Trans Sped PCA Certificate Policy For SAFE-BioPharma

August 02, 2013

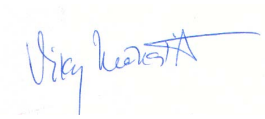
Version 1.0

Document Control

Author(s):	Viky Manaila, Rich Furr
Change Control:	Initial version
Approver:	Trans Sped Policy Management Authorities
Issue Date:	August 02, 2013
Version:	1.0
Source File:	
Security:	Trans Sped/Verizon
Distribution:	

Version History

Version	Date	Revised By	Summary of Changes/Comments
0.1	August 2013		Initial release
0.2	August 2013	Jose Lopez	Review, amended as required
1.0	August 2013	Rich Furr Viky Manaila Jose Lopez	Final version



Digitally signed by Viky-Teodora Manaila
DN: c=RO, title=Managing Director, givenName=Viky-Teodora, sn=Manaila, cn=Viky-Teodora Manaila, o=Trans Sped srl
Date: 2014.03.17 18:00:47 +02'00'

TABLE OF CONTENTS

Approval Statements

The signature below represents the acknowledgement by the Trans Sped Policy Management Authority (PMA) that this Certificate Policy has been approved and has been incorporated into the Trans Sped Document Set.

_____

Trans Sped PMA Chairperson

_____

Date

1 Introduction

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

SAFE-BioPharma operates as a closed business system model. SAFE-BioPharma utilizes Digital Certificates issued by Certification Authorities meeting the rules established by the SAFE-BioPharma Association

These Issuers may be internal to a bio-pharmaceutical company, or may be operated by a third-party provider such as Trans Sped. The intention is that SAFE-BioPharma Digital Certificates will support Digital Signatures on documents and transactions needed to comply with global regulatory and legal requirements

Because SAFE-BioPharma supports the interoperation of Digital Certificates across these different Public Key Infrastructures (PKIs), SAFE-BioPharma operates a SAFE-BioPharma Bridge Certification Authority (SBCA) to cross-certify with each Principal PCA (PCA) of each Issuer in the SAFE-BioPharma network.

As required for interoperation with government regulatory authorities, the SBCA is also cross-certified with the US Federal Bridge Certification Authority (FBCA) in order to permit others who are also cross-certified with the FBCA to trust Digital Certificates meeting the SAFE-BioPharma Standard.

Trans Sped will issue EU-qualified SAFE-BioPharma Digital Certificates. This CP defines the policies under which the Trans Sped PCA operates and shall be used to cross-certify the Trans Sped PCA with the SBCA. This Certificate Policy (CP) complies with the Internet Request for Comment (RFC) 3647 [RFC 3647]. For purposes of this Trans Sped CP, all terms used shall have the meanings set forth in the SAFE-BioPharma System Documentation Glossary.

SAFE-BioPharma Subscriber certificates issued at Medium Assurance level in accordance with this CP and the SAFE-BioPharma CP (SAFECP) will meet the requirements of Qualified Certificates in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC and ETSI Standard EN 319 411-2 V1.1.1 (2013-01).

Trans Sped may either issue qualified certificates 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 qualified 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.

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.

This CP defines two assurance levels for use by SAFE-BioPharma participants:

1. The medium assurance hardware level for Digital Certificates issued to Subscribers (also known as End Entities). This certificate is EU Qualified in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC.
2. The medium assurance hardware roaming level for Digital Certificates issued to Subscribers. (also known as End Entities). This certificate is also EU Qualified in accordance with Annex I and II of the European Union (EU) Directive 1999/93/EC.

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

This CP has been developed under the direction of Trans Sped Policy Management Authorities (PMA) and that group has the responsibility for directing the development of this CP, and for approving it and any updates to it.

Any use of or reference to this CP outside the context of the Trans Sped PCA is completely at the using party's risk. Trans Sped PCA shall not assert the SAFE-BioPharma CP object identifiers (OIDs) listed below in any certificates they issue, except in the *policy Mappings* extension for certificates issued to the SBCA, and then only upon approval by the SAFE-BioPharma PAA.

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

sbca OBJECT IDENTIFIER	::= { 1.3.6.1.4.1.23165}
sbca-cert-policies OBJECT IDENTIFIER	::= {sbca 1}
id-sbca-cert-policies-basicAssurance	::= {sbca-cert-policies 1}
id-sbca-cert-policies-mediumSoftwareAssurance	::= {sbca-cert-policies 2}
id-sbca-cert-policies-mediumHardwareAssurance	::= {sbca-cert-policies 3}
id-sbca-cert-policies-basicAssurance-SHA256	::= {sbca-cert-policies 4}

id-sbca-cert-policies-mediumSoftwareAssurance-SHA256	::= {sbca-cert-policies 5}
id-sbca-cert-policiesmediumHardwareAssurance-SHA256	::= {sbca-cert-policies 6}

All of the requirements for "……–sha256" OIDs are the same as those for the corresponding certificate policy OID without "–sha256" in it except for the hashing requirements for generation of PKI objects such as certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses.

The terms and provisions of this CP shall be interpreted under and governed by the SAFE-BioPharma Operating Policies, applicable Trans Sped Certification Practice Statements (CPSs) and Trans Sped's operating policies and procedures.

As described in this CP and its respective CPSs, Trans Sped shall establish a self-signed PCA henceforth known as the Principal Certificate Authority (PCA). Where this CP refers to "CA" that term shall be interpreted to mean Trans Sped's PCA. Where a more specific or limited interpretation is required (e.g., referring to a particular PCA such as the SBCA, or PCA), this CP shall so indicate.

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

1.1.1 CPS/CP

The Trans Sped PCA is subject to the /Trans Sped PCA CPS/CP documentation.

1.1.2 PCA Certificate Policy (CP)

Certificates issued by the PCA covered under this CP shall contain one or more registered OIDs in the certificate policies extension that in turn shall be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. An OID corresponds to a specific level of assurance established by a CP that should be available to Relying Parties.

1.1.3 Relationship between this CP and the Trans Sped SAFE-BioPharma Issuer Certificate Practices Statement (CPS)

This CP states what assurance can be placed in Certificates issued by Trans Sped's PCA by Relying Parties participating in the SAFE-BioPharma framework. The CPS implementing the provisions of this CP states how Trans Sped meets the requirements of this CP.

1.1.4 Relationship between the SAFE-BioPharma CP and the Trans Sped SAFE-BioPharma Issuer CPS

This CP states what assurance can be placed in Certificates issued by the Trans Sped PCA by Relying Parties participating in the SAFE-BioPharma framework. A CPS implementing the provisions of this CP states how Trans Sped meets the requirements of this CP.

1.1.5 Relationship between the SAFE-BioPharma CP and the Trans Sped SAFE-BioPharma Issuer CP

The SAFE-BioPharma PAA (PAA) has responsibility for mapping the CPs of the Issuers cross-certifying with the SBCA. The relationship between the SAFE-BioPharma CP and this CP is asserted in PCA certificates issued by or to the SBCA in the *policyMappings* extension. This extension shall indicate that the SAFE-BioPharma policy is equivalent to one or more policies as defined by this CP. Conflicts between the SAFE-BioPharma CP and this CP shall be resolved at time of CP mapping for cross certification. In the event of a conflict, Trans Sped shall submit one or more waivers to identify the timeframe for conflict resolution for PAA approval.

1.1.6 Relationship between the SAFE-BioPharma CP and the SAFE-BioPharma Standard

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

1.1.7 Scope

The term Issuer applies to any SAFE-BioPharma Issuer permitted by the SAFE-BioPharma PAA to cross-certify it's PKI with the SBCA and to issue certificates that map to one or more of the certificate policy OIDs listed in the SAFE-BioPharma CP. In the context of the SAFE-BioPharma framework, upon cross-certification of its SAFE-BioPharma PCA, Trans Sped shall act as an external supplier to SAFE-BioPharma Stakeholders and supply Certificates as directed by that SAFE-BioPharma Stakeholder.

References to a Principal PCA within this CP refer to a Trans Sped PCA that has submitted an application to be cross-certified with the SAFE-BioPharma Bridge PCA. PCA and will issue end-entity certificates to SAFE-BioPharma Subscribers.

1.1.8 Interaction with PKIs External to SAFE

The PCA shall not cross-certify with any PCA other than the SBCA. The PCA shall not issue any PCA certificates.

1.2 Identification

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

{ trans sped (1.3.6.1.4.1.39965) safe (2) policies (1) mediumAssuranceHardware (1) }

{ trans sped (1.3.6.1.4.1.39965) safe (2) policies (1) mediumAssuranceHardwareRoaming (3) }

The Trans Sped PCA shall assert these policy OIDs as specified in the certificate profiles found in Section 10.

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

EU Private Cert extension	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD Id-etsi-qcs-QcRetentionPeriod(value=10)

1.3 Trans Sped Certificate and CRL Issuance

Normal Operation

The Trans Sped SAFE PCA will issue two types of certificates:-

- Medium Assurance Hardware (MAH)
  - Used for keys generated on USB Cryptographic tokens
  - Certificate carries the mediumAssuranceHardware OID from Trans Sped (1.3.6.1.4.1.39965.2.1.1) to map to the SHA2 Medium Assurance Hardware OID of SAFE Bridge
  - Certificate carries the EU Qualified Certificate/SSCD (0.4.0.1456.1.1)
- Medium Assurance Hardware Roaming (MAR)
  - Used for keys generated in cloud-based Hardware Security Modules (TACS, Thales NetHSM)
  - Certificate carries the basicAssurance OID from the Trans Sped (1.3.6.1.4.1.39965.2.1.3) to map to the SHA2 Basic Assurance OID of SAFE Bridge
  - Certificate carries the EU Qualified Certificate/SSCD (0.4.0.1456.1.1)
  - This Solution will support the use of a validation service

1.4 PKI Entities

The SAFE-BioPharma PKI is defined as the SBCA and the cross-certified SAFE-BioPharma Issuer PKIs. This CP specifically applies to Certificates issued by Trans Sped's PCA and to the operation of that PCA.

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

The Trans Sped PCA, CSAs, RAs and Trusted Agents supporting this CP are collectively referred to Trans Sped SAFE-BioPharma PKI.

The following roles are relevant to the Trans Sped components participating in the SAFE-BioPharma PKI.

1.4.1 PKI Authorities

1.4.1.1 SAFE-BioPharma Policy Approval Authority (PAA)

The SAFE-BioPharma PAA is a group of individuals chartered by the SAFE-BioPharma Standard and selected by the SAFE-BioPharma Board of Directors. With respect to this CP, the PAA is responsible for confirmation of continued conformance of Trans Sped CA with SAFE-BioPharma requirements as a condition for allowing continued cross certification with the SBCA. For more information on the responsibilities of the SAFE-BioPharma PAA refer to the SAFE-BioPharma CP.

1.4.1.2 SAFE-BioPharma Bridge Certification Authority (SBCA)

The SBCA is the SAFE-BioPharma Bridge PCA operated by the SBCA OA and is authorized by the PAA to create, sign, and issue Public Key Certificates to Trans Sped’s CA and other Principal CAs. For more information on the responsibilities of the SBCA refer to the SAFE-BioPharma CP.

1.4.1.3 Trans Sped Policy Management Authority (PMA)

The PMA is appointed and operates under the authority of the executive management of Trans Sped.

The PMA is chaired by Trans Sped, Operations, Information Security and SAFE-BioPharma Program groups within Trans Sped.

The PMA is responsible for:

- Establishment and maintenance of this CP in accordance with the SAFE-BioPharma Operating Policies
- Establishment and maintenance of this CP in accordance with European Regulations and Standards
- Review and approval of applicable CPSs as being in conformance with this CP and the SAFE-BioPharma Operating Policies
- Ensuring the operation of the PCA and related components comply with the requirements of this CP, applicable CPS and the requirements of the SAFE-BioPharma CP.

1.4.1.4 Trans Sped Operational Authority

The IAM Team is the entity within Verizon that operates and maintains the PCAs under the direction of the PMA.

1.4.1.5 Principal Certification Authority (PCA)

Trans Sped will operate the PCA. Trans Sped is authorized to apply for cross certification with the SBCA and to generate, publish and revoke the SBCA certificate. The PCA shall also be authorized to create, sign, and issue Public Key Certificates. PCA. The Trans Sped PCA is responsible for all aspects of the issuance and management of the certificates it issues including:

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

1.4.1.6 Registration Authority (RA)

The RA for the PCA collects and verifies Subscriber information in accordance with the applicable CPS for issuing certificates.

In the case of end-entity Certificates, the RA operates under an agreement with Trans Sped PCA and collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's certificate. The requirements for RAs are set forth elsewhere in this document.

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

1.4.1.7 Subscribers

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

- SAFE-BioPharma Users of a contracting SAFE-BioPharma Stakeholder requiring a Certificate, including both individuals and Machine Subscribers, for use in accordance with SAFE-BioPharma operating rules.
- PKI operations personnel.
- RA personnel who are required to use a SAFE-BioPharma Certificate to access system components.
- Other categories…

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

1.4.1.8 Relying Parties

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

In order for a Relying Party to be covered by the provisions of SAFE-BioPharma, both the contracting SAFE-BioPharma Stakeholder creating the message, document, or communication and the Relying Party must have a contractual relationship established with SAFE-BioPharma, specifically allowing the Relying Party to rely on Certificates issued by the PCA. Further, the Relying Party must meet requirements prescribed by the SAFE-BioPharma Standard for signature validation.

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

1.4.1.9 Other Participants

The PCA 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).

1.4.1.10 Local Registration Authority (LRA)

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

1.4.1.11 Trusted Agent (TA)

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

1.4.1.12 Certificate Status Authority (CSA)

Server based Certificate Status Authorities (CSAs) such as Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. At a minimum, the Trans Sped PCA shall make its Certificate status information available through an OCSP responder in addition to any other mechanisms it may employ (such as in a CRL).

1.4.1.13 Machine Operator

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

1.4.1.14 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, and with security requirements for a server-side system using certificates in order to create advanced electronic signatures under sole control of a natural person, or a legal person (such advanced electronic signatures produced by legal persons are called electronic seals)

1.5 Certificate Usage

1.5.1 Appropriate Certificate Uses

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

The PCA issues qualified certificates in compliance with applicable local law of the EU member state where the qualified PCA 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 that 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 assurance policies of this CP.

1.5.1.1 Prohibited Certificate Uses

No stipulation.

1.6 Policy Administration

1.6.1 Issuer Administering the Document

The Trans Sped Policy Management Authority (PMA) (see Section 1.3.1.1) is responsible for all aspects of this CP.

1.6.1.1 Contact Person

Questions regarding this CP shall be directed to the Chair of the PMA, who can be contacted at [SAFEpolicy@transsped.ro]

1.6.1.2 Person Determining CPS Suitability for the Policy

The PMA is responsible for approving the applicable CPSs and establishing that the PCAs and the SICAs conform to the requirements of this CP.

2 Publication & Repository Responsibilities

2.1 Repositories

Trans Sped shall operate repositories to support PCA operations. Trans Sped shall ensure interoperability with the SBCA repository so that Relying Parties may obtain PCA Certificates and, if published externally, CRLs from or through that repository. This shall be accomplished using either LDAPv3 queries (including referrals) or by placing the Certificates and CRLs in that repository accessible via SSLv3 for HTTP or through TLSv1. CRLs in a repository shall be accessible via both HTTP and LDAP methods via SSLv3 for HTTP or TLSv1. HTTP only access for CRLs is acceptable if Trans Sped and its associated Stakeholder(s) agree to accept any limitation this may impose on the use of SAFE-BioPharma Certificates for authentication purposes.

2.1.1 Repository Obligations

Trans Sped shall support:

- LDAP Directory Server System that is accessible through the Lightweight Directory Access Protocol (LDAP, version 3), Hypertext Transfer Protocol (HTTP) Secure Sockets protocol (Secure Sockets Layer (SSL) for HTTP, version 3), or Transport Layer Security protocol (TLS, version 1). Only LDAP referrals shall be supported.
- The availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms, when necessary to protect the repository availability and information as described in later sections.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The PCA shall publish in the appropriate repository all PCA certificates and CRLs.

2.2.2 Publication of PCA Information

This CP shall be made available to all SAFE-BioPharma Participants at the following URL:http://www.transsped.ro/repository

Sections of the Trans Sped CPS relevant to use by a Relying Party shall also be made available to all SAFE-BioPharma Participants at the same URL, or upon email request to safepolicy@transsped.ro.

2.2.3 Interoperability

Where Subscriber Certificates, PCA certificates, or CRLs are published in repositories, standards-based schemas for directory objects and attributes shall be employed, specifically, LDAPv3, SSLv3 for HTTP (HTTPS), and TLSv1 protocols. Further requirements are set forth later in this CP.

2.3 Frequency of Publication

This CP and any subsequent changes shall be made available to SAFE-BioPharma Participants as set forth in Section 2.2.2 within one week of approval by the PMA and, if necessary, the SAFE-BioPharma PAA.

PCA and Subscriber Certificates issued by the PCA shall be published upon issuance. CRLs may be published internally to the PKI only, publicly without restrictions on access or dissemination, or on a limited basis with restrictions on access and disseminations within the SAFE-BioPharma community.

2.4 Access Controls on Repositories

Trans Sped shall protect repository information not intended for public dissemination or modification. Certificates and certificate status information in the repository shall be made available through the Internet to SAFE-BioPharma Participants and other parties as determined by the PMA.

3 Identification & Authentication

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

3.1 Naming

3.1.1 Types of Names

The PCA 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 for those certificates issued to the end entities. Details on this may be found in the certificate profiles set forth later in this CP.

3.1.2 Need for Names to be Meaningful

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

DNs shall be used and 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

The PCA shall not issue anonymous certificates.

PCA certificates shall not contain pseudonym identities.

DNs in certificates issued by the PCA may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

The PCA may issue pseudonymous certificates to internal Subscribers to support its operations as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Trans Sped shall enforce name uniqueness and is responsible for ensuring name uniqueness in certificates issued by the Trans Sped SAFE-BioPharma PKI.

Any Subscriber DN in a X.509 certificate issued must uniquely identify a single entity among all of the Subscribers. If necessary, the PCA 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 PCA). In any case, there must not be two X.509 certificates having the same issuer DN and serial number.

3.1.6 Recognition, Authentication, & Role of Trademarks

The PMA shall resolve any name collisions or disputes regarding Trans Sped SAFE-BioPharma issued certificates brought to its attention. Any dispute resolution shall be in accordance with the SAFE-BioPharma Operating Policies.

The PCA shall not be responsible for resolving name claim disputes among Subscribers. The PCA may add, at its own discretion, additional information to a name in order to make it unique among the names of certificates issued by the PCA 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 PCA. This section covers these topics.

3.2.1 Method to Prove Possession of Private Key

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

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

The PCA shall not issue encryption keys to Subscribers.

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

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 PCA or an RA recognized by the PCA shall verify the information, the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Request for cross-certification by the Trans Sped PCA and the SBCA shall be handled as specified in the SAFE-BioPharma CP and SAFE-BioPharma Operating Procedures.

3.2.3 Identity-Proofing of Individual Identity

3.2.3.1 Identity-Proofing of End User Subscribers

For Medium Assurance Hardware and Roaming Levels

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

A Registration Agent (either PCA, RA, LRA or TA) shall record the information set forth below for issuance of each Certificate:

- The identity of the Registration Agent performing the identification;
- A signed declaration by the Registration Agent that he or she verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under local law;
- A unique identifying number(s) from the ID(s) of the Subscriber (or some other trusted source of information on the Subscriber), or a facsimile of the ID(s);
- The date and time of the verification;
- A declaration of identity signed by the Subscriber using a handwritten signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law;
- An end user Subscriber Agreement with Trans Sped, signed by the Subscriber using a handwritten signature or a qualified signature.

For All Assurance Levels

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

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

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

Video Teleconference-based Face to Face Identity Proofing

The following requirements shall be met to support video teleconferencing based face-to-face identity verification:

1. the signal transmission must be secure from interception by persons other than the persons communicating and must be provided using a communications link that complies with current National Institute of Standards cryptographic requirements;
2. the video resolution of the facilities must be sufficient to allow the trusted agent to view and copy the identifying information from the proffered identity document without assistance from the applicant;
3. the persons communicating must simultaneously see and speak with one another;
4. The signal transmission must be live and in real time.

3.2.3.2 Identity-Proofing of Machine Subscribers

No stipulation.

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 affiliation with a Contracting SAFE-BioPharma Stakeholder shall be issued only after ascertaining the applicant has the authorization to act on behalf of the Contracting SAFE-BioPharma Stakeholder in the asserted cap

3.2.5.1 Identity-Proofing for Group Certificates

Trans Sped does not issue Group Certificates.

3.2.5.2 Criteria for Interoperation

The Trans Sped PCA shall interoperate with the SAFE-BioPharma system pursuant to the SAFE-BioPharma Operating Rules and stipulations of the SAFE-BioPharma Issuer Agreement. The PCA shall adhere to the following requirements:

- Have a CP mapped to, and determined by the PMA and PAA to be in conformance with, the SAFE-BioPharma CP;
- Have undergone a successful compliance audit pursuant to Section 8 of this CP and the SAFE-BioPharma CP;
- Issue certificates compliant with the profiles described in this CP, and make certificate status information available in accordance with this CP;
- Either provide a publicly accessible directory that interoperates with the SBCA repository, or make certificates and certificate status information available to other SAFE-BioPharma Participants in accordance with SAFE-BioPharma requirements through other mechanisms
- Make its CRL (or archived CRL) available within the SAFE-BioPharma community as needed either to support resolution of a future SAFE-BioPharma dispute, or to support a future SAFE-BioPharma centralized OCSP functionality.

3.3 Identification and Authentication for Re-key Requests

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

3.3.2 Identification and Authentication for Re-key after Revocation

If a Certificate is revoked, the subject (e.g., PCA, SBCA, CA or Subscriber) shall go through the initial identity-proofing process described in Section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Requests

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

4 Certificate life-cycle

4.1 Application

This section specifies requirements for initial application for certificate issuance by the Trans Sped SAFE-BioPharma CA.
For the purpose of cross-certification with the SBCA, the PCA shall issue certificates to the SBCA.

The PMA must approve requests for any certificate issued by a PCA. The PMA shall review the information provided in the PCA request and determine whether to approve the request.

Once the PMA approves issuance of a CA certificate, the RA and/or the Operational Authority responsible for the CA shall perform the following steps:

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

All communications among PCA, 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 assurance certificates shall be protected using medium 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.

Key generation then shall take place in a secure environment.

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 may be created in software.

4.2 Submission of Certificate Application

The PCA, when seeking to cross-certify with the SBCA shall complete the Issuer application process specified by the PAA**,** include submission of a copy of this CP and the applicable CPS to the PAA for review.

For cross certification with the SBCA, an authorized representative of Trans Sped and the PMA shall submit the application to the PAA.

For Certificates issued by a PCA to the PCA, an application shall be submitted to the PMA pursuant to the policies and procedures described in the applicable CPS.

4.3 Enrollment Process and Responsibilities

The process for enrollment of the PCA with the SBCA is specified in the SAFE-BioPharma CP and SAFE cross certification process.

The PMA shall ensure that all information contained in a PCA's application for cross certification is accurate and shall designate a Principal Point of Contact (POC) who oversees the PCA application to the SBCA.

For Certificates issued by a PCA to the SBCA, an application shall be submitted to the PMA pursuant to the policies and procedures described in Section 3.2. Any Certificate issued by a PCA to the SBCA shall be manually checked by the POC to ensure each field and extension is properly populated with the correct information.

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 the PCA using their Internet browser or other application software. Submitting the application form will automatically deliver the Public Key to the PCA in accordance with section 6.1.3

4.4 Certificate Application Processing

It is the responsibility of the PCA and RA to verify that the information in certificate applications is accurate. Applications for certificates issued by the PCA shall be manually checked to ensure accuracy, completeness and that authorization by the PMA has been established prior to issuance.

4.5 Performing Identity-proofing Functions

Identity proofing for Subscriber Certificates shall follow the provisions of this CP, the SAFE-BioPharma Operating Rules and any requirements stipulated in the policies and procedures that are binding on the RA, LRA and TA as per the agreement with the Contracting SAFE-BioPharma Stakeholder.

4.6 Approval or Rejection of Certificate Applications

The PCA, RA, LRA and TA may accept or reject a Certificate application from the Subscriber.

4.7 Time to Process Certificate Applications

Processing time for Subscriber certificates shall not be longer than 5 working days after receiving all necessary documents requested for issuing the certificate.

4.8 Certificate Issuance

4.8.1 PCA Actions during Certificate Issuance

The PCA 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, the PCA or RA shall, in addition to the above, verify the data contained in the request according to the applicable local legislation on Electronic Signatures.

The PCA 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, the PCA 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.

4.8.2 Notification to Subscriber of Certificate Issuance

The PCA 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 PCA 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.

4.9 Acceptance

4.9.1 Certificate Acceptance

Downloading a certificate or installing a certificate from a message 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.

4.9.2 Publication of the Certificate by the PCA

As specified in Section 2.2, all PCA certificates shall be published in a repository accessible by SAFE-BioPharma Participants and others.

Subscriber certificates shall be published in accordance with the provisions of Section 2.

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

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

4.9.3 Notification of Certificate Issuance by the Principal PCA to Other Entities

No stipulation

4.10 Key Pair and Certificate Usage

4.10.1 Subscriber Private Key and Certificate Usage

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

4.10.2 Relying Party Public Key and Certificate Usage

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

4.11 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 is only permitted for PCA certificates. Renewal of Subscriber certificates shall not be permitted.

4.11.1 Circumstance for Certificate Renewal

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

4.11.2 Who May Request Renewal

The PCA may request renewal of its Certificates through the PMA.

Subscribers may not request renewal but must request re-keying of their Certificates as specified in Section 4.7.

4.11.3 Processing Certificate Renewal Requests

The PCA or 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 3.2.2
- Identification & Authentication for Re-key as described in Section 4.5, except the old key can also be used as the new key.

4.11.4 Notification of New Certificate issuance

See section 4.8.2

4.11.5 Acceptance of a Renewed Certificate

See section 4.9.1

4.11.6 Publication of the Renewal Certificate by the PCA

See Section 4.9.2.

4.11.7 Notification of Certificate Issuance by the PCA to Other Entities

See section 4.9.3

4.12 Certificate Re-Key

Re-keying a certificate consists of creating a new certificate with a different Public Key while retaining other Subject information from the old certificate. The new certificate may be assigned a different validity period and/or signed using a different issuing PCA Private Key.

4.12.1 Circumstance for Certificate Re-key

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

4.12.2 Who May Request Certification of a New Public Key

The PCA may request re-key of its certificate.

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

4.12.3 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 4.3.1

4.12.4 Notification of New Certificate Issuance to Subscriber

See Section 4.8.2.

4.12.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.12.6 Publication of the Re-keyed Certificate by the PCA

See Section 4.9.2.

4.12.7 Notification of Certificate Issuance by the PCA to Other Entities

See section 4.9.3.

4.13 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, LRA or TA shall verify the new updated information in the certificate. For example, if an individual's name changes (e.g., due to marriage), then proof of the name change shall be validated using the initial identity proofing processes as defined in Section 3.2. The RA, LRA or TA shall securely notify the PCA and confirm the validation result prior to the issuance of the certificate.

Trans Sped does not support certificate modification. Certificate modification for a PCA shall be accomplished through re-keying or renewal as specified in section 4.6 and 4.7 respectively.

4.13.1 Circumstance for Certificate Modification

Not applicable.

4.13.2 Who May Request Certificate Modification

Not Applicable.

4.13.3 Processing Certificate Modification Requests

Not Applicable.

4.13.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.13.5 Acceptance of Modified Certificate

Not Applicable.

4.13.6 Publication of the Modified Certificate by the PCA

Not Applicable.

4.13.7 Notification of Certificate Issuance by the PCA to Other Entities

Not Applicable.

4.13.7.1 Revocation

If it is not certain whether the corresponding Private Key has been lost or compromised, the Subscriber must revoke the certificate. 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 PCA 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.

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

4.13.8 Circumstance for Revocation of a Certificate

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

- Identifying information or affiliation components of any names in the Certificate become invalid;
- Subject can be shown to have violated the stipulations of its respective Subscriber, Issuer or Member Agreement, or the stipulations of this CP;
- Private Key is compromised or is suspected of compromise;
- The PAA, PMA, Principal PCA, or SAFE-BioPharma suspects or determines that revocation of a certificate is in the best interest of the integrity of the SAFE-BioPharma PKI;
- Certification of the Subject is no longer in the interest of the Trans Sped PCA or the associated contracting Stakeholder; or
- Subscriber or other authorized agent (as defined in the CPS) asks for his/her Certificate to be revoked. The PCA has learned about false information having been supplied in the certificate application that invalidates the certificate.
- 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 and/or specified as revoked by an OCSP Responder. Revoked Certificates shall be included on all new publications of the certificate status information until the certificates expire. Where CRLs are used, revoked Certificates shall appear on at least one CRL and on at least one archived CRL.

4.13.9 Who Can Request Revocation of a Certificate

Only the Subscriber or an RA can request revocation, except as noted in section 4.13.8. Any entity or third party that confirmed any information contained in a certification should inform the issuing PCA about the fact that this information is not or no longer correct, and request revocation in accordance with section 4.13.8.

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

4.13.10 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 PCA or RA shall authenticate the request as well as the authorization of the requester per Section 4.13.9.

Revocation requests made to a PCA by the SBCA shall be authenticated by the Global Operations Group, which shall confirm the authorization of the requestor as specified in Section 4.9.2.

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

A Subscriber ceasing its relationship with Trans Sped shall be required, prior to departure, to surrender to the RA, LRA or TA (through any accountable mechanism) all

cryptographic hardware tokens that were issued to the Subscriber by Trans Sped. A Subscriber ceasing its employee-employer or other relationship with a contracting SAFE-BioPharma Member that sponsored the subscriber prior to departure shall surrender to a RA, LRA or TA (through any accountable mechanism) all cryptographic hardware tokens that were issued to the Subscriber by the PCA.

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 Subscriber certificates associated with the un-retrieved tokens shall be immediately revoked, expressing reason code “key compromise.”

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 PCA which issued the certificate.

2. If the Private Key has been lost or is inaccessible for any reason, the Subscriber may call the issuing PCA 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 PCA 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).

4.13.11 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.

4.13.12 Time within which PCA must Process the Revocation Request

The PCA shall process a certificate revocation request within eighteen (18) hours of upon receipt of requests.

4.13.13 Revocation Checking Requirements for Relying Parties

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

4.13.14 CRL Issuance Frequency

The PCA shall publish CRLs no less frequently than once every 18 hours.

The PCA shall publish CRLs no less frequently then once every 31 days. If the CRL is issued every 31 days, the PCA shall meet the requirements specified below for issuing Emergency CRLs. The PCA shall also notify the SBCA Operational Authority upon Emergency CRL issuance.

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

4.13.15 Maximum Latency of CRLs

The maximum delay between the time that a certificate is revoked by the PCA and the time that this revocation information is available to SAFE-BioPharma Relying Parties shall be no greater than 24 hours. Certificate status information shall be updated no less frequently than every hour. CRLs shall be published within 4 hours of generation.

4.13.16 Online Revocation Checking Availability

The PCA shall support OCSP.

4.13.17 Online Revocation Checking Requirements

The SAFE-BioPharma standards require the use of OCSP to obtain certificate status information for any certificates in a trust chain when validating digital signatures made pursuant to the SAFE-BioPharma standards. The CSA shall respond to OCSP requests immediately upon receipt. OCSP requests and responses shall comply with the profiles specified later in this CP.

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.

4.13.18 Other Forms of Revocation Advertisements Available

No stipulation.

4.13.19 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.13.20 Special Requirements Related To Key Compromise

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

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 they have been notified by the issuing PCA of the revocation of the certificate.

4.13.21 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. Trans Sped 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.

4.13.22 Who can Request Suspension

See 4.13.9

4.13.23 Procedure for Suspension Request

See 4.13.10

4.13.24 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.

4.14 Certificate Status Services

No stipulation beyond Section 4.13.16.

4.14.1 Operational Characteristics

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

4.14.2 Service Availability

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

4.14.3 Optional Features

No stipulation.

4.15 End of Subscription

Certificates that have expired prior to or upon end of subscription shall not be revoked. Unexpired Subscriber certificate shall be revoked upon the end of the Issuer agreement. A Subscriber certificate shall be revoked upon end of subscription.

4.16 Key Escrow & Recovery

The PCA does not support the issuance of encryption certificates.

4.16.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.16.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility Management & Operations Controls

5.1 Physical Controls

The PCA, CSAs and CCS shall impose the physical security requirements specified in Section 5.1.2.

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

5.1.1 Site Location & Construction

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

5.1.2 Physical Access

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

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

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

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

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

A security check of the facility housing the PCA, CSA or CCS equipment shall occur on a regular basis. The Trans Sped facility shall never be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed"; and for the PCA, that all equipment other than the repository is shut down) when not in use;
- 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 group of persons from the IAM Team shall be made explicitly responsible for making such checks. A log identifying the person performing the check at each instance shall be maintained.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposure

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

5.1.5 Fire Prevention & Protection

The PCA, CSA and CCS equipment shall be housed in a facility with appropriate fire suppression and protection systems.

5.1.6 Media Storage

PCA 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 PCA and shall be protected from unauthorized access.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed using the disposal process. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site backup

Full system backups of PCA, sufficient to recover from system failure, shall be made on a periodic schedule as described in the 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 shall be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational PCA.

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 PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the Trans Sped PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion, and any one individual cannot cause much damage. The following are the trusted roles for the PCA:

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

In addition to the above PCA roles, the Trans Sped SAFE-BioPharma Issuer infrastructure utilizes the following additional roles:

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

The Trans Sped SAFE-BioPharma Issuer infrastructure may also utilize the following roles depending upon the particular agreement with the Contracting SAFE-BioPharma Member.

- *CCS Administrator* – authorized to configure and operate the CCS. This is a Machine Operator role per the SAFE- BioPharma Functional Specification.

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

The following sections contain a detailed description of these roles.

5.2.1.1 PCA Administrator

The PCA Administrator role is responsible for:

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

PCA Administrators are not permitted to issue certificates.

5.2.1.2 PCA Agent

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

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

5.2.1.3 PCA Auditor

The PCA Auditor role is responsible for:

- Reviewing, maintaining, and archiving PCA audit logs; and

- Performing or overseeing internal compliance audits to ensure that the PCA is operating in accordance with its CPS.

5.2.1.4 PCA Operator

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

5.2.1.5 CSA Administrator

The CSA Administrator role is responsible for:

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

5.2.1.6 CSA Auditor

The CSA Auditor role is responsible for:

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

5.2.1.7 CCS Administrator

The CCS Administrator role is responsible for:

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

5.2.1.8 CCS Auditor

The CCS Auditor role is responsible for:

- Reviewing, maintaining, and archiving CCS audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CCS is

operating in accordance with its CPS.

5.2.1.9 Registration Authority (RA)

The RA responsibilities are:

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

5.2.1.10 Local Registration Authority (LRA)

The LRA responsibilities are:

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

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

5.2.1.11 Trusted Agent (TA)

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

5.2.1.12 Machine Operator

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

Machine Operators are not applicable to any PCA 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

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

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in

Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

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

5.2.3 Identity-proofing for Each Role

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

5.2.4 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the PCA, CSA or CCS system, or procedurally, or by both means.

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

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

No individual shall be assigned more than one identity.

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

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

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

5.3.2 Background Check Procedures

Background check procedures shall be described in the CPS and demonstrate that requirements set forth in Section 5.3.1 are met.

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

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

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

The extent to which these investigations are performed is restricted by the applicable local legislation. Trans Sped 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.

Personnel in positions of trust shall provide a notification of any changes in their place of residence.

5.3.3 Training Requirements

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

- PCA/RA security principles and mechanisms
- Use and operation of the all PKI and associated equipment
- All PKI software versions in use on the PCA system
- All PKI duties an individual is expected to perform
- Disaster recovery and business continuity procedures.

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

5.3.4 Retraining Frequency & Requirements

Individuals responsible for PKI roles shall be made aware of changes in the PCA 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 PCA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The PMA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP or CPS) involving the PCA, its repository, CSA and CCS.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the PCA, CSA, and CCS shall be subject to the requirements of Section 5.3.

5.3.8 Documentation Supplied To Personnel

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

5.4 Audit

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

5.4.1 Types of Events Recorded

All security auditing capabilities of the PCA, CSA, CCS RA, LRA operating system and application Components required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. An “X” in a table cell indicates that the respective Component (PCA, CSA, 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	PCA	CSA	CCS	RA	LRA

Auditable Event	PCA	CSA	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	X	X	X	X	X
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	X	X
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 PCA for key recovery purposes	X	-	-	-	-
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE					

Auditable Event	PCA	CSA	CCS	RA	LRA
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	X	X	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	-	-	X	X
CERTIFICATE REVOCATION					
All certificate revocation requests	X	-	-	X	X
CERTIFICATE STATUS CHANGE APPROVAL					
The approval or rejection of a certificate status change request	X	-	-	-	-
PCA 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	-	-	-	-
The access control privileges of a user account or a role are modified	X	-	-	-	-
CERTIFICATE PROFILE MANAGEMENT					
All changes to the certificate profile	X	-	-	-	-
REVOCATION PROFILE MANAGEMENT					
All changes to the revocation profile	X	-	-	-	-
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT					
All changes to the certificate revocation list profile	X	-	-	-	-
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

Auditable Event	PCA	CSA	CCS	RA	LRA
Installation of the PKI Application	X	X	X	X	X
Installation of hardware cryptographic modules	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X
System Startup	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X
Back up of the internal PCA database	X	-	-	-	-
Restoration from back up of the internal PCA database	X	-	-	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-	-	-
Posting of any material to a repository	X	-	-	-	-
Access to the internal PCA database	X	X	-	-	-
All certificate compromise notification requests	X	-	-	X	X
Loading tokens with certificates	X	-	X	X	X
Shipment of Tokens	X	-	-	X	X
Zeroizing Tokens	X	-	-	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	-	-
Access to the Component	X	X	X	-	-
Known or suspected violations of physical security	X	X	X	X	X

Auditable Event	PCA	CSA	CCS	RA	LRA
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	-	-	-	-
Electrical power outages	X	-	-	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-	-	-
Obvious and significant network service or access failures	X	-	-	-	-
Violations of Certificate Policy	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X

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

5.4.2 Frequency of Processing Data

Audit logs from the PCA, CSA, CCS, RA, and LRA shall be reviewed at least once every two months. At a minimum, a statistically significant (approximately 5%) 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 shall be 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 PCA's audit logs shall be reviewed prior to shutdown and upon startup of the PCA, with 100% review of the of security audit data generated by the PCA components since that last review.

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.

Protection of Security Audit Data

Component system configuration and operating procedures shall ensure that:

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

Procedures shall be implemented to protect archived data from destruction prior to the end of the audit log retention period. Audit logs shall be moved to a safe, secure storage location separate from the component equipment.

5.4.4 Security Audit Data Backup Procedures

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

5.4.5 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 PMA shall be notified, and a determination shall be made by the head of Operations whether to suspend the Component operation until the problem is remedied.

5.4.6 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.

5.4.7 Vulnerability Assessments

The Auditor or other party who is independent from PCA operations shall perform vulnerability self-assessments of security controls.

5.5 Archive

5.5.1 Types of Events Archived

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

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	PCA	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	-	-	-	-
Revocation requests	X	-	-	-	-
Subscriber identity authentication data as per Section 3.2.3	X	-	-	X	X
Documentation of receipt and acceptance of certificates	X	-	-	X	X
Documentation of receipt of Tokens	X	-	-	X	X
All certificates issued or published	X	-	-	-	-
Record of Component PCA Re-key	X	X	X	X	X
All CRLs and CRLs issued and/or published	X	-	-	-	-
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 Trans Sped and relevant Contracting SAFE-BioPharma Members, and as specified by the PAA. This period shall be no less than 10 years and 6 months.

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

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

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

Trans Sped does not retain archive data beyond the stated archive period but shall notify the PAA who, at its election, may take responsibility for the archived data.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to add to the archive. The archived records may be moved to another medium when authorized by the Audit Administrator. The contents of the archive shall not be released except as determined by the PAA, the PMA, or as required by law. Records and material information relevant to use of, and

reliance on, a SAFE-BioPharma certificate shall be archived. Archived information of individual SAFE-BioPharma Transactions shall be made available upon request to any Subscribers involved in the transaction or their legally recognized agents. Such information shall be available beyond the end of the validity period of the associated SAFE-BioPharma Subscriber's certificate, up to the retention period indicated in Section 5.5.2. Archive media shall be stored in a safe, secure storage facility separate from the component itself.

5.5.4 Archive Backup Procedures

The applicable CPS shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

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

5.6 Key Changeover

To minimize risk from compromise of the PCA'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 shall 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 may the old key be retained. If the old key is retained, it shall be protected just as the new key.

The PCA shall use the following maximum key usage periods.

Key Size	Private Key Usage Period	Certificate Validity Period
2048 bit RSA	PCA Certificate Validity Period	15 Years
2048 bit RSA	Subscriber Certificate Validity Period	1 Year (for Medium Assurance Hardware/EU certificates[1])

[1] This is a EU requirement – Medium Assurance Hardware/EU Qualified certificates shall only have a validity period of one year.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If Trans Sped detects a potential PCA hacking attempt or other form of compromise to the PCA, it shall perform an investigation in order to determine the nature and the degree of damage.

If the PCA key is suspected of compromise, the procedures outlined in Section 5.7.2 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the PCA needs to be rebuilt, only some certificates need to be revoked, and/or the PCA key needs to be declared compromised.

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

Computing Resources, Software, and/or Data Are Corrupted

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

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

- Before returning to operation, ensure that the system's integrity has been restored.
- If the PCA signature keys are not destroyed**,** PCA 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 PCA signature keys are destroyed**,** PCA operation shall be reestablished as quickly as possible, giving priority to the generation of a new PCA key pair.

5.7.2 PCA Private Key Compromise Recovery Procedures

Where the PCA key is compromised, the trusted self-signed certificate shall be removed from each subscriber, and a new one distributed via secure out-of-band mechanisms. The PCA shall describe its approach to reacting to the key compromise in its CPS. Secure techniques to distribute the new trust anchor shall be described in the applicable CPS.

The PMA shall also investigate and report to the PAA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.3 Business Continuity Capabilities after a Disaster

The PMA shall promptly and securely advise the PAA in the event of a disaster where the PCA installation is physically damaged and all copies of the PCA Signing Keys are destroyed.

If PCA equipment is damaged or rendered inoperative, but the PCA Signing Keys are not destroyed**,** the PCA 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 PCA is not available for any reason, the PMA shall be promptly and securely notified, and then the PAA shall be securely and promptly notified in a fashion set forth in the respective Agreements. This will allow Issuers and those contracted with the Issuers to protect their interests as Relying Parties. The PAA shall also determine whether to revoke the Issuer's PCA Certificate.

If an OCSP Responder associated with a PCA is not available for any reason the PCA shall securely and promptly notify the PMA, provide notification of the subscribers, and may at the direction of the PMA, not issue a new OCSP Responder certificate or revoke the PCA certificate.

In the event that the PMA or its operational authorities or representatives' determine that an OCSP Responder in another SAFE-BioPharma related domain is not available the SAFE-BioPharma related domain as well as the PAA shall be securely and promptly notified in a fashion set forth in the respective agreements.

In the case of a disaster whereby a PCA installation is physically damaged and all copies of the PCA Signing Key are destroyed as a result, the PCA shall request that its certificates be revoked, and shall apprise the SBCA OA and PAA of actions they intend to take to reestablish the PCA and request a new cross-certificate from the SBCA, and will follow whatever processes have been set forth in the respective Agreement for that purpose.

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

The Trans Sped directories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. The PCA shall implement features to provide high levels of directory reliability (99.9% availability or better).

5.8 PCA & RA Termination

5.8.1 PCA Termination

If a PCA terminates operation for convenience, contract expiration, re-organization, or other non-security related reason, the Agreement between Trans Sped and the contracting SAFE-BioPharma Member shall set forth what actions shall be taken to ensure continued support for certificates previously issued by the Trans Sped PKI that are needed for use within SAFE-BioPharma. At a minimum, such actions shall include preservation of the appropriate PCA information archive described in this CP and the respective CPS.

5.9 RA Termination

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

6 Technical Security Controls

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

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

Cryptographic keying material for basic assurance CAs (PCA and Issuer PCA) and associated CSA signing keys shall be generated in FIPS 140-2 Level 2 (or higher) validated or CWA 14167-2 EAL 4+ [EAL 4 Augmented ADV_IMP.2, AVA_CCA.1, and AVA_VLA.4] (or higher) certified hardware cryptographic modules.

Cryptographic keying material for all medium software and medium hardware assurance CAs (PCA, and Issuer PCA) and associated CSA signing keys shall be generated in FIPS 140-1/2 Level 3 (or higher) validated or CWA 14167-2 EAL 4+ [EAL 4 Augmented ADV_IMP.2, AVA_CCA.1, and AVA_VLA.4] (or higher) certified hardware cryptographic modules.

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

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

Cryptographic keying material for End Entities for medium hardware assurance shall be generated in FIPS 140-2 Level 2 (or higher) validated hardware Secure Signature Creation Devices (SSCDs) approved by the local Signature Law of the issuing PCA for the purpose of qualified signatures. These devices shall be under the control of the Subscriber.

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

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

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, the module shall be delivered to the Subscriber by Trans Sped. Trans Sped 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. 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.

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

The PCA shall generate their key pairs in hardware.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber Public Keys must be delivered for certificate issuance in a way that binds the Subscriber'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.

The PCA shall ensure that Public Keys for the PCA and the SBCA are bound to the appropriate operational authorities. The strength of the binding shall be commensurate with the handling of PCA key material.

The Method shall be a manual process as defined in the CPS with in person verifications of the Authorized Agent of the SBCA and visual inspection and recording of any authorization letter from the requesting entity.

6.1.4 PCA Public Key Delivery to Relying Parties

PCA self-signed certificates are the trust anchors for the Trans Sped SAFE-BioPharma Issuer PKI. The PCA shall ensure that its Subscribers receive and maintain its trust anchors in a trustworthy fashion. Methods for trust anchor delivery may include:

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

6.1.5 Key Sizes

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

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

All certificates issued shall use at least 2048 bit RSA, with SHA-256 in accordance with FIPS 186-2 or equivalent.

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

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

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 primarily testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the PAA.

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, but not both, except as specified below. This restriction is not intended to prohibit use of protocols (like the TLS or SSL) that provide authenticated connections using key encryption certificates.

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.

PCA certificates shall 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 standards for cryptographic modules are:

- FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*
- CWA 14167-2, *Cryptographic Module for CSP Signing Operations — Protection Profile (MCSO-PP)*
- CWA 14169, *Secure Signature-Creation Devices "EAL 4+" [Protection Profile — Secure Signature-Creation Device, Type 3]*

The PMA may determine that other comparable qualification, certification, or verification standards are sufficient. Cryptographic modules shall be certified to the levels identified in this section, or certified or qualified to requirements published by the SAFE-BioPharma PAA. The table below summarizes the minimum requirements for cryptographic modules based on FIPS 140; higher levels may be used.

Latest version of FIPS 140	PCA	CSA	CCS	RA	LRA	Subscriber

series						
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)

The following table summarizes the minimum requirements for cryptographic modules based on CWA 14167-2 and CWA 14169; higher levels may be used.

Latest version of CWA Standard	PCA	CSA	CCS	RA	LRA	Subscriber
14167-2 Required	EAL 4+ (Hardware)	EAL 4+ (Hardware)				
14169 Required			EAL 4+ (Hardware)	EAL 4+ (Hardware)	EAL 4+ (Hardware)	EAL 4+ (Hardware)

The CAs may utilize cryptographic modules that satisfy either or both of the applicable FIPS and CWA standards. When following the CWA 14169 standard, the private key associated with the public key in a SAFE-BioPharma Subscriber's certificate shall be protected according to Annex III of the EU Directive 1999/93/EC.

6.2.2 PCA Private Key Multi-Person Control

Use of the PCA private signing key shall require action by multiple persons.

6.2.3 Private Key Escrow

Under no circumstances shall the PCA support a third party escrow of any Signing Keys used to support non-repudiation services.

6.2.4 Private Key Backup

6.2.4.1 Backup of PCA Signing Private Key

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

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

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

6.2.4.2 Backup of Subscriber Signing Private Keys

RA and LRA signing Private Keys shall not be backed up.

Subscriber medium hardware assurance Private Keys shall not be backed up.

6.2.5 Private Key Archival

Signing Private Keys shall not be escrowed or archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

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

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

6.2.7 Private Key Storage on Cryptographic Module

The hardware cryptographic module may store Private Keys in any form as long as the keys are not accessible without a FIPS 140-2 Level 2, CWA 14167-2, and/or CWA 14169 certified authentication mechanism.

When following the CWA 14169 standard, the private key associated with the public key in a SAFE-BioPharma Subscriber's certificate shall be protected according to Annex III of the EU Directive 1999/93/EC.

6.2.8 Method of Activating Private Keys

The Private Key user (e.g. PCA, 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 shall be protected from disclosure (i.e., the data shall not be displayed while it is entered).

The PCA Keys shall only be activated under multi-person control as specified in the CPS.

6.2.9 Methods of Deactivating Private Keys

If cryptographic modules are used to store Subscriber Private Keys, the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity.

Hardware cryptographic modules shall be removed and stored in a secure container or environment when not in use.

6.2.10 Method of Destroying Private Keys

Signing Private Keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. This may be achieved by executing a "zeroize" command. Physical destruction of module is not required.

PCA, CSA, and RA private keys shall be destroyed by individuals in trusted roles.

6.2.11 Cryptographic Module Rating

See table in Section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archive

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

6.3.2 Certificate Operational Periods and Key Usage Periods

See table in Section 5.6 for PCA.

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

Key Size	CSA Private Key	CSA Certificate	Internal Trans Sped RA Certificates and Public Keys	RA, LRA and Subscriber Certificates and Public Keys
2048 bit RSA	Up to 3 years	3 Years	1 Year	1 Year (for Medium Assurance Hardware/EU certificates[2]) 1 Year (for Basic Assurance and Medium Assurance Software certificates).

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

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.

[2] This is a EU requirement - Certificates shall only have a validity period of one year.

Activation data may be user selected. Activation data shall meet the requirements of FIPS 140-2, CWA 14167-2, and/or CWA 14169 as appropriate. 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.

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

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

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

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

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

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

- The PCA shall use software, whether commercial off-the-shelf or custom-built, that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software that is developed specifically for the PCA, CCS or CSA shall be developed in a controlled environment and the development process shall be defined and documented. The PKI owner shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment. This requirement does not apply to off-the-shelf hardware or software.
- All hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The PKI platform (server hardware, operating system software, and PKI application software) shall be dedicated to performing PKI functions. There shall be no non-PKI applications installed on the PKI platform. Connected or associated hardware devices, network connections, or component software that are not part of the PKI platform are exempt from this requirement.

- Proper care shall be taken to prevent malicious software from being loaded. Applications required to perform the PKI operation shall be obtained from sources authorized by local policy.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

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

6.6.2 Security Management Controls

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

The PCA is maintained in an off-line state and software integrity is established each time the system is started. CA software integrity shall be verified at least weekly.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

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

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

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

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

6.8 Time Stamping

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

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

The CPS shall describe how Trans Sped implements this requirement for the PCA.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

The Trans Sped PCA's 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.

Any optional or additional extensions permitted by RFC 3280 shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP. SAFE-BioPharma conforming certificates shall 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:

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}

SHA 256 will be required in accordance with the "SAFE-BioPharma Certificate, CRL and OCSP Profile Guidance" document.

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC3280. Subject and issuer fields for the Trans Sped PCA and subordinate CAs (e.g., SICA) shall include attributes as detailed in the table below.

Trans Sped PCA Name Form

ATTRIBUTE	CONTENT
CN	Descriptive name for PCA, e.g., "PCA CN = Trans Sped SAFE PCA III
OU	OU = Individual Subscriber PCA
O	Trans Sped SRL
C	RO

The Trans Sped subject name form for non-PCA entities shall include attributes as detailed in the table below.

Subject Name Form (Non-CAs)

USAGE	CONTENT
CN	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
OU	As above
O	As above
C	As above

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

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

- Trans Sped registered RDN attribute values of Issuer fields for any certificate can be found in the Certificate Profiles set forth in Section 10.
- Trans Sped registered RDN attribute values for the Subject field of PCA certificates can be found in the Certificate Profiles set forth in Section 10.
- Trans Sped registered RDN attribute values in the Subject field of Subscriber certificates can be found in the Certificate Profiles set forth in Section 10.

The Organizational Unit (OU) attribute is optional in the above name forms, however, Subscriber certificates issued at the behest of SAFE-BioPharma (e.g., to independent investigators), must include an OU attribute populated with a unique identifier for the

Subject. This unique identifier must associate to a specific Subscriber and must not change when issuing a new certificate to that Subscriber.

7.1.5 Name Constraints

The PCA shall assert critical name constraints in certificates issued to the SBCA appropriate for the PKI. The PCA may request the assertion of name constraints in certificates issued by the SBCA to the PCA beyond those specified in the Certificate Formats in Section 10.

A PCA shall assert critical name constraints in. The name constraint shall be based on the SAFE-BioPharma Members serviced by the CA. If name constraints cannot be asserted, a rationale shall be provided and approved by SAFE-BioPharma PAA. An example of the rationale is excessive number of disjoint name spaces.

When the PCA serves more than one SAFE-BioPharma Member, technical means shall be used to constrain the RA and LRA representing the name spaces for which they can submit, approve, and request revocation of certificates.

The PCA may obscure a Subscriber Subject name to meet local privacy regulations so long as such name is unique, meets the requirements set forth in Section 3.1.3 of this CP, and is traceable to a corresponding un-obscured name.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

The Trans Sped PCA shall 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

The Trans Sped PCA 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 OCSP request and/or responses shall be v1.

7.3.2 OCSP Extensions

Responses shall support the nonce extension.

8 Compliance Audit & Other Assessments

The PCA shall utilize a compliance audit mechanism as specified in the CPS to ensure that the requirements of the CP/CPS and the provisions of its Agreements with SAFE-BioPharma Members are being implemented and enforced.

8.1 Frequency Of Audit Or Assessments

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

The PMA has the right to require periodic and aperiodic compliance audits or inspections of the PCA, CSA, CCS or RA operations to validate that the components are operating in accordance with the security practices and procedures described in the applicable CPS.

The PAA has the right to require aperiodic compliance audits of a PCA that is cross-certified with the SBCA. The PAA shall state the reason for any aperiodic compliance audit and shall bear the cost of the audit unless otherwise specified in the respective Issuer Agreement.

8.2 Identity & Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm, which is independent from the component being audited, or it shall be sufficiently organizationally separated from that component to provide an unbiased, independent evaluation.

To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's PCA Facility or CPS.

The PMA 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 the Trans Sped PKI components comply with the requirements of this CP and the applicable CPS as well as the SAFE-BioPharma Standard. Thus all applicable aspects of the SAFE-BioPharma CP, this CP, the applicable CPS and the SAFE-BioPharma Standard shall be covered by a compliance audit.

8.5 Actions Taken As A Result Of Deficiency

The PMA may determine that a Trans Sped PCA is not complying with its obligations set forth in this CP.

- When such a determination is made the PMA shall notify the Trans Sped PCA of the discrepancy.
- The IAM Team shall determine the nature of the discrepancy and direct the party responsible for the component to take corrective actions, documenting the discrepancy and corrective actions taken in an incident report.
- The PMA will review the incident report to determine if further actions and/or notifications are required. If the discrepancy involves the PCA the PMA shall also notify the SAFE-BioPharma PAA promptly

When such a determination is made, the PMA shall notify the PAA who may direct the SBCA to cease interoperating with the applicable PCA (e.g., by revoking the PCA certificate), 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 the SAFE-BioPharma CP, this CP, the applicable CPS, or the SAFE-BioPharma Standard, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the PMA who will notify the Trans Sped PCA responsible for the component of the discrepancy.
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP, the applicable CPS and the Issuer Agreement, and then proceed to make such notifications and take such actions without delay.

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

8.6 Communication Of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Component, shall be provided by the Trans Sped Information Security Group to the PMA and PAA. 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

Trans Sped PCA certificate issuance and renewal fees shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.1.2 Certificate Access Fees

Trans Sped PCA certificate access fees shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.1.3 Revocation or Status Information Access Fee

Trans Sped PCA certificate revocation or status information access fees shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.1.4 Fees for Other Services

Trans Sped PCA services shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.1.5 Refund Policy

Any refunds from the Trans Sped PCA shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.2 Financial Responsibility

Financial responsibility for the Trans Sped PCA shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.2.1 Insurance Coverage

Insurance coverage for the Trans Sped PCA shall be in accordance with the respective Agreement between the contracting SAFE-BioPharma Member and Trans Sped.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

Insurance and/or warranty coverage for end-entities shall be in accordance with the Romanian Law on electronic signature.

9.3 Confidentiality of Business Information

Information pertaining to the PCA and not requiring protection may be made publicly available at the discretion of the PMA. Specific confidentiality requirements for business

information are defined in the Trans Sped's Operating Policies, the SAFE-BioPharma Standard, and associated Member and Issuer agreements.

9.3.1 Scope of Confidential Information

Confidential information concerning the PCA shall include any information provided by a contracting SAFE-BioPharma Member to Trans Sped for purposes of obtaining SAFE-BioPharma compliant certificates.

9.3.2 Information not within the Scope of Confidential Information

Such information as specified by the PAA, PMA and by the SAFE-BioPharma Operating Policies and Issuer Agreements.

9.3.3 Responsibility to Protect Confidential Information

All Trans Sped PKI components shall be responsible for protecting the confidential information it possesses in accordance with the SAFE-BioPharma Operating Policies and applicable contracting SAFE-BioPharma Member requirements.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information treated as Private

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

9.4.3 Information not deemed Private

Shall include any information not specifically identified under Section 9.4.2.

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with SAFE-BioPharma Operating Policies and applicable contracting SAFE-BioPharma Member requirements.

9.4.7 Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with SAFE-BioPharma Operating Policies and applicable contracting SAFE-BioPharma Member requirements.

9.5 Intellectual Property Rights

The PMA retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 Representations & Warranties

9.6.1 PCA Representations and Warranties

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

Acting in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

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

LRAs and TAs shall be bound to the RA obligations.

9.6.3 Subscriber Representations and Warranties

Subscribers shall represent and warrant that they:

- Accurately represent themselves in all communications with the PKI;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- Notify, in a timely manner, the PCA, 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 CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- Use certificates in accordance with the CP, the CPS and, when used to make or verify digital signatures on SAFE-BioPharma documents or transactions, the SAFE-BioPharma requirements governing such use.

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

9.6.4 Relying Parties Representations and Warranties

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

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

9.6.5 Representations and Warranties of other Participants

9.6.5.1 Repository Representations and Warranties

See Section 2.1.1.

9.6.5.2 CSA Obligations

The CSA function for the PCA represents and warrants that it shall conform to the stipulations of this CP, including:

- Providing specific terms governing the CSA in the CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;

- Ensuring that certificate and revocation information is accepted only from valid CAs; and
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the certificate status.

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

9.6.5.3 CCS Obligations

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

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

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

9.7 Disclaimers Of Warranties

Any disclaimer of warranties as shall be specified in the SAFE-BioPharma Operating Policies and the applicable contracting SAFE-BioPharma Member and Issuer Agreements.

9.8 Limitations of Liability

Any such limitations are specified in the SAFE-BioPharma Operating Policies and the applicable contracting SAFE-BioPharma Member and Issuer Agreements. In conformance with EU Directive 1999/93/EC, the SAFE-BioPharma Operating Policies, Section 5.7.3, specify liability limits on individual SAFE-BioPharma signed transactions.

9.9 Indemnities

Indemnification provisions are specified in the SAFE-BioPharma Operating Policies and the applicable contracting SAFE-BioPharma Member and Issuer Agreements.

9.10 Term & Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices & Communications

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

This CP and any subsequent changes shall be made available to SAFE-BioPharma Participants within one week of approval.

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

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute Resolution Provisions

The use of certificates issued for SAFE-BioPharma purposes, 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.

9.14 Governing Law

As specified in the SAFE-BioPharma Operating Policies and the applicable contracting SAFE-BioPharma Member and Trans Sped Agreements.

9.15 Compliance with Applicable Law

As specified in the SAFE-BioPharma Operating Policies and the applicable contracting SAFE-BioPharma Member and Trans Sped Agreements.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

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

9.16.5 Force Majeure

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

9.17 Other Provisions

9.17.1 Fiduciary relationships

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

9.17.2 Administrative processes

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

10 Certificate, CRL, and OCSP Formats

This section contains the formats for the various PKI objects such as certificates, CRLs, and OCSP requests and responses.

All key identifiers shall be encoded in accordance with RFC 3280 Section 4.2.1.2, method 1.

10.1 Trans Sped PCA

The PCA uses the following profile

Field	Content
x.509 Fields	
Version	V3
Serial Number	Allocated automatically
Directory String Type Preference	UTF8
Subject Distinguished Name	CN = Trans Sped SAFE PCA III OU = Individual Subscriber PCA O = Trans Sped SRL C = RO
Issuer Distinguished Name	CN = Trans Sped SAFE PCA III OU = Individual Subscriber PCA O = Trans Sped SRL C = RO
Validity	15 years
Key Algorithm	RSA
Key Length	2048 bit
Signing Algorithm	SHA-256 with RSA
x.509 Extensions	
Key Usage	Critical
Digital Signature	Selected
Non-Repudiation	Selected
Key Encipherment	Not Selected
Data Encipherment	Not Selected
Key Agreement	Not Selected
Certificate Signing	Selected
CRL Signing	Selected
Encipher only	Not Selected
Decipher only	Not Selected
Basic Constraints	Critical
Subject Type	PCA
PathLength	1
Issuer/Serial Number	Not present

Field	Content
Subject Key ID	Not Critical
Key ID	Yes, 160 Bit SHA-1
Certificate Policy extension	Yes - Not Critical
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.1
Policy URL	http://www.transsped.ro/repository
Policy Notice	NA
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.3
Policy URL	http://www.transsped.ro/repository
Policy Notice	NA
Policy Identifier OID	0.4.0.1456.1.1
Policy URL	NA
Policy Notice	NA
Additional Extensions	None

CRL issuing parameters are:

Customer Root PCA	Value
CRL Issuance Period	6 hours
CRL Grace Period (seconds)	43200 (12 hours - more supportable, hosting standard)
Automatically generate a new CRL when certificates are revoked (5.2) or Generate CRL based on revocation reason (5.3)	**Unchecked**
Include Authority Key ID extension in CRL	**Checked (Required by SAFE CP, currently used in** http://www.trustcenter.de/crl/v2/trans_sped_safe_PCA_II.crl**)**
Issuing Distribution Point Extension (when required - inserted in a "CDP" CRL but not in full CRL) is critical	**Unchecked**
Remove Issuing Distribution Point from CRL (5.3 only)	**Checked**
Include Revocation Reason Extension when the reason is Unspecified	**Unchecked**
Include Hold Instruction Code in CRL entries	**Checked**

CRLs will therefore have the following fields:

Field	Content
x.509 Fields	
Version	V2
CRL Number	Allocated automatically

Field	Content
Issuer Distinguished Name	As in the PCA's own certificate
This Update	Allocated automatically
Next Update	Allocated automatically – 18 hours later than this Update
Signing Algorithm	SHA-256 with RSA encryption (1.2.840.113549.1.1.11)
x.509 Extensions	
Authority Key ID	As in the PCA's own certificate
Revoked Certificate List Entries:	
Certificate Serial Number	
Revocation date	
Revocation Reason Code	

10.2 The certificate profile for Medium Assurance Hardware (MAH)

Field	Content
x.509 Fields	
Version	V3
Serial Number	Allocated automatically
Directory String Type Preference	UTF8
Subject Distinguished Name	CN = <First name + Last name> OU = <Organizational Unit> **optional** OU = <Organizational Unit for User ID>**optional** O = <Organization> **optional** C = <Country Code>
Issuer Distinguished Name	CN = Trans Sped SAFE PCA III OU = Individual Subscriber PCA O = Trans Sped SRL C = RO
Validity	12 months
Key Algorithm	RSA
Key Length	2048
Signing Algorithm	SHA-256 with RSA
x.509 Extensions	
Key Usage	Critical
Digital Signature	Selected
Non-Repudiation	Selected
Key Encipherment	Not Selected
Data Encipherment	Not Selected
Key Agreement	Not Selected
Certificate Signing	Not Selected
CRL Signing	Not Selected
Encipher only	Not Selected
Decipher only	Not Selected
Extended Key Usage	Yes, Not Critical
Client Authentication	Selected
Secure Email	Selected
Authority Key ID	Yes - Not Critical
Key ID	Key ID of issuer of certificate
Subject Key ID	Yes - Not Critical
Key ID	Yes, 160 Bit SHA-1
Certificate Policy extension	Yes - Not Critical

Field	Content
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.1
Policy URL	http://www.transsped.ro/repository -
Policy Notice	NA
Policy Identifier OID	0.4.0.1456.1.1
Policy URL	NA
Policy Notice	NA
CRL Distribution Point	http://cdp3.com-strong-id.net/CDP/TS-SAFE-PCA-III.crl
Authority Information Access	Yes – not critical
Access Method :CAIsuuers	http://aia3.com-strong-id.net/PCA/TS-SAFE-PCA-III.p7c
Access Method: Location:OCSP	http://ocs3.com-strong-id.net/TS-SAFE-PCA-III
Qualified Certificate Statements	Yes, Not Critical
ETSI	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod(value=10)
SubjectAltNames	Yes, rfc822-Name = (Email Address)

10.3 The certificate profile for Medium Assurance Hardware Roaming (MAR)

Field	Content
x.509 Fields	
Version	V3
Serial Number	Allocated automatically
Directory String Type Preference	UTF8
Subject Distinguished Name	CN = <First name + Last name> OU = <Organizational Unit> **optional** OU = <Organizational Unit for User ID>**optional** O = <Organization> **optional** C = <Country Code>
Issuer Distinguished Name	CN = Trans Sped SAFE PCA III OU = Individual Subscriber PCA O = Trans Sped SRL C = RO
Validity	12 months
Key Algorithm	RSA
Key Length	2048
Signing Algorithm	SHA-256 with RSA
x.509 Extensions	
Key Usage	Critical
Digital Signature	Selected
Non-Repudiation	Selected
Key Encipherment	Not Selected
Data Encipherment	Not Selected
Key Agreement	Not Selected
Certificate Signing	Not Selected
CRL Signing	Not Selected
Encipher only	Not Selected
Decipher only	Not Selected
Extended Key Usage	Yes, Not Critical
Client Authentication	Selected
Secure Email	Selected
Authority Key ID	Yes - Not Critical
Key ID	Key ID of issuer of certificate
Subject Key ID	Yes - Not Critical
Key ID	Yes, 160 Bit SHA-1
Certificate Policy extension	Yes - Not Critical
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.3
Policy URL	http://www.transsped.ro/repository
Policy Notice	NA

Field	Content
Policy Identifier OID	0.4.0.1456.1.1
Policy URL	NA
Policy Notice	NA
CRL Distribution Point	http://cdp3.com-strong-id.net/CDP/TS-SAFE-PCA-III.crl
Authority Information Access	Yes – not critical
Access Method :CAIsuuers	URL = http://aia3.com-strong-id.net/PCA/TS-SAFE-PCA-III.p7c
Access Method: Location:OCSP	http://ocs3.com-strong-id.net/TS-SAFE-PCA-III
Qualified Certificate Statements	Yes, Not Critical
ETSI	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod(value=10)

10.4 Subscriber Encryption Certificates

Currently not supported

10.5 Machine Certificates

Currently not supported

10.6 OCSP Responder Certificates

Trans Sped PCA Signed SAFE-BioPharma OCSP Responder Certificate

Field	Content
x.509 Fields	
Version	V3
Serial Number	Allocated automatically
Subject Distinguished Name	As defined by Verizon for shared OCSP responder
Issuer Distinguished Name	CN = Trans Sped SAFE PCA III OU = Individual Subscriber PCA O = Trans Sped SRL C = RO
Validity	1 month (no longer than one month from the date of issue)
Key Algorithm	RSA
Key Length	2048
Signing Algorithm	SHA-256 with RSA
x.509 Extensions	
Key Usage	Critical
Digital Signature	Selected

Field	Content
Non-Repudiation	Selected
Key Encipherment	Not Selected
Data Encipherment	Not Selected
Key Agreement	Not Selected
Certificate Signing	Not Selected
CRL Signing	Not Selected
Encipher only	Not Selected
Decipher only	Not Selected
Authority Key ID	Yes - Not Critical
Key ID	Key ID of issuer of certificate
Subject Key ID	Yes - Not Critical
Key ID	Yes, 160 Bit SHA-1
Certificate Policy extension	Yes - Not Critical
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.1
Policy URL	http://www.transsped.ro/repository
Policy Notice	*userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/for* *SAFE use see SAFE CP at http://www.safe-biopharma.org/cp-pdf; other use see Trans Sped CP at http://www.transsped.ro/repository*
Policy Identifier OID	1.3.6.1.4.1.39965.2.1.3
Policy URL	http://www.transsped.ro/repository
Policy Notice	*userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/for* *SAFE use see SAFE CP at http://www.safe-biopharma.org/cp-pdf; other* *use see Trans Sped CP at http://www.transsped.ro/repository*
CRL Distribution Point	NA (Vo CRL checking for OCSP certificates, hence NOcheck extention and refresh every 30 days).
Authority Information Access	Yes – not critical
Access Method :CAIsuuers	URI = http://aia3.com-strong-id.net/PCA/TS-SAFE-PCA-III.p7c
OCSP No Check	Yes, Not Critical
Extended Usage	Yes- Not Critical
Extended Key Usage	OCSP Server
SubjectAltNames	Yes, http URL for the OCSP responder: http://ocs3.com-strong-id.net/TCA-III

10.7 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	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Signature	Optional; sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Request Extension	**Value**
Nonce	c=no; Required for digital signature validation only
Request Entry Extension	**Value**
None	None

10.8 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	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[3], thisUpdate, nextUpdate[4]
Responder Signature	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**
None	None

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

[4] The OCSP Responder shall use this Update and nextUpdate from PCA CRL. nextUpdate value shall be 1 hour or less.

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

The Trans Sped PCA 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

Trans Sped directory system shall permit “none” authentication to read certificate and CRL information.

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

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

11.3 Naming

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

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

11.4 Object Class

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

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

11.5 Attributes

PCA 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 .
CWA 14167-1	European Committee for Standardization (CEN) Workshop Agreement (CWA) Standard: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures — Part 1: System Security Requirements
CWA 14167-2	European Committee for Standardization (CEN) Workshop Agreement (CWA) Standard: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures — Part 2: Cryptographic Module for CSP Signing Operations — Protection Profile (MCSO-PP)
CWA 14169	European Committee for Standardization (CEN) Workshop Agreement (CWA) Standard: Secure Signature-Creation Devices “EAL 4+” [Protection Profile — Secure Signature-Creation Device, Type 3]
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.
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani et. Al., October 2003.
CIMC PP	Protection Profile for Certificate Issuing Management Components, Version 1, October 2001 http://www.csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf

13 ACRONYMS & ABBREVIATIONS

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

DN	Distinguished Name
DSS	Digital Signature Standard
EU	European Union
FBCA	Federal Bridge Certification Authority
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
IETF	Internet Engineering Task Force
HTTP	Hypertext Transfer Protocol
HTTPS	SSL for HTTP
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
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
SICA	SAFE-BioPharma Issuer Certificate Authority
TA	Trusted Agent
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

14 GLOSSARY

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

Access	Ability to make use of any information system (IS) resource.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
PCA 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 PCA	The PCA is a PCA designated by an Issuer to interoperate with the SBCA. An Issuer may designate multiple 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 PCA	In a hierarchical PKI, a PCA whose certificate Signing Key is certified by another PCA, and whose activities are constrained by that other PCA (see superior PCA).
Superior PCA	In a hierarchical PKI, a PCA who has certified the certificate Signing Key of another PCA, and who constrains the activities of that PCA. (See subordinate PCA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trust Anchor	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trust anchors are used to start certification paths.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

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

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

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

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

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