authority (PMA) is the body with the highest level of authority to oversee the creation and update of the approved CPs, review and approve Certification Practice Statements, monitor and ensure CPRD compliance. The PMA has responsibility for mapping this CP with the CPRD to ensure compliance with SISAC requirements.

I.1.1.4 Scope

The scope of this CP is limited to the TC TrustCenter Root CAs, TC TrustCenter and its contractors' SAFE CAs, SISAC/MBA, and to the SBCA.

I.1.3.3 End Entities

In addition to section 1.3.3 the term End Entities also refers to SISAC Users and other users within the Mortgage Industries.

End Entities in the SISAC Environment have to sign a Subscriber Agreement. A Subscriber Agreement is a contract between a Certificate Holder/Subscriber and the Issuing CA that details the procedures, rights, and obligations of each party with respect to a Certificate issued to the Certificate Holder/Subscriber.

I.1.3.4 Relying Parties

Prior to relying on a Certificate issued by Chosen Security pursuant to this CP/CPS, a Relying Party in the SISAC environment must review and agree to the Relying Party obligations set forth in this CP/CPS and to the Relying Party Agreement. Different applications require different levels of security, and the Relying Party is solely responsible for making the decision to rely on digitally signed data verifiable by the respective Certificate in the given application context, and for checking that the Certificate is neither invalid nor revoked.

I.1.3.5.5 Centralized Credential Server

Centralized credential servers are not supported in the SISAC environment.

I.1.4 Aplicability

In addition to the provisions in section 1.3 of the TC TrustCenter CP for SAFE this Addendum to the TC SAFE CP applies to all users of the Chosen Security Mortgage Industry CMS including Chosen Security, CMS Customers, Subscribers, and Relying Parties.

I.1.5 Obligations

I.1.5.1 Subscriber obligations

A Certificate Holder/Subscriber's obligations must be governed by a Subscriber Agreement. The Subscriber Agreement must require Certificate Holder/Subscribers to

(a) provide complete and accurate responses to all requests for information made by the AIA (or an LRA) during Applicant registration and the I&A process,

(b) upon issuance of a Certificate naming the Applicant as the Certificate Holder/Subscriber, review the Certificate to ensure that all Certificate Holder/Subscriber information included in it is accurate, and

(c) to accept or reject the Certificate in accordance with Section 4 of this CPRD.

Subscribers must use their keys and certificates in a manner and for a purpose consistent with the requirements of this CP and this Addendum and the SISAC CPRD, especially the protection of private keys.

If a Subscriber discovers or has reason to believe there has been a compromise of the private key or the associated password/PIN, or the information within the certificate is incorrect or has changed, the subscriber must promptly

- Notify either TC TrustCenter, Chosen Security, or the RA which approved the certificate application and request revocation of the certificate in accordance with section 4.9

and

- Notify any person that may reasonably be expected by the subscriber to rely on the subscriber's certificate.

Subscribers have to cease use of their private key at the end of the key usage period.

I.1.5.2 Relying Party obligations

Prior to relying on a Certificate issued by one of TC TrustCenter's CAs pursuant to this CP, a Relying Party must review and agree to the Relying Party obligations set forth in this CP and the Relying Party Agreement. Different applications require different levels of security, and the Relying Party is solely responsible for making the decision to rely on digitally signed data verifiable by the respective Certificate in the given application context, and for checking that the Certificate is neither invalid nor revoked.

I.4.9.7 CRL Issuance Frequency

Certificate status information shall be made available to all relevant entities through Certificate Revocation Lists (CRLs) which shall be available from the repository of the CA that issued the certificate.

CRLs may also be available upon request by e-mail.

Each CRL shall be digitally signed so that entities can validate the integrity of the CRL and the date of issuance, and it shall include a monotonically increasing sequence number.

CRLs shall be issued at least once a day.

In the case of CA compromise or Key compromise, a CA shall issue an emergency CRL within 6 hours of notification.

I.4.9.8 Maximum Latency of CRLs

The maximum delay between the time that a SISAC User's certificate is revoked and the time that this revocation information is available to Relying Parties shall be no greater than 12 hours.

Certificate suspension is not required for certificates issued in the SISAC environment.

I.8.5 Actions Taken as a Result of Subsequent Audits

In addition to the provisions in section 8.5 audit results must be submitted to SISAC. If irregularities are found, TC TrustCenter must submit, within forty-eight hours, a report to SISAC as to the action that the affected CA will take to remedy such irregularities. Where the CA fails to take satisfactory action in response to the audit report, in SISAC's sole discretion, SISAC may:

(i) acknowledge the irregularities, but allow the CA to continue operations until the next Audit;

(ii) allow the CA to continue operations for the maximum of 90 days pending correction of any problems prior to revocation; or

(iii) immediately revoke the CA's Accreditation Agreement and Conditional License. Any decision regarding which of these actions to take will be in the sole discretion of SISAC, and the election of any such remedy is not a waiver by SISAC or the MBA of any other remedies available to it.

I.9.2 Financial Responsibility

I.9.2.1 Insurance Coverage

The issuing CA maintains and will continue to maintain Errors and Omissions insurance coverage in an amount of not less than five million dollars ($5,000,000.00) relating to its provision of Mortgage Industry CMS.

Whenever any party wishes to or has to notify any other party with respect to this CP/CPS, such a notice shall be given by digitally signed e-mail or in writing.

The former must be sent to

pkipolicy@trustcenter.de,

the latter must be delivered either by certified mail (including return receipt request), or by a courier service confirming the delivery in writing, and it must be addressed to:

TC TrustCenter GmbH
CA Administration
Sonninstrasse 24-28
20097 Hamburg
Germany

or

Chosen Security, Inc
CA Administration
57 Wells Avenue
Suite 1
Needham, MA 02459

Electronic e-mail must be confirmed by the recipient within one week, by digitally signed e-mail. If the sender does not receive a confirmation within the specified time period, the notice must be re-sent in writing as described above.

I.9.6.1 CA Representations and Warranties

An Issuing CA must agree under the terms of the Authorized Relying Party Agreement to bear liability resulting from improper I&A with respect to a Certificate, up to the liability limits established for such type of Certificate, if an Authorized Relying Party's decision to rely on a Certificate Constitutes Reasonable Reliance was reasonable. Reliance by an Authorized Relying Party must be considered Reasonable Reliance under such agreement if such party:

- Has entered into an Authorized Relying Party Agreement and agreed to be bound by the terms and conditions thereof and of the Approved CP.

- Verified that the Certificate in question was not revoked at the time of the Authorized Relying Party's reliance, by conducting a revocation status check of the Certificate's then-current validity as required by the AIA.

- Used the Certificate for purposes appropriate under this CP, this Addendum, and under circumstances where reliance would be reasonable and in good faith in light of all the circumstances that were known or should have been known to the Authorized Relying Party

prior to reliance. (An Authorized Relying Party bears all risk of relying on a Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate).

The CA must provide the following warranties in the Authorized Relying Party Agreement, to all Authorized Relying Parties:

- The CA has issued and managed the Certificate in accordance with the approved CP.

- The CA complied (or caused its LRAs to comply) with the requirements of the approved CP when verifying the identity of the Certificate Holder/Subscriber.

- There are no material misrepresentations of facts, in the Certificate, known to the CA, and the CA has taken steps as required under this CP to verify the information contained in the Certificate.

- The CA has taken all steps required by this CP to ensure that the Certificate Holder/Subscriber's submitted information has been accurately transcribed to the Certificate.

- The Certificate meets all material requirements of this CP and any applicable CPS.

These warranties must be offered to any Authorized Relying Party who:

(i) relies on a Certificate in an electronic transaction in which the Certificate played a material role in verifying the identity of one or more persons or devices;

(ii) exercises Reasonable Reliance on that Certificate; and

(iii) follows all procedures required by this CPRD and by the applicable Authorized Relying Party Agreement for verifying the revocation status of the Certificate.

These warranties must be made to the Authorized Relying Party as of the time the Repository is referenced to determine Certificate revocation status, but cannot be enforceable if the Authorized Relying Party is notified that the Certificate has been revoked at that time.