TRANS SPED
Certificate Policy for DirectTrust

June 2023

Version 2.4

Document Control

Area	Description
Author(s):	Trans Sped Core Team
Change Control	Trans Sped Procedure Team
Approver	Trans Sped Policy Management Authorities
Issue Date	June, 2023
Version	2.4
Source File	Trans Sped PCA Certificate Policy for DirectTrust 2.2.
Distribution	

Guide to verb usage* when signifying requirements in this Certificate Policy.

Must	An absolute requirement
must not	An absolute prohibition
should	There may exist valid reasons in particular circumstances to ignore this requirement, but the full implications must be understood and carefully weighed before choosing a different course.
Should not	There may exist valid reasons in particular circumstances when a particular behavior is acceptable or useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
May	Describes a behavior that is optional. An implementation that does not include a particular option must be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality.

*Definitions derived from RFC 2119

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
1.1	September 2014	Rich Furr, Dale Rickards, Viky Manaila	Update Art.3.2.3.1 - Mention regarding collecting of DoB and CoB
2.0	April 2017	Viky Manaila	Update ETSI ESI standards and eIDAS Regulation Update OIDs for qualified certificates according to eIDAS Regulation Update q-cert statements
2.1	December 2017	Jose Lopez	This is a minor update to address the CP and CPS audit finding from 2017 SAFE audit,,
2.2	August 2021	Camelia Ivan	Change SAFE Bio-Pharma to SAFE Identity and update according to SAFE Identity Policy
2.3	September 2022	Camelia Ivan	Incorporate policies for CMS Incorporate DirectTrust Identity changes Updates to Section Titles to align with RFC 3647 Updates to Section 3.1.3 to align with Federal Policy Updates to 3.2.3 to clarify Basic Assurance Proofing Updates to 4.9 to clarify timing of CRL Issuance
2.4	June 2023	Camelia Ivan	Certificates profile update

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

This Certificate Policy (CP) 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 community. These Issuers may be internal to a single company, or may be operated by a third-party provider such as Trans Sped. The intention is that the Digital Certificates issued by these PKI domains will support Authentication, Digital Signature, and Key Management in a manner needed to provide assurance of the integrity ofthe related transaction.

The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it reflects how well the Relying Party can be certain that the individual whose subject nameis cited in the certificate is controlling the use of the private key that corresponds to the public key inthe certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task.

DirectTrust Identity will employ a DirectTrust Identity Bridge Certification Authority (DIBCA) to cross-certify with each Principal CA in a peer-to-peer fashion.

The DIBCA will seek to cross-certify with other Bridge Certification Authorities in order to promote interoperability among the members of both communities.

Trans Sped will issue EU-qualified DIRECTTRUST Digital Certificates. This CPdefines the policies

under which the Trans Sped PCA operates and shall be used to cross-certify the Trans Sped

PCA with the DIBCA. This Certificate Policy (CP) complies with the Internet Engineering

Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509

Public Key Infrastructure Certificate Policy, andCertification Practice Statement Framework.

For purposes of this Trans Sped CP, all terms used shall have the meanings set forth in the DIRECTTRUST Identity System Documentation Glossary.

DIRECTTRUST Identity Subscriber certificates issued at Medium Assurance level in accordance with this CP and the DIRECTTRUST Identity CP (DIRECTTRUSTCP) will meet the requirements of Qualified Certificates in accordance with eIDAS Regulation (910/2014) and ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

Qualified certificates issued by Trans Sped 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 refers to the following:

- 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 DIRECTTRUST-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 eIDAS Regulation.
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 eIDAS Regulation.

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 must not assert the DIRECTTRUST Identity CP object identifiers (OIDs) listed below in any certificates they issue,except in the *policy Mappings* extension for certificates issued to the DIBCA, and then only upon approval by the DIRECTTRUST Identity PAA.

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

mediumSoftwareAssurance- SHA256	
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 must be interpreted under and governed by the DIRECTTRUST Identity 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 must 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 suchas the SBCA, or PCA), this CP shall so indicate.

The Subscriber certificates issued at a medium assurance level in accordance with this CP must serve the purpose of a Qualified Certificate in accordance with eIDAS Regulation.

1.1.1 PCA Certificate Policy (CP)

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

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

1.1.2 Relationship between this CP and the Trans Sped DirectTrust Identity Issuer Certificate Practices Statement (CPS)

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

1.1.3 Relationship between the DirectTrust Idenity CP and the Trans Sped Identity Issuer CPS

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

The DirectTrust Identity PMA (PMA) has responsibility for mapping the CPs of the Issuers cross-certifying with the DIBCA. The relationship between the DirectTrust Identity CP and this CP is asserted in PCA certificates issued by or to the DIBCA in the *policyMappings* extension. This extension shall indicate that the DirectTrust Identity policy is equivalent to one or more policies as defined by this CP. Conflicts between the DirectTrust Identity 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 PMA approval.

1.1.4 Scope

The DirectTrust Identity PKI exists to facilitate trusted electronic business activities among

DirectTrust Identity Members, between DirectTrust Identity Members and their partners, and between DirectTrust Identity Members and other Bridge communities.

The term Issuer applies to any DirectTrust Identity Issuer permitted by the DirectTrust Identity PMA to cross-certify it's PKI with the DIBCA and to issue certificates that map to one or more of the certificate policy OIDs listed in the DirectTrust Identity CP.

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 DirectTrust identity Bridge PCA. PCA and will issue end-entity certificates.

1.2 Document Name and 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 QCA G3 OID
0.4.0.194112.1.2
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
1.3.6.1.4.1.39965.1.1.1
Trans Sped Mobile eIDAS QCA G3 OID
0.4.0.194112.1.2
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
1.3.6.1.4.1.39965.4.1.1
Trans Sped Electronic Seal QCA G3 OID
0.4.0.194112.1.3
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (2)
1.3.6.1.4.1.39965.5.1.1
Trans Sped Advanced eIDAS CA G3 OID
0.4.0.2042.1.1
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)
1.3.6.1.4.1.39965.6.1.1
Trans Sped Time Stamping CA G3
0.4.0.2023.1.1
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)
1.3.6.1.4.1.39965.1.2.1

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

The Subscriber certificates issued at a medium assurance level in accordance with this CP must serve the purpose of a Qualified Certificate in accordance with eIDAS Regulation. The following extension will be asserted in these certificates.

Qualified Certificate Statements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD Id-etsi-qcs-QcRetentionPeriod(value=10) id-etsi-qcs-QcPDS (location of PKI Disclosure Statements = http://www.transsped.ro/repository)

The Trans Sped DirectTrust 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 DIRECTTRUST Bridge
  - Certificate carries the EU Qualified Certificate/SSCD (0.4.0.194112.1.2)
- Medium Assurance Hardware Roaming (MAR)
  - Used for keys generated in cloud-based Hardware Security Modules 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 DIRECTTRUST Bridge
  - Certificate carries the EU Qualified Certificate/SSCD (0.4.0.194112.1.2)
  - This Solution will support the use of a validation service

1.3 PKI Participants

The DirectTrust Identity PKI is comprised of the DITA, DIBCA and the cross-certified 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 DirectTrust Identity PKI.

The following roles are relevant to the Trans Sped components participating in the DirectTrust Identiy PKI.

1.3. Certification Authorities

1.3.1.1 DIRECTTRUST Identiy Policy Approval Authority (PMA)

The DirectTrust Identity PMA is comprised of DIRECTTRUST Identity members and operates under the DirectTrust Identity PMA Charter. With respect to this CP, the PMA is responsible for:

- Review, maintenance, clarification, approval, and updates to this DirectTrust Identity CP,
- Review and approval of applications from Issuers requesting cross-certification with the DIBCA, to include determination of the CP equivalency mapping betweenthe Issuer's CP and this CP, and
- Confirmation of continued conformance of an Issuer's PKI with DirectTrust Identityrequirements as a condition for continued cross-certification with the DIBCA.

1.3.1.2. Technical Policy Working Group (TPWG)

The Technical Policy Working Group (TPWG) reports to the PMA. The TPWG is responsible for thefollowing:

- Review of CP change requests and recommendations to the DirectTrust Identity PMA for approvalor rejection by the DirectTrust Identity PMA, and
- Review of Applicant CP mapping and interoperability testing and providing recommendationsto the PMA for approval or rejection by the PMA.

1.3.1.3. *DirectTrust* Identity Operational Authority (OA)

The DirectTrust Identity Operational Authority (OA) operates and maintains the DIBCA on behalf ofDirectTrust Identity and under direction from the Operational Authority Manager.

1.31.4. DirectTrust Identity Operational Authority Manager (OAM)

The DirectTrust Identity Operational Authority Manager (OAM) is the individual within DirectTrust Identity who has principal responsibility for overseeing the operation of the DIBCA and DITA including therepositories.

1.3.1.5 *DirectTrust* Bridge Certification Authority (DIBCA)

The DIBCA is operated by the DirectTrust Identity OA and is authorized by the PMA to create, sign, and issue Public Key Certificates to Principal CAs. As operated by the DirectTrust Identity OA, the DIBCA isresponsible for all aspects of the issuance and management of certificates it issues including:

- Control over the registration process,
- The identification and authentication process,
- The Certificate generation process,
- Publication of Certificates to Issuer CAs and OCSP Responders,
- Revocation of all certificates issued,

- Publication of revocation information,
- Re-key of DIBCA signing material,
- Establishment and maintenance of the DIBCA CPS in accordance with this DirectTrust Identity CP, and
- Performance of all aspects of the DIBCA services, operations and infrastructurerelated to Certificates issued under this CP, in accordance with the requirements,representations, and warranties of this CP, and in accordance with the DIBCA CPS.

1.3.1.6 Root Certification Authority (CA)

A Root CA is a trust anchor for subscribers of a PKI domain, when the subscribers act as relying parties.

1.3.1.7 Issuer Principal Certification Authority (CA)

Trans Sped will operate the CA. Trans Sped is authorized to apply for cross certification with the DIBCA and to generate, publish and revoke the DIBCA certificate. The CA 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 certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Ensuring that all aspects of the services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.8 Trans Sped Certification Authority (TSP CA)

The TSP CA is appointed and operates under the authority of the executive managementof Trans Sped.

The TSP CA is chaired by Trans Sped, Operations, Information Security and DirectTrust Identity Program groups within Trans Sped.

The TSP CA is responsible for:

1.3.1.8.1 Establishment and maintenance of this CP in accordance with the DirectTrust -Identity Operating Policies

1.3.1.8.2 Establishment and maintenance of this CP in accordance with European Regulations and Standards

1.3.1.8.3 Review and approval of applicable CPSs as being in conformance with this CP and the DirectTrust Identity Operating Policies

1.3.1.8.4 Ensuring the operation of the PCA and related components comply with the requirements of this CP, applicable CPS and the requirements of the DirectTrust Identity CP.

1.3.1.8.5 Review and approval of applicable CPSs as being in conformance with this CP and the DirectTrust Identity Operating Policies

1.3.1.8.6 Ensuring the operation of the PCA and related components comply with the requirements of this CP, applicable CPS and the requirements of the DirectTrust Identity CP.

1.3.1.9 Direct Trust Identity Anchor

Not applicable

1.3.1.10 Credential Management System

The Credential Management System is responsible for managing device content. In the context of this CP, use of the CMS is optional. When a CMS is implemented, the CMS requirements in this CP are mandatory.

1.3.1.11 Certificate Status Authority (CSA)

A CSA provides status of certificates or certification paths. A CSA can be operated in conjunction with an Entity's CAs or independent of the CAs. Examples of CSAs are:

- OCSP Responders that provide revocation status of certificates.
- Simple Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services[2].

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide certificate validation services adhere to the same security requirements as repositories.

1.3.1.12 Remote Signing Service Provider (RSSP)

The private keys for multiple subscribers may be stored on a remote signing service provider, or RSSP, 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 the 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 RSSP asspecified in this CP.

1.3.1.13 Remote Administration Workstation

Remote Administration Workstations may be used to administer CA, CMS, CSA and RSSP equipment and/or associated HSMs from a specific secure location outside the security perimeter of the CA, CSA or RSSP. In essence, the Remote Administration Workstation is a logical extension ofthe secure enclave in which the CA, CMS, CSA and/or RSSP equipment reside.

1.3.2 Registration Authorities

The RA for the PCA collects and verifies Subscriber's identity and information for inclusion in the Subscriber's certificate 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.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in an end-entity certificate, agrees to use its key and certificate in accordance with the certificate policy asserted in the certificate, and does not itself issue certificates.

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

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

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

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name

to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can usethe certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

1.3.5.1 Related Authorities

The Trans Sped CAs may require the services of other security, community, andapplication authorities. If required, the applicable CPS must identify the parties, define the services, and designate the mechanisms used to support these services. Examples of other participants include compliance auditors and attribute authorities.

1.3.5.2 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.

1.3.5.3 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. A TA does not have privileged access to the CA to enter or approve subscriber information; a TA acts on the behalf of the LRA/RAonly to verify the identity of the Subscriber. A Trusted Agent may be an entity certified by a National or State Government as authorized to confirm identities (e.g. Notary).

The TA, certified entity, or the applicant must forward the information collected directly to the RA or LRA in a secure manner. Packages secured in a tamper-evident manner by the TA or certified entity satisfy this requirement; other secure methods are also acceptable. Such identity-proofing doesnot relieve the RA and LRA of its responsibility to verify the presented data.

1.3.5.4 Machine Operator

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

1.3.5.5 Affiliated Organization

Subscriber certificates may be issued on behalf of an organization that has a relationship with the Issuer PKI; this is termed *Affiliation*. The organizational affiliation shall be indicated in a relativedistinguished name in the subject field in the certificate, and the certificate shall be revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.6 Applicability

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding

description of the applicability for applications suited to each level.

Assurance Level	Applicability
Basic Software	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
Medium Software	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in software at this assurance level.
Medium-hardware or Content Signing	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware at this assurance level.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Appropriate certificate usage is defined in the *keyusage* and *extendedkeyusage* extensions of thepublic key certificate.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 *Contact Person*

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

1.5.3 *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.

1.5.4 CPS Approval Procedures

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

The Trans Sped CA may replicate posted certificates and CRLs to additional repositories in order to enhance the overall performance and security of the Trans Sped PKI. Trans Sped will operate repositories needed to support Trans Sped operations on a 24 hour per day/365 day per year basis, with this service including a directory.

Trans Sped must operate repositories to support PCA operations. Trans Sped must ensure interoperability with the DIBCA repository so that Relying Parties may obtain PCA Certificates and, if published externally, CRLs from or through that repository.

The repositoryobligations must include:

- Accessibility through Hypertext Transfer Protocol (HTTP).
- Availability of the information as required by the certificate information posting andretrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository fromunauthorized modification as described in later sections.

2.2 Publication of Certification Information

2.2.1 Publication of PCA Information

This CP is made available publicly; information on how to obtain a copy of this CP is posted on the: http://www.transsped.ro/repository

Sections of the Trans Sped CPS relevant to use by a Relying Party must also be made available to public at the same URL, or upon email requestto office@transsped.ro

2.2.2 Interoperability

CRLs and .p7c files posted to repositories must be binary DER encoded files.

When Subscriber certificates are published using LDAPv3, they are published using standards-basedschemas for directory objects and attributes.

2.3 Frequency of Publication

The CP and any subsequent changes will be made available publicly within one week of approval bythe PMA.

CA certificates and CRLs must be published as specified in Section 4 of this CP.

2.4. Access Controls on Repositories

Trans Sped must protect repository information not intended for public dissemination or modification. The CP, CA certificates and certificate status information must be publicly available.

3. Identification & Authentication

3.1 Naming

3.1.1 Types of Names

A CA must only generate and sign Certificates that contain a non-null subject DistinguishedName (DN) complying with the X.500 standard.

Content Signing certificates must clearly indicate the organization administering the CMS.

Assertion Signing certificates must clearly indicate the organization that is authoritative for theassertion.

In addition, Human Subscriber certificates must include the RFC822 e-mail address of the Subject in the Subject Alternative Name (SAN) field. For all other subscriber certificates, theSAN is optional. There is no restriction on the use of additional name forms in the SAN.

OCSP Responder certificates must include the HTTP URL of the subject Responder in theSAN.

3.1.2 Need for Names to be Meaningful

Names used in the certificates must identify the person or machine to which they are assigned ina meaningful way and must not be misleading.

The directory information tree must accurately reflect organizational structure.

The common name must observe name space uniqueness requirements and should represent the subscriber in a way that is easily understandable for humans. For people this is typically a legal name. For machines, this may be an application process (e.g. Organization X Primary Router). Thisdoes not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

3.1.3 Anonymity or Pseudonymity of Subscribers

CA certificates must not contain anonymous or pseudonymous identities.

A CA may issue pseudonymous certificates to Subscribers to support its operations, provided name space uniqueness requirements are met and the pseudonym is traceable to the actual identity.

A CA must not issue anonymous certificates to its subscribers.

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 DIBCA.

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

Trans Sped does not knowingly use trademarks in names unless the subject has the rights to use thattrademarked name.

3.1.7 Name Claim Dispute Resolution

Trans Sped must resolve any name collisions or disputes brought to their attention regarding certificates they issue.

3.2 Initial Identity Validation

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) must 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 therequesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of Individual Identity

3.2.3.1 Identity-Proofing of Human Applicants

All identity proofing of human applicants must meet or exceed NIST SP 800-63A Identity Assurance Level Two (IAL2). IAL2 allows remote or in-person identity proofing. Within the DirectTrustIdentity community, remote identity proofing is valid for basic assurance policy OIDs; in-person (or supervised remote) identity proofing is valid for both basic and medium assurance policy OIDs (see Section 1.2).

3.2.3.1.1 Basic Assurance Identity Proofing

Identity may be established through an in-person proofing process before a Registration Authority, Local Registration Authority or Trusted Agent (see requirements for medium hardware below); or remotely by verifying information provided by an Applicant through an on-line identity proofing process. For the case of in-person proofing, the Registration Authority, Local Registration Authority or Trusted Agent must ensure to validate that all presented identity documents are not expired and are not fraudulent. For cases of remote verification, the information provided by the applicant is verified through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that name, Date of Birth (DoB), address and other personal information in such records are consistent with the application and sufficient to identify a unique individual. All such record checks will take place over an authenticated protected channel.

For remote identity proofing, the applicant must provide the credential numbers associated with at least two pieces of documentary evidence (e.g. passport, driver's license, alien registration number, credit card number). In all cases, the documents must be valid and unexpired. Each document presented must be validated with the issuer or other authoritative source and the information contained in the application verified against the document issuer's records.

Address confirmation is attained by sending an enrollment code to a postal address of record. Minimally, the enrollment code must be a random six character alphanumeric or a machine-readableoptical label, such as a QR Code that contains data of similar or higher entropy as a random six character alphanumeric, for use by the applicant in completing the enrollment process.

in completing the enrollment process.

Practice Note: An address of record may be home residence, business address or an address provided by the registrant that must be verifiable either with a company representative or through a lease or utility bill in the registrant's name.

A registration agent (either RA, LRA or TA) must 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 ofthe applicant. This declaration must use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law;
- Unique ID number(s) provided by the applicant, or other unique ID number(s) thatare linked directly to the applicant, and the names of the databases from which the number(s) were verified;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of an RA, LRA, TA or an individual certified by a State orNational Entity as being authorized to confirm identities using the format set forth at28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

3.2.3.1.2 Medium Software and Medium Hardware Identity Proofing

Identity must be established by in-person or supervised remote[3] identity proofing before a RA, LRA,TA or an individual certified by a State or National Entity as being authorized to confirm identities. Information provided must be verified to ensure legitimacy.

Credentials required are either one National Government-issued Picture I.D, one U.S. REAL ID Actcompliant picture ID[4], or two Non-National Government I.D.s, one of which must be a photo I.D.[5] For applicants in the EU, presentation of a national identity card or comparable satisfies this requirement. Any credentials presented must be unexpired.

The individual performing the identification must record the information set forth below for issuance of each Certificate:

- The identity of the individual performing the identification;
- A signed declaration by that individual that he or she verified the identity of the applicant. This declaration must use the format set forth at 28 U.S.C. 1746 (declaration under penalty ofperjury) or comparable format under local law;
- A unique identifying number(s) from the ID(s) of the applicant or a facsimile ofthe ID(s). In the case of an in-person antecedent, another trusted source of information may be used provided it meets the requirements set forth below for *Antecedent Identity Proofing*;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate

Practice Note: In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signaturecertificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails tosign the declaration of identity then the certificate must be revoked.

- digital 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.

Identity must be established no more than 90 days before initial certificate issuance

3.2.3.1.3 Antecedent Proofing

Identity may be established by means of an antecedent in-person proofing process that satisfies thein-person requirements for issuance of a credential that asserts the individual's identity.

The antecedent proofing process must include information created by a previously conducted in-person proofing event. This event must have occurred less than 9 years before the date of application.

A trust relationship between the TA and the applicant which is based on an antecedent in-personrelationship may suffice as meeting the in-person identity proofing requirement.

3.2.3.2 Authentication of Machine Subscribers

Trans Sped does not issue machine certificates

3.2.3.3 Authentication for Group Certificates

Trans Sped does not issue Group Certificates.

3.2.3.4Authentication of Human Subscribers for Role-based Certificates

Subscribers may be issued role certificates. A role certificate must identify a specific role title on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificatecan be used in situations where non-repudiation is desired. A role certificate is not a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time; however, the signature key pair must be unique to each role certificate issued to each individual;

Subscribers issued role certificates must protect the corresponding role credentials in the same manneras individual credentials.

The procedures for issuing role certificates must comply with all other stipulations of this CP

(e.g.,subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations).

Individuals assigned the role may identify themselves for role-based certificate issuance through use oftheir current Signing Key, provided it has an equivalent or higher assurance level than the certificate being requested, otherwise, the initial identity proofing process associated with the role-based certificate's level of assurance must be followed.

Role-based certificates must have a role sponsor. The role sponsor (which is not a trusted role) isresponsible for:

1. Authorizing individuals for a role certificate;
2. Recovery of the private decryption key
3. Request for revocation of individual role certificates;
4. Always maintaining a current up-to-date list of individuals who are assigned the role; and
5. Always maintaining a current up-to-date list of individuals who have been provided thedecryption private key for the role.

For the role signature certificate, the individual assigned to the role or the role sponsor may act on behalf of the certificate subject for certificate management activities such as renewal, re-key and revocation. Issuance and modification of a role signature certificate requires the approval of the role sponsor. Rekey and renewal of a role signature certificate requires the approval of the role sponsor ifthe validity period is extended beyond that already approved by the role sponsor.

The role sponsor must hold an individual certificate in his/her own name issued by the same CA at thesame or higher assurance level as the role certificate. The CA or the RA must validate from the role sponsor that the individual subscriber has been approved for the role certificate. The role sponsor is responsible for providing the following information to the RA or CA before issuing a role certificate:

- Identity of the individual role holder(s)
- Individual authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

Role based certificate is equivalent to eSeal according to eIDAS Regulation

Trans Sped does not issue certificates for encryption

3.2.1 Non-verified Subscriber Information

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

3.2.2 Validation of Authority

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

3.2.3 Criteria for Interoperation

Trans Sped must have to the following:

- CP mapped to and determined by the PMA to be in conformance with the Direct Trust Identity CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8of this CP;
- Issue certificates conformant with the profiles described in this CP, and
- Make certificate status information available in accordance with this CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Subscribers and CAs must identify themselves through use of their current Signing Key or by using the initial identity-proofing process described above. Identity must be established through the initialidentity-proofing process at least once every nine years. See Section 3.2.3.

3.3.2 Identification and Authentication for Re-key After Revocation

If a Certificate is revoked, the Subject must go through the initial identity-proofing process describedin Section 3.2 to obtain a new certificate, unless the subject can be authenticated through the use of avalid public key certificate of equal or higher assurance as specified in Section 3.3.1.

3.4 Identification and Authentication for Revocation Requests

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

4 Certificate life-cycle Operational Requirements

4.1 Application

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

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 eIDAS Regulation shall be created in cryptographic hardware devices (QSCD) that are approved to be used for such purposes.

Other keys may be created in software.

4.1.1 Who Can Submit a Certificate Application

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

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

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.

Applicants must complete the online application form and generate a key pair in accordance with Section 6.1.1 The Applicant must submit the certificate application to the PCA using their Internet browser or other application software. Submitting theapplication form will automatically deliver the Public Key to the PCA in accordance with section 6.1.3

4.1.2 Enrollment Process and Responsibilities

The process for enrollment of the PCA with the DIBCA is specified in the DIRECTTRUST-Identity CP and DIRECTTRUST cross certification process.

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

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

To obtain a Trans Sped digital certificate, the end user must complete a user agreement form, e.g. Https://uaf.transsped.ro/en/UA_Person.aspx , complete the private data and accept the terms and conditions and the Data Privacy Agreement. After completing the form, the end user will meet a trusted agent (TA) (it can be a physical meeting or using video identification). The TA will verify the ID (passport and driving licenses are acceptable as well) and will ensure that the data is correct and the person in the ID is identical to reality and proves identity. Trans Sped RO receives the information from TA and will register the user based on the information provided by TA, and the end user will receive an e-mail with the instructions for activating the certificate.

4.2. 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 PMAhas been established prior to issuance.

In order to prove the user's identity, each user before obtaining a Trans Sped certificate is identified, by RO Trans Sped or by TA. Identification can be done face to face or video. The client's identification evidence is kept by the Trans Sped for 10 years and 6 months from the expiration of the certificate.

4.2.1. Performing Identification and Authentication Functions

Identity proofing for Subscriber Certificates must follow the provisions of this CP, the DirectTrust Identity 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 Subscriber.

4.2.2. Approval or Rejection of Certificate Applications

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

4.2.3. Time to Process Certificate Applications

For subscriber certificates, certificate application processing should not exceed 90 days from the timethe subscriber undergoes identity proofing to certificate issuance.

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

4.3. Certificate Issuance

4.3.1. PCA Actions during Certificate Issuance

The PCA shall:

- Verify the source of a certificate request before issuance;
- Check certificates to ensure that all fields and extensions are properly populated; and
- Post the certificate as set forth in its respective CP, after generation, verification, andacceptance.

Because medium hardware assurance level certificates shall serve the purpose of qualified certificates, the PCA or RA must, in addition to the above, verify the data contained in the request according to the applicable local legislation on Electronic Signatures.

The PCA must generate certificates using the appropriate certificate format, and set validity periods and extension fields in accordance with relevant standards, such as X.509. Certificates must be checked to ensure that all fields and extensions are properly populated.

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

Certificates must be valid for no more than three years from the date of issuance.
After generation, verification, and acceptance, CAs must post the certificate as set forth in section 4.4.2 and publish it in the repository.

4.3.2. Notification to Subscriber by the PCA of Issuance of Certificate

The PCA must 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 must inform the Subscriber that the certificate

is available and notify the Subscriber about the means for obtaining the certificate.

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

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Downloading a certificate or installing a certificate from a message must constitute the Subscriber's reception of the certificate. Usage of the Private Key by the Subscriber, corresponding to a certificate issued under this CP, must be deemed to be acceptance of the certificate.

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

4.4.2. Publication of the Certificate by the PCA

As specified in Section 2.2, all PCA certificates must be published in a published accessible repository.

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

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

4.4.3. Notification of Certificate Issuance by the Principal PCA to Other Entities

For all other CAs, the DIRECTTRUST Identity PMA must be notified upon issuance of all CA certificates.See Section 9.11 for acceptable methods of notification to the PMA.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Keys from access by any other party.

Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Certificates may specify restrictions on use through certificate extensions. Relying partiesare expected to accept public key certificates and associated public keys for the

purposes intended as constrained by the extensions (such as key usage, extended key usage, certificatepolicies, etc.) in the certificates.

4.6. Certificate Renewal

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key

identifier, remainunchanged.

The new certificate may have an extended validity period and may include new issuer information(e.g. different CRL distribution point, AIA and/or be signed with a different issuer key).

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

4.6.1. Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the 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.

4.6.2. Who May Request Renewal

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

The certificate subject (Human Subscriber or Machine Operator for the Machine Subscriber) andLRAs/RAs may request renewal of Subscriber Certificates.

4.6.3. Processing Certificate Renewal Requests

The PCA must approve certificate renewal.

In all cases, the certificate renewal identity-proofing must 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.

4.6.4. Notification of New Certificate issuance to Subscriber

See Section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewed Certificate

See Section 4.4.1

4.6.6. Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.7. Certificate Re-Key

Re-key is identical to renewal except the new certificate must have a different subject public key andsubject key identifier.

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

4.7.1. Circumstance for Certificate Re-key

Section 5.6 establishes maximum usage periods for private keys for both CAs and subscribers. Other circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a newhardware token, and hardware token failure.

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and isentitled to a certificate.

4.7.2. Who May Request Certification of a New Public Key

The PCA may request re-key of its certificate.

Subscribers with a currently valid certificate may request rekey of the certificate.

CAs and RAs may request certification of a new public key on behalf of a subscriber. The Machine Operator may request re-key of the corresponding machine certificate.

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.

4.7.3. Processing Certificate Re-keying Requests

Subscribers must identify themselves for the purpose of re-keying as required in Section 3.3(Identification and Authentication for rekey Requests).

A certificate re-key identity-proofing must 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

4.7.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6. Publication of the Re-keyed Certificate by the PCA

See Section 4.4.2

4.7.7. Notification of Certificate Issuance by the PCA to Other Entities

See section 4.4.3

4.8. Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different subject Public Key and a different serial number, and the new certificate differs in one or more other fields from the old certificate. The old certificate must be revoked if the Subscriber no longer holds one ormore of any authorizations explicitly stated in the old certificate.

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

Once modified, the old certificate may or may not be revoked, but must not be reused for requestingfurther renewals, re-keys or modifications.

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.

4.8.1. Circumstance for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not Applicable.

4.8.3. Processing Certificate Modification Requests

Not Applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6. Publication of the Modified Certificate by the PCA

Not Applicable.

4.8.7. Notification of Certificate Issuance by the PCA to Other Entities

Not Applicable.

4.9. Certificate Revocation and Suspension

Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. Request for revocation may also be submitted via a wet signed letter that is authorized directly with the entity signing the letter, to validate authenticity and to ensure that the entity signing the letter meets the requirements of an entity that may request revocation of the particular certificate.

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 must 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 must be available 24 hours a day, 7 days a week.

4.9.1. Circumstance for Revocation

A Certificate must 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 DIRECTTRUST Identity suspects or determines that revocation of a certificate is in the best interest of the integrity of the DIRECTTRUST Identity 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.

For Certificates that express an organizational affiliation:

- If the affiliated organization no longer authorizes the affiliation of a Subscriber, Trans Sped must revoke any certificates issued to that Subscriber containing the organizational affiliation.
- If an organization terminates its relationship with Trans Sped such that it no longer provides affiliation information, Trans Sped must revoke all certificates affiliated with thatorganization.

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.

If a private key used to approve requests for one or more certificates may have been compromised, all certificates authorized since the date of actual or suspected compromise and

directly or indirectly chaining back to that private key must be revoked or verified as appropriately issued.

4.9.2. Who Can Request Revocation

A human certificate subject, supervisor of a human subject, Human Resources (HR) representativefor the human subject, machine operator for a device subject, issuing CA, or RA may request revocation of a certificate.

For Certificates that express an organizational affiliation:

Trans Sped must accept revocation requests from the designated POC for the organization.

The Trans Sped agreement with the affiliated organization must require that the organization inform Trans Sped of any changes in the subscriber affiliation.

4.9.3. Procedure for Revocation Request

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

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

A Subscriber ceasing its relationship with an Issuer PKI is required to surrender all cryptographic hardware tokens that were issued to the Subscriber by the Issuer PKI, prior to departure. The tokenmust be zeroized or destroyed promptly upon surrender and must be protected from malicious use between surrender and zeroization or destruction. If the hardware tokens cannot be obtained from the Subscriber, then all Subscribers' certificates associated with the un-retrieved tokens must be revoked immediately for the reason of "key compromise."

4.9.4. Revocation Request Grace Period

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

4.9.5. Time within which CA must Process the Revocation Request

The CA must process an authenticated certificate revocation request before the next CRL is generated unless the request and its authentication are received within two (2) hours of CRL generation.

4.9.6. Revocation Checking Requirements for Relying Parties

The matter of how often new revocation data should be obtained is a determination to be made bythe Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

4.9.7. CRL Issuance Frequency

CRLs are issued periodically, even if there are no changes to be made, to ensure timeliness ofinformation. Certificate status information may be issued more frequently than the issuance frequency described below. CAs must ensure that superseded certificate status information isremoved from the PKI Repository upon posting of the latest certificate status information.

Certificate status information must be published not later than the next scheduled update. This willfacilitate the local caching of certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post certificate status information to reduce latency between creation and availability.

The PCA must publish CRLs no less frequently then once every 18 hours. If the CRL is issued every 31 days, the PCA must meet the requirements specified below for issuing Emergency CRLs. The PCA must also notify the DIBCA Operational Authority upon Emergency CRL issuance.

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

4.9.8. Maximum Latency of CRLs

The maximum delay between the time a Subscriber's certificate is revoked by a CA and the time thatthis revocation information is available to Relying Parties must be no greater than 24 hours.

Furthermore, each CRL must be published no later than the time specified in the *nextUpdate* field ofthe previously issued CRL for same scope.

4.9.9. Online Revocation Checking Availability

In addition to CRLs, CAs and Relying Party client software may support on-line status checking.Client software using on-line status checking need not obtain or process CRLs.

If on-line revocation/status checking is supported by a CA, the latency of certificate status informationdistributed on-line by the CA or its delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.9.7.

4.9.10 Online Revocation Checking Requirements

Relying Parties are not required to utilize OCSP. If a Relying Party relies on OCSP, it should do soin accordance with the requirements in RFC 6960.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information must be implemented in a mannerconsistent with the security and latency requirements for the implementation of CRLs and on-line revocation status checking.

In order to support long-term validation of digital signatures on electronic files, issuers must preserve a record of all certificate revocations.

The alternative method(s) must be described in the CA's approved CPS.

4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

Suspension may be permitted for subscriber certificates. Examples of circumstances when suspensionmay be used are: 1) the discretion of the certificate issuer; 2) the user's token is temporarily unavailable; 3) authority to use the token has been temporarily suspended; 4) token possession is unknown.

4.9.14 Who can Request Suspension

The subject Human Subscriber, Machine Operator for the Machine Subscriber (as applicable), supervisory or human resources personnel, and LRAs/RAs or Issuing CA may request suspension ofSubscriber Certificates.

4.9.15 Procedure for Suspension Request

A request to suspend a certificate must identify the certificate to be suspended, explain the reason forsuspension, and allow the request to be authenticated (e.g., digitally or manually signed).

The reason code CRL entry extension must be populated with "certificateHold".

4.9.16 Limits on Suspension Period

Suspension must be resolved as soon as practical. Until that time, the certificate must be treated as revoked. Removal from hold (i.e., suspension) must not be authenticated using the certificate that ison hold, revoked, expired or is otherwise invalid.

The CPS shall describe in detail how this maximum suspension period is enforced. If the subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked for reason of "Key Compromise".

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity must be authenticated in person using initial identity proofing process describedin Section 3.2.3 or using the Human Subscriber Re-Authentication process described in Section 3.2.3.2.

If a certificate is suspended for a period greater than 30 days, an authorizing official must verify theneed for restoring the credential to the individual. Certificates that have expired or otherwise been revoked for other reasons must not be restored.

4.10 Certificate Status Services

Trans Sped are not required to support certificate status services such as SCVP.

4.10.1 Operational Characteristics

No stipulation

4.10.2 Service Availability

When implemented, Certificate Status Services must be available on a 24x7 basis, with a minimum of 99.9% availability overall per year and a scheduled downtime not to exceed 0.5%annually.

4.10.3 Operational Features

No stipulation. Optional features associated with a Certificate Status Server implemented and required by Trans Sped should be described in the applicable CP, otherwise this section is NotApplicable.

4.11 End of Subscription

For Certificates that have expired prior to or upon end of subscription, revocation is not required. Unexpired CA certificates must be revoked at the end of subscription.

4.12 Key Escrow & Recovery

The PCA does not support the issuance of encryption certificates.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility Management & Operations Controls

5.1 Physical Controls

All CA, CSA, CMS and RSSP equipment including their cryptographic modules must be protectedfrom unauthorized access at all times.

All physical control requirements specified below apply equally to the DIRECTTRUST Identity Bridge CA,Issuer CAs, CSAs, CMSs, RSSPs and any remote workstations used to administer the CAs exceptwhere specifically noted.

5.1.1 Site Location & Construction

The location and construction of the facility housing the CA, CSA, CMS and RSSP equipment, as well as sites housing remote workstations used to administer these components, must have protections that are 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, must provide robust protection against unauthorized access tothe CA, CSA and RSSP equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The CA, CSA, CMS, RSSP equipment and remote workstations used to administer these components must be protected from unauthorized access at all times. The security mechanisms mustbe commensurate with the level of threat in the equipment environment.

The physical security requirements pertaining to CAs, CSAs, remote workstations used to administerthe CAs and RSSPs that issue Basic assurance certificates are as follows:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in securecontainers.

In addition to these requirements, the following requirements apply to CAs that issue Medium andMedium Hardware assurance certificates:

- Monitor, either manually or electronically, for unauthorized intrusion at all times;
- Maintain and periodically inspect access logs; and
- Require two-person physical access control to both the cryptographic module and computersystem.

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

A security check of the facility housing the CA, CSA, CMS, RSSP equipment or Administration Workstation must occur if the facility is to be left unattended. At a minimum, the check must verifythe 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 forthe DITA and DIBCA, that all equipment other than the repository is shut down);
- For off-line systems, all equipment other than the PKI Repository is shut down;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

RA equipment must be protected from unauthorized access while the RA cryptographic

module isinstalled and activated. The RA must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms must be commensurate with the level of threat in the RA equipment environment.

5.1.3 Power and Air Conditioning

CAs must have sufficient alternative power supply in the event of a primary power source failure toeither maintain CA operations or, at a minimum, prevent loss of data. The repositories (containing CA certificates, CRLs, and pre-generated OCSP responses) must be provided with uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposure

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

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

5.1.5 Fire Prevention and Protection

Facilities housing CA equipment must comply with local commercial building codes for fireprevention and protection.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

CA backups sufficient to recover from system failure must be made on a periodic schedule as described in the respective CPS. Backups must be performed and stored off-site no less than onceper week, unless the CA is off-line, in which case, it must be backed up whenever it is activated orevery seven (7) days, whichever is later.

At least one full backup copy must be stored at an offsite location. Only the latest full backup needbe retained. The backup must be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if notcarried 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 performedin these roles form the basis of trust for all uses of the DIRECTTRUST Identity PKI. Two approaches are takento 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.

- The requirements of this policy are drawn in terms of four roles (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):*Administrator* – authorized to install, configure, andmaintain the CA; establish and maintain user accounts; configure profiles andaudit parameters; and generate component keys.
- *Agent* – authorized to request or approve certificates, or certificate revocations.
- *Audit Administrator* – authorized to view and maintain CA audit logs.
- *Operator* – authorized to perform system backup and

recovery.

The following sections contain a detailed description of these

5.2.1.1 CA Administrator

The CA Administrator is responsible for:

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

CA Administrators are not permitted to issue certificates.

5.2.1.2 CA Agent

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

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

5.2.1.3 CA Audit Administrator

The CA Audit Administrator is responsible for:

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

- Performing or overseeing internal compliance audits to ensure that the CA isoperating in accordance with its CPS.

5.2.1.4 CA Operator

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

5.2.1.5 CSA Roles

The CSA roles may be held by the corresponding CA trusted role personnel. The CSA requires thefollowing roles:

- The CSA Administrator 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.
- The CSA Audit Administrator 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.
- The CSA Operator is responsible for:
  - The routine operation of the CSA equipment; and
  - Operations such as system backups and recovery or changing recordingmedia.

5.2.1.6 RSSP Roles

The RSSP requires the following roles:

- The RSSP Administrator is responsible for:
  - Installation, configuration, and maintenance of the RSSP;
  - Establishing and maintaining RSSP system accounts;
  - Configuring audit parameters, and;
  - Generating and backing up RSSP keys.The RSSP Audit Administrator is responsible for:
- Reviewing, maintaining, and archiving RSSP audit logs; and
- Performing or overseeing internal compliance audits to ensure that the RSSPis operating in accordance with its CPS.

The RSSP Operator is responsible for

- The routine operation of the RSSP equipment; and
- Operations such as system backups and recovery or changing recordingmedia.

5.2.1.7 Registration Authority (RA)

The RA responsibilities are:

- Verifying identity, pursuant to Section 3.2;
- Entering Subscriber information, and verifying its correctness;
- Securely communicating requests to and responses from the CA; and
- Receiving and distributing Subscriber certificates.

5.2.1.8 Local Registration Authority (LRA)

The LRA responsibilities are:

- Verifying identity, pursuant to Section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA and RA; and
- Receiving and distributing Subscriber certificates.

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

5.2.1.9. CMS Roles

CMS is not implemented

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 must require actions by at least two individuals.

Where multiparty control for logical access is required, at least one of the participants must 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 Identification and Authentication for Each Role

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

An individual in a trusted role must authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) access control, where at least onefactor is a hardware token must be used for log in to a Remote Administration Workstation. In addition, the hardware token used must be acceptable for the highest certificate policy OID supported by the associated CA. Also See Section 6.7 for authentication to the PKI

enclave.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, orprocedurally, or by both means

Individual CA, CSA, and RSSP personnel must be specifically designated to the four roles definedin Section 5.2.1 above as applicable.

For CAs that exclusively issue certificates at the basic levels of assurance, individuals may assume more than one role, except no one individual may assume both the Agent and Administrator roles. This may be enforced procedurally.

For CAs that issue at the medium levels of assurance, individuals may assume only one of the Administrator, Agent, and Audit Administrator roles, but any individual may assume the operatorrole.

Individuals in trusted roles must not be assigned more than one identity

2. 5.3 Personnel Controls

5.3.1 Qualifications, Experience, & Security Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA, RSSP and CSA mustbe identified and assigned to trusted roles per Section 5.2.1.

All persons filling trusted roles must be selected on the basis of loyalty, trustworthiness, and integrity.

For PKIs operated at medium-software and/or medium-hardware, each person filling a trusted rolemust satisfy at least one of the following requirements:

- The person shall be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person shall be acitizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the memberstates of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in ArmsRegulation (ITAR) – 22 CFR 120.32.

For RAs and personnel appointed to the trusted roles for the CSAs, in addition to the above, the personmay be a citizen of the country where the function is located.

For PKIs operated at any of the Basic or Commercial Best Practice (CBP) assurance levels, there is nocitizenship requirement or security clearance specified.

5.3.2 Background Check Procedures

Trusted role personnel must, at a minimum, pass a background investigation covering the followingareas:

- 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. Adjudication of the background investigation must be performed by a competent adjudication Authority using a process consistent with U.S. Executive Order 12968, August 1995, or equivalent. Regardless of the date of award, thehighest educational degree must be verified.

If a formal clearance or other check is the basis for background check, the background refresh must be in accordance with the corresponding formal clearance or other check. Otherwise, the backgroundcheck must be refreshed every ten years.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA, CSA, CMS, or RSSP mustreceive comprehensive training in all operational duties they are expected to perform.

In particular, they must receive training in the following areas:

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

Documentation must be maintained identifying all personnel who received training and the level oftraining completed.

5.3.4 Retraining Frequency & Requirements

All personnel performing duties with respect to the operation of a CA, CSA, CMS, RSSP, RA or LRA must be aware of changes in the CA, CSA, CMS, RSSP, RA or LRA operations, as applicable.Any significant change to the operations shall have a training (awareness) plan, and the execution ofsuch plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation must be maintained identifying all personnel who received training and the level oftraining completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation. If regular job rotation is implemented by an Issuer CA, it should be identified in thecorresponding CP, otherwise this is Not Applicable (N/A).

5.3.6 Sanctions for Unauthorized Actions

DIRECTTRUST Identity or the Issuer must take appropriate administrative and disciplinary

actions against personnel who perform unauthorized actions (i.e. in violation of governing CP and CPS) involvingthe CA, its repository, the CMS, the RSSP or the CSA.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the CA, CSA, CMS, RSSP, RA orLRA operations are subject to the requirements of this CP.

5.3.8 Documentation Supplied To Personnel

The CA, CSA, and RSSP must make documentation sufficient to define duties and procedures foreach trusted role available to the personnel fulfilling those roles.

5.4 Audit Logging Procedures

Audit log files must be generated for all events relating to the security of the CA, CSA, CMS, RSSP,RA and LRA. For Issuer CAs, the audit must encompass the signing CA that is cross certified with DIBCA and any CAs subordinate to the signing CA. For CAs operated in a virtual machine environment (VME)[6], audit logs must be generated for all applicable events on both the virtualmachine (VM) and isolation kernel (i.e. hypervisor).

Where possible, the security audit logs must be automatically collected. Where this is not possible, alogbook, a paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section must be maintained in accordance with the retention period for archive, Section 5.5.2.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CSA, CMS, RSSP, RA, LRA operating system and application Components required by this CP must be enabled. As a result, most of the events identified in the table are automatically recorded. An “X” in a table cell indicates that the respectiveComponent (CA, CSA, CMS, RSSP, RA or LRA) must 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. At a minimum, each audit record must 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.

A message from any source requesting an action by a CA is an auditable event. The message mustinclude message date and time, source, destination and contents.

For the RSSP, all access and use of subscriber private keys are auditable events.In addition,

the following events must be audited:

Auditable Event	CA	CSA	RSSP	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
AUTHENTICATION EVENTS					
Successful and unsuccessful attempts to assume a role	X	X	X	X	X

Auditable Event	CA	CSA	RSSP	RA	LRA
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
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* 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 CA for key recovery purposes	X	N/A	X[2]	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE					
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X	X
SECRET KEY STORAGE					
Auditable Event	**CA**	**CSA**	**RSSP**	**RA**	**LRA**
The manual entry of secret keys used for authentication (not required for Basic Assurance).	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	N/A	N/A	X	X
CERTIFICATE REVOCATION					
All certificate revocation requests	X	N/A	N/A	X	X
CERTIFICATE STATUS CHANGE APPROVAL					
The approval or rejection of a certificate status change request	X	N/A	N/A	N/A	N/A
CA CONFIGURATION					
Any security-relevant changes to the configuration of the Component	X	X	X	X	X
ACCOUNT ADMINISTRATION					
Roles and users are added or deleted	X	-	-	-	-
The access control privileges of a user account or a role are modified	X	-	-	-	-
CERTIFICATE PROFILE MANAGEMENT					
All changes to the certificate profile	X	N/A	N/A	N/A	N/A
REVOCATION PROFILE MANAGEMENT					
All changes to the revocation profile	X	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE					
All changes to the certificate revocation list profile	X	N/A	N/A	N/A	N/A

MISCELLANEOUS					
Appointment of an individual to a Trusted Role	X	X	X	X	X
Designation of personnel for multiparty control (not required for Basic assurance.)	X	X	-	-	-
Installation of the Operating System	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	X
Installation of hardware cryptographic modules (not required for Basic assurance.)	X	X	X	X	X

Auditable Event	CA	CSA	RSSP	RA	LRA
Removal of hardware cryptographic modules (not required for Basic assurance.)	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 (not required for BASIC Assurance)	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X
Back up of the internal CA database	X	-	N/A	-	-
Restoration from back up of the internal CA database	X	-	N/A	-	-
File manipulation (e.g., creation, renaming, moving) (not required for Basic assurance.)	X	-	-	-	-
Posting of any material to a repository (not required for Basic assurance.)	X	-	N/A	-	-
Access to the internal CA database (not required for Basic assurance.)	X	X	N/A	-	-
All certificate compromise notification requests	X	N/A	N/A	X	X
Loading tokens with certificates (not required for Basic assurance.)	X	N/A	X	X	X
Shipment of Tokens (not required for Basic assurance.)	X	N/A	N/A	X	X
Zeroizing Tokens	X	N/A	N/A	X	X
Re-key of the Component	X	X	X	X	X
CONFIGURATION CHANGES					
Hardware	X	X	X	-	-

Software	X	X	X	X	X
Operating System	X	X	X	X	X
Patches	X	X	X	-	-
Security Profiles	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY					
Personnel Access to room housing Component (not required for Basic assurance.)	X	-	X	-	-
Access to the Component (not required for BASIC Assurance)	X	X	X	-	-

Auditable Event	CA	CSA	RSSP	RA	LRA
Known or suspected violations of physical security	X	X	X	X	X
ANOMALIES					
Software error conditions	X	X	X	X	X
Software check integrity failures	X	X	X	X	X
Receipt of improper messages (not required for Basic assurance.)	X	X	X	X	X
Misrouted messages (not required for Basic assurance.)	X	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X	X
Equipment failure	X	-	-	-	-
Electrical power outages (not required for Basic	X	-	-	-	-
Uninterruptible Power Supply (UPS) failure (not required for Basic assurance.)	X	-	-	-	-
Obvious and significant network service or access failures (not required for Basic assurance.)	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

5.4.2 Frequency of Processing Audit Log

For CA Systems operating at Medium Assurance, audit logs from the CA, CSA, CMS, RSSP, RA, and LRA must be reviewed at least once every two months. At a minimum, a statistically significantset of security audit data generated by the Component since the last review must be examined (wherethe confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a

review), as well as a reasonable search for any evidence of malicious activity.

The analysis must 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 logentries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews must be documented.

For CA Systems operating at Basic assurance, documentation and explanation of significant eventsin an audit log summary is required only for cause.

5.4.3 Retention Period for Audit Log

At medium assurance, audit logs must be retained onsite until reviewed.

At basic assurance, audit logs must be retained onsite for 60 days or until reviewed.

For the CA, CMS, CSA, RSSP and the remote Administration Workstations, the Audit Administrator is the only person authorized to manage the audit log (e.g., review, backup, rotate, delete, etc.). For the RA, a System Administrator other than the RA is responsible for managing theaudit log.

5.4.4 Protection of Audit Log

Component system configuration and operating procedures must ensure that:

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

The individual performing audit log archive need not have modify access, but procedures must beimplemented to protect audit log data from destruction prior to the end of the audit log retention period (note that deletion may require modification access). Audit logs must be moved to a DirectTrust, secure storage location separate from the CA System.

It is acceptable for the system to overwrite audit logs after they have been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up at least once every 30 days, unless the CA isoffline, in which case audit logs and audit summaries must be backed up when the system is activated or every 30 days, whichever is later. A copy of the audit log must be sent off-site following review.

5.4.6 Audit Collection System (Internal or External)

The audit log collection system may or may not be external to a component. Audit processes must 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 (or comparable Issuer PKI entity) must be notified, and a determination must be made whether to suspend the Component operation until theproblem is remedied.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the

individual,organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

No stipulation beyond Section 5.4.2.

5.5 Records Archival

CA, CSA, RSSP, RA and LRA archive records must be sufficiently detailed to verify the proper operation of the PKI and to verify the validity of any certificate (including those revoked or expired)issued by the CA.

5.5.1 Types of Events Archived

Records and material information relevant to use of, and reliance on, a DIRECTTRUST Identity certificatemust be archived. At a minimum, the following data must be recorded for archive in accordancewith each assurance level:

Data To Be Archived	CA	CSA	RSSP	RA	LRA
Certification Practice Statement	X	X	X	X	X
All Contractual obligations	X	X	X	X	X
Certificate Policy	X	X	X		
All required audit reports					
System and equipment configuration	X	X	X	-	-
Modifications and updates to system or configuration	X	X	X	-	-
Certificate requests	X	-	N/A	-	-
Revocation requests	X	-	N/A	-	-
Subscriber identity authentication data as per Section 3.2.3	X	N/A	N/A	X	X
Documentation of receipt and acceptance of certificates	X	N/A	N/A	X	X
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	-	-	N/A	N/A
All access to certificate subject private keys retained within the CA for key recovery purposes	X	-	X	N/A	N/A
All changes to the trusted public keys, including additions and deletions	X	X	-	N/A	N/A
The export of private and secret keys (keys used for a single session or message are excluded)	X	-	X	N/A	N/A
The approval or rejection of a certificate status change request	X	-	-	N/A	N/A
Appointment of an individual to a Trusted Role	X	-	-	N/A	N/A

Remedial action taken as a result of violations of physical security	X	X	X	N/A	N/A
Violations of Certificate Policy	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X
Documentation of receipt of Tokens	X	N/A	N/A	X	X
All certificates issued or published	X	N/A	N/A	N/A	N/A
Record of Component Re-key	X	X	X	X	X
All CRLs issued and/or published	X	N/A	N/A	N/A	N/A
All Audit Logs	X	X	X	X	X

Data To Be Archived	CA	CSA	RSSP	RA	LRA
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 is 10 years and 6 months for Medium and MediumHardware assurance levels and 7 years & 6 months for Basic assurance levels.

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

Alternatively, data may be retained using whatever procedures have been approved by the U.S. National Archives and Records Administration or by the respective records retention policies in accordance with whatever laws apply for that category of documents. Applications required to process the archive data must also be maintained for the minimum retention period specified above.

Once the Remote Administration Workstation logs have been reviewed and reconciled with the corresponding CA, RSSP or CSA logs, they shall be retained for at least one year, further archive ofthe Administration Workstation logs is not required. However, the reconciliation summary must be retained for the full archive period prescribed for the CA archive. In addition, events external to theAdministration Workstation (e.g. physical access) must be retained for the full archive period prescribed for the CA archive.

5.5.3 Protection of Archive

Only authorized individuals are permitted to add to or delete from the archive. The archived records may be moved to another medium only when authorized by the Audit Administrator. The contents ofthe archive must not be released except as determined by the PMA (or comparable Issuer PKI entity)or as required by law.

Records of individual transactions may be released upon request of any subscribers involved in thetransaction or their legally recognized agents.

Archive media must be stored in a DirectTrust, secure storage facility separate from the component itselfwith physical and procedural security controls equivalent or better than those of the PKI.

5.5.4 Archive Backup Procedures

If an Issuer CA chooses to back up its archive records, the CPS or a referenced document must describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CA archive records must be automatically time-stamped as they are created. The CPS must 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. Issuer CAs should identify the Archive Collection System in the applicable CP orCPS.

5.5.7 Procedures to Obtain & Verify Archive Information

No Stipulation. Procedures detailing how to create, verify, package, transmit, and store the archiveinformation, must be described in the applicable CPS.

5.6 Key Changeover

To minimize risk from compromise of a CA's Private Signing Key, that key may be changed often. Once changed, only the new key may be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using theassociated Private Key have also expired. If the old Private Key is used to sign CRLs, it may be retained. If retained, the old key must be protected at the same level as the new key. As an alternative, after all certificates signed with that old key have expired or have been revoked, the CA may issue a final long-term CRL using the old key, with a *nextUpdate* time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed.

Certificates issued by the DIBCA have a maximum validity period of six years.
The following table provides the life times for the private keys and certificates issued to the owner of that private key.

Type of Certificate	Lifetime	
	Private Key	Certificate
Self-signed Root CA	20 years	20 years
Intermediate CA	20 years	20 years

Signing CA	10 years	10 years
Signing CA (4096 bit keys)	13 years	13 years
Subscriber Identity or Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
Content Signer	3 years	9 years
Assertion Signer	3 years	90 days
OCSP Responder	3 years	1 month
SCVP Server[7]	3 years	3 years
Server	3 years	3 years

No CA, including a Bridge CA, shall have a private key that is valid for longer than 20 years.

CAs utilizing 4096-bit keys for signing subscriber certificates may use their private keys to sign subscriber certificates for a maximum of 10 years. For all other Issuer CAs, private keys may be usedto sign subscriber certificates for a maximum of six years. CA certificates may be used to sign CRLs and OCSP Responses for the life of the CA certificate.

CAs must not issue subscriber certificates that extend beyond the expiration date of their owncertificates and public keys.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 must be followed. Otherwise, the scope of potential damage must be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised. If it is determined that an incident has occurred with the potential to affect the operations and/or security environments, DIRECTTRUST Identity must be notified within 24 hours of determination and provided a preliminary remediation analysis.

Within 10 business days of incident resolution, the CA or CMS owner must post a notice on its public web page identifying the incident and notify DIRECTTRUST Identity that the notice has been posted.The public notice shall include the following:

- Which CA components were affected by the incident;
- The CA's interpretation of the incident;
- Who is impacted by the incident;
- When the incident was discovered;
- A statement that the incident has been fully remediated.

A CA Operational Authority must reestablish operational capabilities as quickly as possible inaccordance with procedures set forth in the respective CPS.

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

The CMS must have documented incident handling procedures that are approved by the head of theorganization responsible for operating the CMS. If the CMS or CMS keys are compromised, all certificates issued to the CMS must be revoked, if applicable. The damage caused by the CMS compromise must be assessed and all Subscriber certificates that may have been compromised mustbe revoked, and Subscribers notified of such revocation.

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

If a CA or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed; the operation must be reestablished as quickly as possible, giving priority to the ability togenerate certificate status information. Before returning to operation, ensure that the system's integrity has been restored.

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently validCRL, then all CAs that have been issued certificates by the CA must be securely notified immediately. This will allow other CAs to protect their subscribers' interests as Relying Parties.

If the ability to revoke certificates is inoperative or damaged, the CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. Ifthe CA's revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all subscribers that use the CA as a trust anchor to delete the trust anchor.

Trans Sped must post a notice on its web page identifying the incident andnotify the DIRECTTRUST Identity PMA. See Section 5.7.1 for the contents of the notice.

5.7.3 CA Private Key Compromise Recovery Procedures

If a CA's signature keys are compromised, lost, or suspected of compromise:

All cross certified CAs shall be securely notified at the earliest feasible time (so that entities mayissue CRLs revoking any cross-certificates issued to the CA);

A new CA key pair must be generated by the CA in accordance with procedures set forth in theapplicable CPS;

New CA certificates must be requested in accordance with the initial registration process describedelsewhere in this CP;

If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e.,not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the notAfter date remaining the same as in original certificates; and

If the CA is a Root CA, it must provide the Subscribers the new trust anchor using secure means.

The CA governing body must investigate what caused the compromise or loss, and what measuresmust be taken to preclude recurrence.

If a CSA key is compromised, all certificates issued to the CSA must be revoked, if applicable. TheCSA must generate a new key pair and request new certificate(s), if applicable. If the CSA is a trust anchor, the relying parties must be provided the new trust anchor in a secure manner (so that thetrust anchor integrity is maintained) to replace the compromised trust anchor.

If a CMS key is compromised, all Certificates issued to the CMS must be revoked. The CMS willgenerate a new key pair and request new Certificate(s).

If RA signature keys are compromised, lost, or suspected of

compromise: The RA certificate must be revoked immediately;

A new RA key pair must be generated in accordance with procedures set forth in the applicable CPS;

A new RA certificate must be requested in accordance with the initial registration process described elsewhere in this CP;

All certificate registration requests approved by the RA since the date of the suspected compromisemust be reviewed to determine which are legitimate;

For those certificate requests or approvals whose legitimacy cannot be ascertained, the resultant certificates must be revoked and their subjects (i.e., subscribers) must be notified of revocation.

In the event of any of the above, DIRECTTRUST Identity or Issuer CA must post a notice on its web page identifying the incident and notify the DIRECTTRUST Identity PMA and all cross-certified organizations. SeeSection 5.7.1 for the contents of the notice.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CASigning Key are destroyed as a result, the CA must request revocation of its certificates. Further, the CA must re-establish operations by following the procedures for CA key loss or compromise detailed in Section 5.7.3 above.

5.8 CA, CSA and RA Termination

In the event Direct Trust Identity terminates the DIBCA, cross-certified organizations will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought. All certificates signed by the DIBCA will be revoked. Prior to DIBCAtermination, all archive data will be transferred to an archival facility.

In the event of an Issuer CA termination, the Issuing organization responsible must provide notice toall cross certified CAs. Prior to the termination, the Issuer CA shall request revocation of all certificates issued to it. In addition:

- The CA, CSA, and RA shall archive all audit logs and other records prior to termination.
- The CA, CSA, and RA shall destroy all its private keys upon termination.
- The CA, CSA, and RA archive records shall be transferred to an appropriate authority.
- If a Root CA is terminated, the Root CA shall use secure means to notify Subscribers to deleteall trust anchors representing the terminated CA.

Whenever possible, notification of termination must be provided at least two weeks prior to the CAtermination.

Any issued certificates that have not expired must be revoked and a final long term CRL with a *nextUpdate* time past the validity period of all issued certificates must be generated. This final CRLmust be available for all relying parties until the validity period of all issued certificates has passed.

Once the last CRL has been issued, the private signing key(s) of the terminated CA will bedestroyed.

The CA can only be terminated by the Romanian Supervisory Body (SB) or by the Board of Directors of Trans Sped. Trans Sped will inform subscribers of valid certificates (i. e., neither revoked nor expired) in as much advance as circumstances permit, and attempt to provide alternative sources of interoperation.

Trans Sped will make a reasonable effort to transfer the records of the CA and the certificate repository to another issuer of qualified certificates. Trans Sped will also attempt to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of certification services, in order to minimize the effects of Trans Sped ceasing to provide these services by itself.

If no alternative certificate provider continues Trans Sped's services all certificates that have not expired or have not been revoked by the respective subscribers will be revoked by Trans Sped. All relevant documentation will be transferred to the Romanian Supervisory Body as required in the Romanian Electronic Signature Act, DIBCA and eIDAS Regulation.

Subscribers will be notified of such action taken by Trans Sped.

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

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information must be generated inFIPS 140 validated cryptographic modules or equivalent international standards.

Entity	FIPS 140 Level	Minimum Required Security Module
CA (medium assurance)	3	Hardware
CA (basic assurance)	2	Hardware
CMS	2	Hardware
RA/LRA	2	Hardware
OCSP Responder	2	Hardware
SCVP Server	2	Hardware
RSSP	2	Hardware
Code Signing	2	Hardware
Content Signing	2	Hardware
Assertion Signing	2	Hardware
End Entity Signature or Authentication (basic software)	1*	Software
End Entity Signature or Authentication (medium-software)	1*	Software
End Entity Encryption (basic software)	1*	Software
End Entity Encryption (medium-software)	1*	Software
End Entity Signature or Authentication (basic hardware)	2	Hardware

Entity	FIPS 140 Level	Minimum Required Security Module
End Entity Signature or Authentication (medium-hardware)	2	Hardware
End Entity Encryption (medium-hardware)	2	Hardware
Server (medium-software)	1*	Software
Server (medium-hardware)	2	Hardware

*For software modules, FIPS 140 level 1 validation is required for the current or some prior versionof the software; however, software updates can be applied without further evaluation, provided the validated functionality of the module is not materially altered.

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

Multiparty control must be used for CA key pair generation, as specified in Section 5.2.2

Subscriber keys may be generated by the subscriber, RA, LRA, RSSP, or CA using a FIPS-approvedmethod or equivalent international standard.

6.1.2 Private Key Delivery to Subscriber

CAs must generate their own key pairs in hardware.

If subscribers generate their own key pairs, there is no need to deliver private keys and this sectiondoes not apply.

When CAs or RAs generate keys on behalf of the Subscriber, the private key must be deliveredsecurely to the subscriber.

Private keys may be delivered electronically or may be delivered on a hardware cryptographicmodule. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber must not retain any copy of thekey after delivery of the private signing key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during thedelivery process.
- The Subscriber must acknowledge receipt of the private key(s).
- Delivery must be accomplished in a way that ensures that the correct tokens and activation dataare provided to the correct Subscribers.

- For hardware modules, accountability for the location and state of the module must bemaintained until the Subscriber accepts possession of it.
- For electronic delivery of private keys, the key material must be encrypted using a cryptographic algorithm and key size at least as strong as the private key being delivered.Activation data must be delivered using a separate secure channel.

- The CA or the RA must maintain a record of the subscriber acknowledgement of receipt of thetoken.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys generated by the Subscriber or RA must be delivered securely to the CA for certificate issuance in a way that binds the subscriber's verified identity to the Public Key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

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

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers viasecure mechanisms;
- Distribution of the trust anchor through secure out-of-band mechanisms;
- Calculation and comparison of the trust anchor hash or fingerprint against the hashmade available via authenticated out-of-band sources (note that fingerprints orhashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); or
- Downloading the trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloadedprovided the trust anchor is not in the certification chain for the website certificate.

6.1.5 Key Sizes

All FIPS-approved signature algorithms are considered acceptable. If the PMA determines that the security of a particular algorithm has been compromised, it will direct the DIRECTTRUST Identity OA to revoke the affected certificates.

All public keys placed in newly generated certificates (including self-signed certificates) and uses of public key cryptography by PKI components for signature and/or key agreement/encryption operations must use the following algorithm suites for the time periods indicated:

	Public Key Algorithm	Sunset Date
Signature	2048 bit RSA, 224 bit ECDSA in prime field, or 233 bit ECDSA in binary field	12/31/2030

	3072 or 4096 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field	No stipulation

If the Subject Public Key is RSA, it must use the following format:Algorithm OID: rsaEncryption {1 2 840 113549 1 1 1} Parameters: NULL

Modulus m and public exponent e where,m is 2048, 3072, or 4096 bits; and
$2^{16} < e < 2^{256}$

If the Subject Public Key is Elliptic Curve key, it must use the following format. It is assumed thatP256 curve is used.

Algorithm OID: ecPublicKey {1 2 840 10045 2 1},

Parameters: namedCurve P-256 {1 2 840 10045 3 1 7},Subject Public Key: Uncompressed EC Point

All data encryption (including network protocols) used by or in connection with PKI componentsfor administration, communications, and protection of keys or other sensitive data must use the following symmetric algorithms for the time periods indicated:

Symmetric Algorithm	**Sunset Date**
3 Key TDES	Deprecated. May be used until 12/31/2023 only for data blocks that are 8 MB or less per unique key bundle. [9]
AES	No stipulation

All certificates (excluding self-signed certificates), CRLs, and OCSP Responses must use one of thefollowing hashing algorithms for the time periods indicated:

	Expire before 12/31/2030	**Expire after 12/31/2030**
Hash Algorithm for Certificates, CRLs and OCSP Responses	SHA-224 SHA-256 SHA 384	SHA-256 SHA 384 SHA 512

CRLs, OCSP Responder certificates, and OCSP Responses must use the same or stronger signaturealgorithms, key sizes, and hash algorithms as used by the CA to sign the certificate in question.

All PKI components that use hash algorithms for security relevant functions, such as key generationor agreement, communication protocols (e.g. TLS), or password protection, must use the same or larger bit versions of the hash algorithm(s) used by the CA to sign certificates.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) must be generated in accordance with FIPS 186 or equivalent based upon a recognized standard.

Parameter quality checking (including primality testing for prime numbers) must be performed in accordance with FIPS 186 or an equivalent standard; additional tests may be specified by the PMA.

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

The use of a specific key is determined by the key usage and extended key usage extensions in

The X.509 certificate.

- Certificates used for authentication must set the *digitalSignature* bit only.
- Certificates used for digital signatures must set the *digitalSignature* and *nonRepudiation* bits.
- Certificates that have the *nonRepudiation* bit set, must not have the *keyEncipherment* bit or *keyAgreement* bit set.
- Certificates used for encryption must set the *keyEncipherment* bit.
- Certificates used for key agreement must set the *keyAgreement* bit.
- CA certificates must set *cRLSign* and *keyCertSign*

bits. Group certificates must not assert non-repudiation.

Public keys that are bound into certificates must be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (e.g. Transport Layer Security) that provide authenticated connections using key management certificates and require setting both *digitalSignature* and *keyEncipherment* bits.

For End Entity certificates, the Extended Key Usage extension must always be present and must not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs must be consistent with key usage bits asserted.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

The relevant standards for cryptographic modules are found in FIPS PUB 140, *Security Requirements for Cryptographic Modules*. The PMA may determine that other comparable qualification, certification, or verification standards are sufficient. The PMA will identify acceptable alternate standards.

Cryptographic modules must be certified to the levels identified in the table in Section 6.1.1, higher levels may be used. Additionally, the PMA reserves the right to review technical documentation associated with any crypto-modules under consideration for use by any CA.

In addition, private keys shall not exist outside the cryptographic module in plaintext form.

6.2.1.1 Remote Signing Service Provider Key Stores

Remote Signing Service Provider (RSSP) Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in asingle location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber; therefore, RSSP Key Stores must utilize a minimum FIPS 140 Level 2 orequivalent cryptographic module for key storage.

The RSSP must be deployed so as to provide 24 hour per day/365 day per year availability. RSSP providers should implement features to provide high levels of RSSP reliability (99% availability orbetter).

Authentication to the RSSP in order to activate the private key associated with a given certificaterequires multi-factor authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-Person Control

Use of CA, CSA or Content Signing private signing key requires action by multiple persons inaccordance with requirements of Section 5.2.2.

6.2.3 Private Key Escrow

Under no circumstances are signature keys escrowed.

Subscriber private keys issued to human beings and used for decryption must be escrowed to provide key recovery as described in Section 4.12. For end entity private keys issued to machine subscribers and used for decryption, escrow is mandatory unlessthe data protected by these keys will never require recovery. This escrow must take place prior to the generation of the corresponding certificates.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Signing Private Key

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

All copies of the CA private signature keys must be accounted for and protected in the same manneras the originals.

6.2.4.2 Backup of Subscriber Private Signature Keys

RA and LRA signing Private Keys must not be backed up. Subscriber medium hardware assurancesignature private keys must not be backed up or copied.

Subscriber basic and medium software assurance signature private keys may be backed up or copiedas long as they remain under the subscriber's control and meet all the protection and

usage requirements for the subscriber private keys.

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

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

6.2.4.3 Backup of Subscriber Key Management Private Keys

Backed up subscriber private key management keys must not be stored in plain text form outside thecryptographic module. Storage must ensure security controls consistent with the protection providedby the subscriber's cryptographic module.

6.2.4.4 Backup of CSA Private Key

CSA private keys may be backed up. The backup must be performed under the same control as theCSA key activation. All copies of the CSA private keys must be accounted for and protected in thesame manner as the original keys.

6.2.4.5 Backup of Device Private Keys

Machine private keys may be backed up or copied, but must be held under the control of the device'smachine operator or other authorized administrator. Backed up machine private keys must not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the machine's cryptographic module.

6.2.4.6 Backup of RSSP Private Keys

RSSP private keys may be backed up. If backed up, all copies must be accounted for and protectedin the same manner as the original.

6.2.4.7 Backup of Content Signing Private Keys

If backed up, the Content Signing private keys must be backed up under the same multi-person control used to generate the original content signing key. When implemented, procedures for Content Signing private key backup and storage must be included in the appropriate CPS and mustmeet the multiparty control requirement of Section 5.2.2.

6.2.5 Private Key Archival

Private Signature Keys must not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA, CMS, RSSP and CSA private keys must be generated by and remain in an approved cryptographic module. The CA, RSSP and CSA private keys may be exported from the cryptographic module only to perform key back up procedures in accordance with Section 6.2.4.1.

At no time may the CA, RSSP or CSA private key exist in plain text outside the cryptographicmodule.

Subscriber medium hardware assurance signing keys, including RA and LRA signing keys, must notbe transferred from the module in which they are generated.

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

Private or symmetric keys used to encrypt other private keys for transport must be protected fromdisclosure.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store Private Keys in any form as long as the keys are not accessiblewithout the use of an authentication mechanism that is in compliance with the FIPS 140, rating of the cryptographic module.

6.2.8 Method of Activating Private Keys

The user must 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. When pass-phrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data must not be displayed whileit is entered). Biometrics, if used, must provide liveness property to ensure that the user is present. Activation of private keys stored on an RSSP requires multi-factor authentication.

For machine certificates, the device may be configured to activate its private key without requiringits human sponsor or authorized administrator to authenticate to the cryptographic token, providedthat appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9 Methods of Deactivating Private Keys

Cryptographic modules that have been activated must not be left unattended or otherwise availableto unauthorized access.

If cryptographic modules are used to store Subscriber Private Keys, then the cryptographic modulesmust be deactivated via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CP or CPS. CA, CSA and CMS hardware cryptographic modules must beremoved and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles must destroy CA, RA, and CSA private signature keys when they are nolonger needed.

Subscriber Private Signature Keys must be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software

cryptographic modules, this can be achieved by overwriting the data. For hardware cryptographic modules, this will usually require executing a zeroize command. Physical destruction of hardware module is not required.

6.2.11 Cryptographic Module Rating

See table in Section 6.1.1.

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 Section 5.6.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For machines, private keys may be activated without entry of activation data.

For all other certificate types, the activation data used to unlock private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected. Activation data must meet the requirements of FIPS140 Level 2. If the activation data must be transmitted, it must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

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

Subscriber activation data presented to an RSSP in order to access subscriber keys must be changedwhenever the private key is changed, at a minimum.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometricin nature or memorized. If written down, it must be secured at the level of the data that the associated cryptographic module is used to protect, and must not be stored with the cryptographic module. In all cases, the protection mechanism must include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

Subscriber activation data presented to an RSSP in order to access subscriber keys must be protectedfrom disclosure to unauthorized parties, from eavesdropping, and from replay.

6.4.3 Other Aspects of Activation Data

CAs, CMS, CSAs, RSSPs and RAs must change the activation data whenever the token is

rekeyedor returned from maintenance

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions must be provided by the operating system, or through acombination of operating system, software and physical DirectTrustguards. The CA, CSA, CMS, RSSP, Remote Administration Workstations, RA and LRA must include the following functionality (in a VME, these functions are applicable to both the VM and hypervisor):

- Require authenticated logins
- Provide Discretionary Access Control, including managing privileges of users to limit usersto their assigned roles
- Provide a security audit capability (See Section 5.4)
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for user identification and authentication
- Provide domain isolation for processes
- Provide operating system self-protection
- Support recovery from key or system failure.

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

The computer system must be configured with the minimum of the required accounts and network services.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA and CSA are as follows:

- CA must use software, whether off-the-shelf or custom-built, that has been designedand developed under a formal, documented development methodology.
- Procured hardware and software must be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring theequipment was randomly selected at time of purchase).

- Hardware and software that is developed specifically for the CA, CSA, or RSSP must be developed in a controlled environment, and the development process mustbe defined and documented. The PKI owner must demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment. This requirement does not apply to off-the-shelf hardware or software.
- Where open source software has been utilized, the PKI owner must demonstratethat security requirements were achieved through software verification & validation and structured development/life-cycle management.
- All hardware and software must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operationslocation.
- The PKI platform (server hardware, operating system software, VME hypervisor and PKI application software) must be dedicated to performing PKI functions. There must be no non-PKI applications installed on the PKI platform. In a VME, a single hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA. All VM systems must operate in the same security zone as the CA.
- Proper care must be taken to prevent malicious software from being loaded.
- Applications required to perform the PKI operation must be obtained from sources authorizedby local policy.
- Hardware and software updates must be purchased or developed in the same manneras original equipment, and be installed by trusted and trained personnel in a defined manner.
- CA, CSA, CMS, RSSP, and RA/LRA hardware and software must be scanned formalicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

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

All Remote Administration Workstations must be dedicated to remote administration and must be protected while at rest. In particular, they must not be used as personal workstations. The Remote Administration Workstations must be maintained at the same level as the equipment they access (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems apply to this workstation as well).

In addition, only applications required to perform the organization's mission may be loaded on theRA/LRA workstation, and all such software must be obtained from sources authorized by local policy.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The DITA and DIBCA must not be connected to any network. Information to be transferred from theDITA and DIBCA to directories or databases must be done through “out of band” means (e.g., removable media).

CAs, CSAs, CMSs, Repositories, RSSP, Remote Administration Workstations, RAs, and LRAs mustemploy appropriate network 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 must be turned off. Any network software present must be necessary to the functioning of the CA, CSA, CMS, RSSP, or Remote Workstation.

Remote Administration Workstations must access the PKI Enclave using site-to-site VPN. The VPNmust use FIPS approved cryptography commensurate with the cryptographic strength of certificates issued by the PKI being administered. The VPN must be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret-based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

Remote access must be mediated by a bastion host or “jump server” (i.e. a machine that presents a limited interface for interaction). All network activity to the PKI components (e.g. CA, CMS, and/orCSS) must be initiated from the bastion host. The bastion host is considered part of the CA, CMS, and/or CSS and must meet the security requirements for these components. A remote workstation oruser must perform mutual authentication with the bastion host using strong authentication (e.g., PKI credential) commensurate with the cryptographic strength of certificates issued by the PKI being administered. Cryptographic material derived from the authentication must be used to protect the communication with the bastion host. (Note: client-authenticated TLS, SSH and IPSEC are examples of protocols that meet this requirement.) In addition, the user must authenticate to the PKIcomponent being administered via the bastion host. In other words, authentication to the bastion host does not alleviate the need to authenticate to the PKI component(s) being administered.

Remote administration must be designed such that there are positive controls to meet the two-personcontrol requirements specified in this CP. In addition, the remote administration must be designed such that there are positive controls to meet the requirement for the Audit Administrator to control the event logs. Remote administration must continue to fully enforce the integrity, source authentication and destination authentication, as applicable for administrative functions such as configuration, patch management, and monitoring.

All Directories connected to the Internet must provide continuous service to DIRECTTRUST IdentityParticipants and their relying parties.

When used, Transport Layer Security (TLS) must be implemented in a manner such that it meets orexceeds NIST SP 800-52, *Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementation*.

Redundancy must be employed to ensure continuity of service even during periods of maintenanceor backup.

Any boundary control devices used to protect the network on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment even if those services are enabled for otherdevices on the network.

The PCA, CSAs, CCSs, RAs, and LRAs must 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 necessaryto the functioning of the PCA, CSA or CCS.

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

The CPS or supporting operating policies must 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

All CA, CSA, and RSSP components must regularly synchronize with a trusted time service (e.g. National Institute of Standards and Technology (NIST) Atomic Clock or the NIST Network Time Protocol (NTP) Service). Time derived from the trusted time service must be used for establishingthe time of:

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

Asserted times must be accurate to within three minutes. Electronic or manual procedures may beused to maintain system time. Clock adjustments are auditable events. See Section 5.4.1.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Numbers

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

7.1.2 CertificateExtensions

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

Issuer CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions must be non-critical and must not conflict with the certificate and CRL profiles defined inthis CP.

Section 10 contains the certificate formats.

7.1.3 Algorithm Object Identifiers

Certificates must use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 4}

Certificates must use the following OIDs to identify the algorithm associated with the subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters must be specified as one ofthe following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4 Name Forms

The subject and issuer fields of the certificate must be populated with a unique Distinguished Namein accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC5280. Subject and issuer fields must include attributes as detailed in the table below.

CA Name Form

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Required	O	1	Issuer name, e.g., “O=XYZ”
	Optional	ST	0…1	State or Province Name e.g., “ST = Maryland
	Required	C	1	Country name, e.g., “C=US”
2	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ”
	Optional	ST	0…1	State or Province Name e.g., “ST = Maryland
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyz”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

Subject Name Form (Non-CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Subject organization name, e.g., “O=ABC Ltd”
	Optional	ST	0…1	State or Province Name e.g., “ST = Sussex
	Required	C	1	Country name, e.g., “C=GB”
2	Required	See right	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Subject organization name, e.g., “O=ABC Ltd”

	Optional	ST	0…1	State or Province Name e.g., “ST = Delaware
	Required	C	1	Country name, e.g., “C=US
	Required	DC	1	Subject organization domain name, e.g., “DC=abcltd”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

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

7.1.5 Name Constraints

The DIBCA asserts name constraints in certificates issued to Principal CAs appropriate for the PKIbeing certified.

Principal CAs may assert name constraints in the certificates they issue to other CAs within theorganization.

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

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

When the PCA serves more than one users, technical means must 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

CA and Subscriber Certificates must assert one or more of the OIDs listed in Section 1.2 of theappropriate CP.

Depending on the issuing Root CA, Trans Sped has several policy OIDs, as below:

Trans Sped QCA G3 OID

0.4.0.194112.1.2

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

1.3.6.1.4.1.39965.1.1.1

DIRECTTRUST CA OID

1.3.6.1.4.1.39965.2.1.1 mediumAssuranceHardware

trans sped (1.3.6.1.4.1.39965) DirectTrust (2) policies (1) mediumAssuranceHardware (1)

1.3.6.1.4.1.39965.2.1.3 mediumAssuranceHardwareRoaming

trans sped (1.3.6.1.4.1.39965) DirectTrust (2) policies (1) mediumAssuranceHardwareRoaming (3)

MOBILE QCA (Issued by CT-CSSP-CA-A1 / Cybertrust)

1.3.6.1.4.1.39965.3.1.1

1.3.6.1.4.1.39965.3.1.3

MOBILE eIDAS QCA

1.3.6.1.4.1.39965.4.1.1

7.1.7 Usage of Policy Constraints Extension

The DIBCA asserts the policy constraints extension with *inhibitPolicyMapping* and *requireExplicitPolicy* in all cross certificates it issues.
The DIBCA asserts inhibit policy mapping with skipCerts value = 1 when issuing certificates to other Bridge CAs. All other cross certificates have skipCerts = 0. Bridge certification paths will include nomore than two Bridge CAs. In other words, all Bridge – Bridge interoperability is on a bilateral basis.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates may contain policy qualifiers such as user notice, policy name, and CP and CPSpointers.

The Trans Sped PCA must adhere to the Certificate Formats described in this CP.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificate Policy extensions must be marked non-critical.

7.2 CRL Profile

7.2.1 Version Numbers

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

7.2.2 CRL & CRL Entry Extensions

Critical private extensions must be interoperable in their intended community of

use. Section 10 contains the CRL formats.

7.3 OCSP Profile

OCSP requests and responses must be in accordance with RFC 6960. Section 10 contains the OCSP request and response formats.

7.3.1 Version Number

The version number for OCSP requests and responses is v1.

7.3.2 OCSP Extensions

Responses may support the nonce extension.

8. Compliance Audit & Other Assessments

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

8.1 Frequency and Circumstances of Assessments

CAs are subject to a periodic compliance audit, which is no less frequent than once per year for Medium and Medium Hardware assurance levels and once every two years at the Basic assurance level. The periodic compliance audit must be carried out in accordance with the terms of the applicable Issuer Agreement or MOA.

Further, the PMA has the right to require aperiodic compliance audits of Issuer Principal CAs (and, when needed, their subordinate CAs) that interoperate with the DIBCA. The PMA must state the reason for any aperiodic compliance audit.

The PCA, CSAs, CCSs and RAs must 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 DIBCA. The PAA must state the reason for any aperiodic compliance audit and must bear the cost of the audit unless otherwise specified in the respective Issuer Agreement.

8.2 Identity & Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits for security and PKIs, and must be thoroughly familiar with the requirements of the applicable CP. The

compliance auditor must perform such compliance audits as a primary responsibility.

DIRECTTRUST Identity will review the qualifications of the Auditor and reserves the right to reject an audit opinion prepared by an auditor that does not demonstrate adequate experience or competence.

8.3 Assessor's Relationship to Assessed Entity

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

The PMA will determine whether a compliance auditor meets this requirement.

8.4 Topics Covered By Assessment

The purpose of a compliance audit is to verify that a PKI component is complying with the requirements of the applicable CP, CPS the agreement between DIRECTTRUST Identity and the Organization, and any additional MOAs between the Organization and other entities. The audit must include an assessment of the applicable CPS(s) against the Issuer CP, to determine that the CPS adequately addresses and implements the requirements of the CP.

8.5 Actions Taken as a Result Of Deficiency

The PMA may determine that a CA or CSA is not complying with its obligations set forth in this CP and any applicable MOAs. When such a determination is made in relation to the DITA or DIBCA, the PMA may suspend operation of the affected CA until a remediation has been performed. When such a determination is made in relation to an Issuer CA, the PMA may direct the DIBCA OA to cease interoperating with the affected Issuer Principal CA (e.g., by revoking the certificate that the DIBCA had issued to the Issuer Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how a component operates and the requirements of this CP, the Issuer CP, the applicable CPS, any applicable MOAs, or the DIRECTTRUST Identity Standard, the following actions must be performed:

- The compliance auditor must note the discrepancy;
- The compliance auditor must notify the Issuer responsible for the component of the discrepancy. The issuer must also notify DIRECTTRUST Identity promptly; and
- The party responsible for correcting the discrepancy must determine what further notifications or actions are necessary pursuant to the requirements of this CP and the Issuer Agreement, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may take action as described above,.

8.6 Communication of Results

An Audit Opinion Letter, including identification of corrective measures taken or being taken by theComponent, must be provided to the DIRECTTRUST Identity PMA. The Letter must be prepared in accordance with the Compliance Audit Reference Document and must include an assertion from the Issuer PKI that all PKI components have been audited – including any components that may be separately managed and operated. The Letter must identify the CP and CPS used in the assessment,including their dates and version numbers.

Additionally, where necessary, the results must 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 CA certificate issuance and renewal fees must be in accordance with the respective Agreement between the contracting Entities/End User and Trans Sped.

9.1.2 Certificate Access Fees

Trans Sped CA does not charge for access to any certificates.

9.1.3 Revocation or Status Information Access Fee

Trans Sped CA does not charge for access to any revocation or status information.

9.1.4 Fees for Other Services

Trans Sped CA services must be in accordance with with the respective Agreement between the contracting Entities/End User and Trans Sped.

9.1.5 Refund Policy

Any refunds from the Trans Sped CA must be in accordance with the respective Agreement between the contracting Entities/End User and Trans Sped.

9.2 Financial Responsibility

Financial responsibility for the Trans Sped CA must be in accordance with the respective Agreement between the contracting Entities/End User and Trans Sped.

9.2.1 Insurance Coverage

Trans Sped CA must maintain reasonable levels of insurance coverage to address all foreseeable liabilityobligations to PKI Entities, as those entities are described in Section 1.3 of this CP.

9.2.2 Other Assets

Trans Sped CA must also maintain reasonable and sufficient financial resources to conduct operations, fulfill duties, and address commercially reasonable liability obligations to

participants in the DIBCA.

9.2.3 Insurance/warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

Trans Sped CA must maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should reasonably be understood to be confidential,and must treat such information with the same degree of care and security as the Issuer CA treats its own most confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All Subscribers identifying information as defined by local privacy regulations must 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 Entities/End User and Issuer Agreements, and the CPS.

9.4.3 Information not Deemed Private

Information not deemed private must include any information not specifically identified underSection 9.4.2. Information included in the certificates must be deemed not to be private.

9.4.4 Responsibility to Protect Private Information

Trans Sped CAs, collection of PII must be limited to the minimum necessary to validate the identity of the subscriber and conduct its operations under this CP. This may include attributes that correlateidentity evidence to authoritative sources. The RA must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information.

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 Entities/End User and Trans Sped Agreements, and the CPS.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure must be handled in accordance with DIRECTTRUST Identity Privacy Policy, and anyapplicable Issuer internal rules.

9.4.7 Other Information Disclosure Circumstances

Any disclosure must be handled in accordance with DIRECTTRUST Identity Privacy Policy and

Trans Sped Privacy Policy available on Trans Sped public website https://www.transsped.com/files/policy/GDPR%20Information%20TSP%20EN.pdf

9.5 Intellectual Property Rights

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

9.5.1 Property Rights in Certificates and Revocation Information

Subject to any agreements between DIRECTTRUST Identity and its members, Trans Sped CA must retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. For any certificates issued under the DIBCA, DIRECTTRUST Identity grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to a Memorandum of Agreement (or equivalent contractual mechanism) with the relevant Issuer CA.

9.5.2 Property Rights in the CPS

All Intellectual Property Rights in this CP are owned by Trans Sped and/or its licensors. All Intellectual Property Rights in the DITA and DIBCA CPSes are owned by DIRECTTRUST Identity.

9.5.3 Property Rights in Names

As between DIRECTTRUST Identity and Trans Sped CA Applicant, Trans Sped CA Applicant retains all rights, if any, in any trademark, service mark, or trade name of the Trans Sped CA Applicant contained in any Trans Sped CA Application, subject to a non-exclusive, royalty-free, fully paid right and license to use anysuch trademark, service mark, or trade name solely in conjunction with the operation of the DIBCA.

9.5.4 Property Rights in Keys

Ownership of and property rightsin key pairs corresponding to Certificates of Trans Sped CAs and Subscribers must be specified in the applicable CPS of Trans Sped CA regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these key pairs.

Notwithstanding the foregoing, (a) DIRECTTRUST Identity's root public keys and the root Certificates containing them are the property of DIRECTTRUST Identity and (b) each Issuer CA grants to DIRECTTRUST Identity anon-exclusive, royalty-free, fully paid right and license to use any public key or certificate corresponding to such public key solely in conjunction with the operation of the DIBCA.

9.6 Representations and Warranties

Representations and warranties contained in commercial agreements between DIRECTTRUST Identity andother involved parties may be contained in separate documents, including, without limitation, thefollowing:

- Master Service Agreements between DIRECTTRUST Identity and its Members and Issuers.

- Current Member and Issuer Service Orders

The above listed documents may contain additional and/or supplemental representation andwarranties between the parties.

Representations and guarantees contained in trade agreements between Trans Sped and other parties involved may be contained in separate documents, including, without limitation, the following:

• Main service agreements between Trans Sped and its entities and subscribers

• Current service orders for its customers, entities and subscribers The documents listed above may contain additional and / or additional representations and warranties between the parties.

9.6.1 CA Representations and Warranties

DIRECTTRUST Identity represents and warrants that, to its knowledge:

- There are no material misrepresentations of fact in the Cross Certificates known to ororiginating from DIRECTTRUST Identity as a result of approving the Cross-certification Applications or issuing the Cross Certificates,
- There are no errors in the information in the Cross Certificates that were introduced by DIRECTTRUST Identity as a result of (a) approving the Cross-certification Application or issuingthe Cross Certificate or (b) a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- DIRECTTRUST Identity certificates meet all material requirements of this CP, and
- Revocation services and use of a repository conform to the applicable CPS in all materialaspects.

The applicable contractual agreements described in Section 9.6 may include additionalrepresentations and warranties.

DIRECTTRUST Identity Member and Issuer CAs represent and warrant that:

- The CA signing private key is protected and that no unauthorized person has ever hadaccess to that private key;
- All representations made by the DIRECTTRUST Identity Issuer CA in any applicable agreementsare true and accurate, to the best knowledge of the applicable CA;
- If applicable (i.e., if the Issuer CA has issued certificates to a Subscriber), each Subscriber has been required to represent and warrant that all information supplied by theSubscriber in connection with, and/or contained in the Certificate is true;
- If applicable, CAs must maintain an agreement with Affiliated Organizations concerningthe obligations required by this CP; and
- The Cross Certificate and any other certificates issued by the Cross-Certified CA is beingused exclusively for authorized and legal purposes, consistent with this and any other applicable CP or CPS, to the best knowledge of the Cross-Certified CA.

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

In addition to the representation and warranties contained in the DIRECTTRUST Identity Operating Policies, the PCA represents and warrants that it must 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 itcomplies with the stipulations of this policy, and complies with a CPS approved by an appropriate authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

A Subscriber must be required to sign a document (e.g., a subscriber agreement) containing therequirements the Subscriber must meet respecting protection of the private key and use of the certificate before being issued the certificate.

In signing the document described above, each Subscriber must agree to the following:

- Subscriber must accurately represent itself in all communications with the Issuing CAauthorities.
- Subscriber must promptly notify the appropriate CA upon suspicion of loss or compromise ofits private keys. Such notification must be made directly or indirectly through mechanisms consistent with the Issuing CA's CPS.

In signing the document described above, each Subscriber must represent and warrant that:

- The data contained in any certificates issued to the Subscriber is accurate;
- The Subscriber lawfully holds the private key corresponding to the public key identified inthe Subscriber's certificate;
- The Subscriber will protect its private keys at all times, in accordance with this

policy, asstipulated in the certificate acceptance agreements, and local procedures; and

- The Subscriber will abide by all the terms, conditions, and restrictions levied on the use ofthe private keys and certificates.

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

9.6.4 Relying Parties Representations and Warranties

Parties who rely upon the certificates issued under the DIRECTTRUST Identity PKI represent and warrant thatthey must act in accordance with the following provisions:

- Use of the certificate is limited to the purpose for which it was issued, as indicated inthe certificate information (e.g., the key usage extension);
- A check is performed for each certificate in a trust path for validity, priorto reliance;
- Preserve original signed data, the applications necessary to read and processthat data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and must be avoided.

9.6.5 Representations and Warranties of other Participants

9.6.5.1 Repository Representations and Warranties

See Section 2.1.

9.6.5.2 CSA Obligations

A CSA that provides revocation status and/or complete validation of certificates represents andwarrants that it conforms to the stipulations of this CP including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that certificate and revocation information is accepted only from valid CAs;and

9.6.5.3 RSSP Obligations

A RSSP that securely stores and uses roaming credentials when requested by the subscribersrepresents and warrants that it must 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, modificationand destruction at all times; and

- Subscriber private keys are used only when the subscriber appropriately authenticatesto the RSSP and requests the use of their key.

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

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, any agreements between relevant stakeholders may contain disclaimers of warranties (other than any express warranties contained in such agreements or set forthin this CP). TO THE EXTENT PERMITTED BY APPLICABLE LAW, DIRECTTRUST IDENTITY CAS MAY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTIES, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CP.

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN DIRECTTRUST IDENTITY AND ITS MEMBERS, UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY DIRECTTRUST IDENTITY ARE PROVIDED "AS IS", AND DIRECTTRUST IDENTITY, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FORNEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY DIRECTTRUST IDENTITY CERTIFICATES, ANY SERVICES PROVIDED BY DIRECTTRUST IDENTITY, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 Limitations of Liability

Any such limitations are specified in the DIRECTTRUST Identity Operating Policies and the applicable contracting DIRECTTRUST Member and Issuer Agreements. In conformance with EU eIDAS Regulation, the DIRECTTRUST Identity Operating Policies, Section 5.7.3, specify liability limits on individual DIRECTTRUST Identity signed transactions.

9.9 Indemnities

9.9.1 Indemnification Member and Issuer CAs

To the extent permitted by applicable law, each DIRECTTRUST Identity Member and Issuer CA must indemnifyDIRECTTRUST Identity and its contractors, agents, assigns, employees, officers, and directors from and against any third party claims, liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising out of any certificates issued by DIRECTTRUST Identity, including, without limitation, for:

- Falsehood or misrepresentation of fact by the DIRECTTRUST Identity Member or Issuer CA in theapplicable contractual agreements.
- Failure by the DIRECTTRUST Identity Member or Issuer CA to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligentlyor with intent to deceive any party,

- The DIRECTTRUST Identity Member or Issuer's CA's failure to protect the DIRECTTRUST Identity MemberCA private key, to use a Trustworthy System, or to otherwise take the precautions necessaryto prevent the compromise, loss, disclosure, modification, or unauthorized use of the DIRECTTRUSTIdentity Member or Issuer's CA private key, or
- The DIRECTTRUST Identity Member or Issuer's CA's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable contractual agreement between DIRECTTRUST Identity and an Entity CA that is a member of DIRECTTRUST Identity within the DIRECTTRUST Identity PKI may include additional indemnity obligations, but thesewould not apply to cross-certified CAs that are not members of DIRECTTRUST Identity.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, each Relying Party must indemnify DIRECTTRUST Identity and its contractors, agents, assigns, employees, officers, and directors from and against any third party claims,liabilities, damages, costs and expenses (including reasonable attorney's fees), relating to or arising outof the use of or reliance by the Relying Party on any certificates issued by DIRECTTRUST Identity, including, without limitation:

- The Relying Party's improper, illegal, or unauthorized use of a Certificate (including use ofany expired, revoked, or unvalidated Certificate);
- The Relying Party's unreasonable reliance on a Certificate, given the circumstances;
- The Relying Party's use of a Certificate that asserts a "pass-through" policy OID as defined inSection 1.2 of this CP, or
- The Relying Party's failure to check the status of a Certificate on which it relies to determineif the Certificate is expired or revoked.

Any applicable contractual agreement between DIRECTTRUST Identity and a Relying Party within the DIRECTTRUST Identity PKI may include additional indemnity obligations, but these would not apply to relying partiesthat are not members of DIRECTTRUST Identity.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

While this CP may be amended from time to time, it must remain in force until replaced by a newer version or explicitly terminated by a resolution of the Trans Sped Board. For purposesof clarity, termination of any Agreement must not operate as a termination of this CP unless this CP isexplicitly terminated by a separate resolution of the Trans Sped Board of Directors.

9.10.3 Effect of Termination and Survival

As specified in the DIRECTTRUST-Identity Operating Policies and the applicable contracting DIRECTTRUST-Identity Member and Issuer Agreements.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, DIRECTTRUST Identity must use commercially reasonable methods to communicate with cross-certified CAs, taking into account the criticality and subject matter of the communication.

Unless otherwise specified by agreement between the parties, all DIRECTTRUST Identity Member and Issuer CAs must use commercially reasonable methods to communicate with DIRECTTRUST Identity, taking into account the criticality and subject matter of the communication.

Any planned change to the infrastructure of a DIRECTTRUST Identity Member or Issuer CA that has the potential to affect the DIRECTTRUST Identity operational environment must be communicated to the PMA at least two weeks prior to implementation, and any new CA certificates produced as a result of the change provided to the PMA within 24 hours following implementation.

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

9.12 Amendments

9.12.1 Procedure for Amendment

The DIRECTTRUST Identity PMA is responsible for keeping this policy current. Errors, updates, or changes to this CP must be communicated to DIRECTTRUST Identity PKI participants and subscribers. Such communication must include a description of the change, a change justification, and contact information.

Any PMA Member may recommend a change to this CP, which will be referred to the CPWG for review prior to being presented to the PMA for review and vote. Requests for changes may be submitted to the PMA Chair using the *DIRECTTRUST Identity Change Proposal Template.*

The DIRECTTRUST Identity PMA must review the CP at least once every year. Additional reviews may be enacted at any time at the discretion of the PMA or at the request of the DIRECTTRUST Identity Board.

If the CPWG wishes to recommend amendments or corrections to the CP, such modifications must be circulated to the PMA and DIRECTTRUST Identity Board (including, without limitation, all DIRECTTRUST Identity Member and Issuer CAs). Comments from such parties will be collected by the PMA Chair.

The DIRECTTRUST Identity Board of Directors has final authority over the incorporation of modifications in the DIRECTTRUST Identity CP; however, authority has been delegated to the PMA to act on the DIRECTTRUST Identity Board of Directors behalf for maintaining and updating the CP and for processing new applicants for DIRECTTRUST Identity membership. For clarity, it should be noted that the PMA has primary authority and responsibility for the DIRECTTRUST Identity PKI and, under normal circumstances, its decisions are final. The

only situation where the DIRECTTRUST Identity Board would intervene is in a case where the PMA has decided to or not to cross-certify an applicant, and such decision impacts the fiduciary duty of the DIRECTTRUST Identity Board. In these cases, the DIRECTTRUST Identity Board will act as the final decision authority after reviewing all evidence. If the evidence suggests the PMA acted outside of its scope orwithout impartiality, it could result in the PMA recommendation being modified or disregarded.

Notwithstanding the foregoing, if DIRECTTRUST Identity believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the DIRECTTRUST Identity, DIRECTTRUST Identity must be entitled to make such amendments effective immediately upon publication in the Repository. DIRECTTRUST Identity must use commercially reasonable efforts to immediately notify the PMAand Board of Directors (including, without limitation, all DIRECTTRUST Identity Member and Issuer CAs) of such changes.

The PMA must review this CP at least once every year. The PMA, in collaboration with the PAA, must determine if there are any errors, updates, or suggested changes to the CP. The PMA must maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP must be communicated to DIRECTTRUST Identity PKI participants and subscribers as specified in the Certificate Policy Plan. Such communication must 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

Errata, anticipated changes, and the most up-to-date copy of the CP are published online at: https//:www.transsped.ro/repository/

This CP and any subsequent changes must be made publicly available within seven days of approval.

9.12.3 Circumstances under which OID must be changed

The policy OID must 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

9.13.1 Disputes among DIRECTTRUST Identity and Members

Provisions for resolving disputes between DIRECTTRUST Identity and its Members must be set forth in theapplicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

Except as otherwise agreed (e.g., under an agreement described in Section 9.13.1 above), any disputeunder this CP must be resolved by binding arbitration in accordance with the commercial rules or international rules of the Romanian Law.

9.14 Governing Law

Subject to any limits appearing in applicable law, the Romanian Law must govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Romania.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances,decrees, and orders including, but not limited to, (a) restrictions on exporting or importing software, hardware, or technical information or (b) digital identity laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP represents the entire requirements and understanding among the Trans Sped with respect to the DIBCA and supersedes all prior CP versions.

9.16.2 Assignment

As specified in the DIRECTTRUST Identity Operating Policies and the applicable contracting DIRECTTRUST Identity Member and Issuer Agreements.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remainingprovisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder will be construed asa waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

Neither DIRECTTRUST Identity nor any Member or Issuer is liable for any default or delay in the performance of its obligations under this CP if and to the extent such default or delay arises,either directly or indirectly, by any of the following:

Any provision of any present or future law, regulation or order of the United States of America, or any state thereof, or any foreign country, or any subdivision thereof, or of anycourt of competent jurisdiction insofar as such law, regulation or order is applicable to the DIRECTTRUST Identity Member or Issuer,

- By failure of any electrical, communication or other system operated by third parties otherthan DIRECTTRUST Identity or the DIRECTTRUST Identity Member or Issuer and its Third-Party Processor,

- Fire, flood, earthquake, or any act of God, war, terrorist attack or other emergency condition beyond the control of the DIRECTTRUST Identity Member or Issuer, except to the extent that the non-performing DIRECTTRUST Identity Member or Issuer is at fault in failing to prevent or causing such default or delay, and provided that such default or delay cannot reasonably becircumvented by the non-performing DIRECTTRUST Identity Member or Issuer through the use of commercially reasonable alternate plans.

In the event of a force majeure event, the non-performing DIRECTTRUST Identity Member or Issuer is excused from further performance or observance of the obligations affected for as long as such circumstances prevail and such DIRECTTRUST Identity Member or Issuer continues to use all commercially reasonable efforts to recommence performance or observance. Any DIRECTTRUST Identity Member or Issuerso prevented, hindered or delayed in its performance must, as quickly as practicable under the circumstances, notify the other DIRECTTRUST Identity Members and Issuers to whom performance is due by telephone and describe in reasonable detail the circumstances of the force majeure event, the steps being taken to address such event, and the expected duration of such force majeure event.

9.17 Other Provisions

9.17.1 Fiduciary Relationships

As specified in the applicable DIRECTTRUST Identity Member and Issuer Agreements.

9.17.2 Administrative Processes

This English version of this CP is the official and binding document, and any inconsistency between this version and translated versions must be resolved according to the terms and reasonable inferences drawn from this English version.

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.

Global Unique Identifier (GUID) used in certificates shall conform to the RFC 4122 requirements. Since GUID is associated with a card, the same GUID shall be asserted as the UUID in all applicablecertificates and in all applicable other signed objects on the card.

10.1 Trans Sped CA Certificate

The CA uses the following profile

Field	Content
x.509 Fields	
Version	V3
Serial Number	Unique Allocated automatically
Directory String Type Preference	UTF8
Subject Distinguished Name	CN = Trans Sped DIRECTTRUST PCA III OU = Individual Subscriber PCAO = Trans Sped SRL C = RO
Issuer Distinguished Name	CN = Trans Sped DIRECTTRUST PCA III OU = Individual Subscriber PCAO = 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

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Root CA G3		
Validity	2023 – 2038 (15 years)		
Subject	Attribute	Value	Coding
	CN	Trans Sped Mobile eIDAS QCA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 4096 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: TRUE pathLenConstraint: 0	
keyUsage	yes	keyCertSign cRLSign	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository	

subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G3
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g3.p7c
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g3.crl

End User QC

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Mobile eIDAS QCA G3		
Validity	1 year		
Subject	Attribute	Value	Coding
	CN	<Common Name = First name + Last name>	PrintableString
	G	<First name>	PrintableString
	SN	<Last name>	PrintableString
	SER	<Personal Identification Code>	PrintableString
	Title	<Title> **optional**	PrintableString
	OU	<Organizational Unit> **optional**	PrintableString
	O	<Organization> **optional**	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	[RSA Key, 2048 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: FLASE	
keyUsage	yes	digitalSignature nonRepudiation	
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository	
Private CertExtensions	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	

		id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS (0.4.0.1862.1.5) https://www.transsped.ro/repository EN
subjectAltNames	no	Other Name / rfc822-Name = <Email Address>
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Mobile eIDAS QCA G3
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_mqca_g3.p7c [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_mqca_g3.crl

OCSP responder certificate

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Mobile eIDAS QCA G3		
Validity	1 year		
Subject	Attribute	Value	Coding
	CN	Trans Sped Mobile eIDAS QCA G3 OCSP Signer	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 2048 Bit]		
Extension	Critical	Value	
keyUsage	yes	digitalSignature	
extKeyUsage	no	OCSPSigning (1.3.6.1.5.5.7.3.9)	
noCheck	no	NULL (OID=id-pkix-ocsp-nocheck, (1.3.6.1.5.5.7.48.1.5))	

certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Mobile eIDAS QCA G3
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_mqca_g3.p7c

Trans Sped Mobile eIDAS QCA G3 CRL

CRL issuing parameters are:

Customer Root PCA	Value
CRL Issuance Period	6 hours
CRL Grace Period (seconds)	86400 (24 hours)
Automatically generate a new CRL when certificates are revoked (5.2) or Generate CRL based on revocation reason (5.3)	**Checked**
Include Authority Key ID extension in CRL	**Checked (http://www.transsped.ro/crl/ts_mqca_g3.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
Issuer Distinguished Name	Trans Sped Mobile eIDAS QCA G3
This Update	Allocated automatically
Next Update	Allocated automatically

Field	Content
Signing Algorithm	SHA-256 with RSA encryption (1.2.840.113549.1.1.11)

x.509 Extensions	
Authority Key ID	KeyID= 253d8d17bccf969767a6a574e83a80983c7ab633
Revoked Certificate List Entries:	
Certificate Serial Number	
Revocation date	
Revocation Reason Code	

The certificate profile for Medium Assurance Hardware (MAH)

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
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 DIRECTTRUST CP, currently used in** http://www.trustcenter.de/crl/v2/trans_sped_DirectTrust_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**

Customer Root PCA	**Value**
CRL Issuance Period	**6 hours**
Automatically generate a new CRL when certificates are revoked (5.2) **or** **Generate CRL based on revocation reason (5.3)**	**Checked**
Include Authority Key ID extension in CRL	**Checked (http://www.transsped.ro/crl/ts_qca_g2.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
Issuer Distinguished Name	Trans Sped QCA G2
This Update	Allocated automatically
Next Update	Allocated automatically
Signing Algorithm	SHA-256 with RSA encryption (1.2.840.113549.1.1.11)
x.509 Extensions	
Authority Key ID	KeyID=62 b5 7d f9 68 21 a6 0b b4 b6 5a 20 45 4b 4a 70 e0 53 e2 e9
Revoked Certificate List Entries:	
Certificate Serial Number	
Revocation date	
Revocation Reason Code	

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 DIRECTTRUST PCA III OU = Individual Subscriber PCAO = Trans Sped SRL C = RO
Validity	Up to 3 years
Key Algorithm	RSA
Key Length	2048
Signing Algorithm	SHA-256 with RSA
x.509 Extensions	
Key Usage	Critical
Digital Signature	Selected
Non-Repudiation	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
CRL Distribution Point	Yes, Not Critical http://cdp3.com-strong-id.net/CDP/TS-DIRECTTRUST-PCA-III.crl
Authority Information Access	Yes – not critical
Access Method :CAIsuuers	Selected http://aia3.com-strong-id.net/PCA/TS-DIRECTTRUST-PCA-III.p7c
Access Method: Location:OCSP	Selected http://ocs3.com-strong-id.net/TS-DIRECTTRUST-PCA-III
Qualified Certificate Statements	Yes, Not Critical
ETSI	Yes, 160 Bit SHA-1. id-etsi-qcs-QcCompliance Yes - Not Critical id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod(value=10) PdsLocation=hhttps://ca.transped.ro/repository/pds_en.pdf Language=en
SubjectAltNames	Yes, rfc822-Name = (Email Address)

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	0.4.0.1456.1.1.2
Policy URL	NA
Policy Notice	NA

The certificate profile for Medium Assurance Hardware Roaming

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 DIRECTTRUST PCA III OU = Individual Subscriber PCAO = Trans Sped SRL C = RO
Validity	Up to 3 years
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	0.4.0.1456.1.1.2
Policy URL	NA
Policy Notice	NA
CRL Distribution Point	http://cdp3.com-strong-id.net/CDP/TS-DIRECTTRUST-PCA-III.crl
Authority Information Access	Yes – not critical
Access Method :CAIsuuers	http://aia3.com-strong-id.net/PCA/TS-DIRECTTRUST-PCA-III.p7c
Access Method: Location:OCSP	http://ocs3.com-strong-id.net/TS-DIRECTTRUST-PCA-III
Qualified Certificate Statements	Yes, Not Critical
ETSI	i id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod(value=10) PdsLocation=hhttps://ca.transped.ro/repository/pds_en.pdf Language=en
SubjectAltNames	Yes, rfc822-Name = (Email Address)

Role-based Certificate

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	= Subject of Trans Sped Root CA G2	
Validity	2020 - 2029	
Subject	Attribute	Value
	CN	Trans Sped Electronic Seal QCA G2
	OU	LEGAL PERSON CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	30 82 01 0a 02 82 01 01 00 81 82 9f 43 41 f4 92 e3 9c 59 65 70 53 a1 7d cd f0 3e 2f 47 2a 4e 4f d1 43 a3 79 f6 e2 6f 56 0d 21 f3 49 53 3f 0a b8 e0 74 61 89 23 39 c8 e0 0c 09 ce b6 61 18 a1 0b 2b da d0 a0 37 e6 47 6e 4c 6c 93 50 fa 7a be 24 b6 88 56 1b f6 c4 59 bb ce 5b 9b d0 cf d7 d5 61 b5 6e 9a ab 81 85 81 35 b6 87 49 50 e6 27 73 05 ac 5a 15 80 a3 aa 27 2a 2e 14 bc 64 60 33 5a fc 68 47 7a 68 d6 bb b6 10 f4 a2 4e 60 46 1d 78 fc b8 7c 8a 65 a1 85 b5 e8 95 86 41 14 04 47 3c e9 0f 3d 44 1b 98 75 55 3c 4d 82 68 42 47 52 8d f7 09 26 12 7d 79 0f 6d be 3c 5c c0 4b 27 46 eb fe 73 e8 e2 05 e5 ee a3 e8 b8 17 f3 43 28 19 8c 0c ad 12 3f 2f dd b8 4f 71 20 b6 0f 9b 39 ff 97 d8 5b ba 9b dc f0 d6 5a 0f 6e eb 68 fc 70 cd f3 bf f8 10 c5 2f b4 2c c2 1e 28 a9 12 6b f6 8f 5f f4 cc 81 27 86 da 16 a4 f5 df 02 03 01 00 01		
Extension	Critical	Value
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.39965.5.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G2
authorityInfoAccess	no	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

		Alternative Name: URL=http://www.transsped.ro/cacerts/ts_root_g2.crt [2]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl
Thumbprint algorithm	no	sha1

Subscriber Encryption Certificates

Currently not supported

Machine Certificates

Currently not supported

OCSP Responder Certificates

Trans Sped PCA Signed DIRECTTRUST Identity 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 DIRECTTRUST PCA III OU = Individual Subscriber PCAO = 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

Field	Content
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
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* *DIRECTTRUST use see DIRECTTRUST CP at http://www.DirectTrust-Identity.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* *DIRECTTRUST use see DIRECTTRUST CP at http://www.DirectTrust-Identity.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-DIRECTTRUST-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

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

Trans Sped implemented a PKI Repository that provides HTTP protocol access to certificates andCRLs.

11.2 Authentication

If a URL appears in a certificate the repository must allow anonymous, unauthenticated access.

Repositories hosting CA certificates, CRLs, and OCSP services (if implemented) must be publiclyaccessible. Information not intended for modification or public dissemination must be protected.

11.3 Naming

This CP has defined the naming convention.

When a LDAP repository is used:

1. Certificates must be stored in the LDAP Repository in the entry that appears in the certificatesubject name;
2. The issuedByThisCA element of crossCertificatePair must contain the certificate(s) issued by aCA whose name the entry represents; and
3. CRLs must be stored in the LDAP Repository in the entry that appears in the CRL issuer name.

11.4 Object Class

When a LDAP repository is used:

1. Entries that describe CAs must be defined by the organizationUnit structural object class.These entries must also be a member of pkiCA cpCPS auxiliary object classes; and
2. Entries that describe individuals (human entities) must be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson. These entries must also bea member of pkiUser auxiliary object class.

11.5 Attributes

When a LDAP repository is used:

1. CA entries must be populated with the caCertificate, crossCertificatePair,certificateRevocationList, cPCPS attributes, as applicable; and
2. User entries must be populated with userCertificate attribute containing the encryptioncertificate. Signature certificate need not be published to the LDAP Repository.

12. REFERENCES

The Following documents are sources and/or references for this CP:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-03-11
ANSI X9.63-2011	Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, 2011
CHARTER	CertiPath PMA Charter
Directive 95/46/EC	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
EBCA CP	TeleTrusT EBCA European Bridge Certificate Authority, Certificate Policy for members of the TeleTrusT European Bridge CA, Version 2.6, 30/05/2019, https://www.ebca.de/fileadmin/user_upload/190530_TeleTrusT-EBCA_A2_Certificate_Policy_V2-6.pdf
Regulation (EU) No 910/2014	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
FIPS 140-2	Security Requirements for Cryptographic Modules, May 2001 http://csrc.nist.gov/publications/PubsFIPS.html
FIPS 186-4	Digital Signature Standard, July 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
PKCS #12 v.1.1	Personal Information Exchange Syntax Standard, October 2012. http://www.emc.com/collateral/white-papers/h11301-pkcs-12v1-1-personal-information-exchange-syntax-wp.pdf
RFC 4210	Certificate Management Protocol, Adams Farrell et al, September 2005. http://www.ietf.org/rfc/rfc4210.txt.

RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Santesson, Myers et. al., June 2013 http://www.ietf.org/rfc/rfc6960.txt

RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003. http://www.ietf.org/rfc/rfc3647.txt

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper et. al., May 2008 http://www.ietf.org/rfc/rfc5280.txt

13. ACRONYMS & ABBREVIATIONS

This section addresses acronyms and abbreviations used in this CP and not already defined in theDIRECTTRUST Identity System Documentation Glossary.

CA	Certification Authority
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
IETF	Internet Engineering Task Force
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSSP	Remote Signing Service Provider
SHA	Secure Hash Algorithm
DIBCA	DIRECTTRUST Identity Bridge CA
DITA	DIRECTTRUST Identity Trust Anchor
SSL	Secure Sockets Layer
TA	Trusted Agent
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

14. GLOSSARY

This glossary addresses terms used in this CP and not already defined in the DIRECTTRUST Identity SystemDocumentation 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
CA Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and that may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Components, PKI Components	Collective name for Certification Authorities, Certificate Status Authorities (CSAs), Registration Authorities (RAs) and Trusted Agents
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Duration	A field within a certificate that is composed of two subfields; “date of issue” and “date of next issue”.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Immediately	In accordance with an expedient and well defined process.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding signing Private Key. Legal non- repudiation refers to how well possession or control of the private Signing Key can be established.

Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Principal CA	The Principal CA is a CA designated by an Issuer to interoperate with the DIBCA. An Issuer may designate multiple Principal CAs to interoperate with the DIBCA.
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.
Registration Agent	An individual authorized to perform identity proofing on behalf of the PKI. Includes Registration Authorities, Local Registration Authorities and Trusted Agents. Entities certified by a national or state government to perform identity proofing (certified entities) do so on behalf of the RA and are not considered registration agents.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Revoke (a Certificate)	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate Signing Key is certified by another CA, and whose activities are constrained by that other CA (see superior CA).
Superior CA	In a hierarchical PKI, a CA who has certified the certificate Signing Key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	A remote identity proofing process that employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3.

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. [FIPS 140-1]