TRANS SPED

Certification Practice Statement and Certificate Policy for *Qualified Certificates*

Version 4.1, 5th December 2017

Changes history

Date	Version	Description	Author
29th July 2017	4.0	Changes for SAFE-BioPharma cross-certification	Viky MANAILA
5th December 2017	4.1	Extension of validity period for end-user certificates up to 3 years	Viky MANAILA

TABLE of CONTENTS

1 Introduction

Doing business and communicating across public and private networks becomes more and more important in electronic commerce. One requirement of such electronic communication is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. Technically this can be achieved by electronic signatures. The value of electronic signatures increases significantly if the assignment of an electronic signature to an individual is done by an independent and reliable third party. This third party is commonly called a Certification Service Provider (CSP) or Certification Authority (CA). A Certification Authority issues certificates binding a public key to the entity named in the certificate and holding the corresponding private key.

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with the issuance of certificates.

This document specifies the practices of the operation and management of Trans Sped's CAs issuing qualified certificates in accordance with the eIDAS Regulation (910/2014), in accordance with the Romanian Electronic Signature Act (Law No. 455/2001), and in accordance with the European Telecommunications Standards Institute's Technical Specification EN 319 401: **General Policy Requirements for Trust Service Providers**.

It is common practice for a CA to have two documents in place:

- a Certification Practice Statement (CPS) describing the practices which a CA employs in managing certificates (application, issuance, use, and revocation);
- a Certificate Policy (CP) describing the vetting processes and allowing an estimation of the trustworthiness and reliability of certificate contents based on the extent of verification steps undertaken to verify the contents of certificates.

Because all qualified certificates underlie the same regulations and requirements defined in the eIDAS Regulation and in the Romanian Electronic Signature Act, both above mentioned documents (CPS and CP) have been merged into one single document, this CPS/CP.

1.1 Overview

Certificates are used with public key encryption, which is a technique where any participating entity has a key pair. One of these keys is private and must be kept secret; the other is public and is made available for retrieval from a public key directory, much like telephone numbers in a public phone book. Anything encrypted with the private key can only be decrypted with the corresponding public key (and vice versa). This technique can be used to implement digital signatures: the sender encrypts data using his private key, and any recipient is able to verify its integrity by using the corresponding public key available from a public key directory.

A certificate is, in essence, a digitally signed public key. It always contains the name of the holder of the corresponding private key, who is called the subscriber. Since anyone can create a public key with any given name, it is essential to verify that a certificate retrieved from a directory actually belongs to the subscriber named therein, because otherwise signatures might be forged.

A Certification Authority acts as a trusted third party that binds certificates to the indicated entity. A certificate issued by a CA contains the subscriber's name, the name of the CA, the subscriber's public key, and it is signed by the CA.

Trans Sped offers qualified certificates issued in compliance with eIDAS Regulation and Romanian Electronic Signature Act. Qualified certificates may be used to produce electronic signatures which are legally considered as being equivalent to handwritten signatures. As a natural consequence qualified certificates may be issued to individual persons only. The qualified certificates are issued on certified qualified electronic signature creation devices (Secure Signature Creation Devices or HSMs) that meet the requirements of eIDAS Regulation.

To allow an estimation of the trustworthiness of issued qualified certificates and to prove compliance with the eIDAS Regulation in combination with the Romanian Electronic Signature Act, and in compliance with the requirements of ETSI EN 319 401, Trans Sped publishes this CPS/CP describing the procedures used for the issuance of qualified certificates as well as a description how the verification of data contained in a certificate is done.

This CPS/CP describes the structure and practices of Trans Sped. It does neither constitute a declaration of self-escrow, nor does it state legally binding warranties.

This CPS/CP makes extensive use of the vocabulary related to the field of digital signatures and certificates, cryptography and public key encryption, which is referenced in the Glossary (Chapter 10). The glossary also provides the definitions of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

1.2 Identification

SC Trans Sped SRL of 38 Despot Vodă, 020656 Bucharest, Romania (referred to as “Trans Sped” in this CPS/CP), is a Trust Service Provider (TSP) authorized by the Romanian Supervisory and Regulatory Authority [RARS] to issue qualified certificates under the regulations of the Romanian Electronic Signature Act [RESA].

This CPS/CP is available upon request by e-mail or it may be retrieved from http://www.transsped.ro/repository.

1.3 Community and Applicability

This CPS/CP is intended for qualified certificates which:

a) meet the requirements laid down in eIDAS Regulation;

b) are issued by a TSP who fulfils the requirements laid down in eIDAS Regulation;

c) are for use only with secure signature creation devices (SSCD) which meet the requirements laid down in eIDAS Regulation;

d) are issued to the public.

1.3.1 Certification authorities

Trans Sped is a Trust Service Provider that issues qualified certificates under this CPS/CP. Trans Sped operates one or more Certification Authorities (CA) which create and sign qualified certificates for end entities. Trans Sped uses various PKI services where its CAs are hosted in highly secure datacenters.

All equipment for running its PKI services including but not limited to CAs, OCSPs, RA Servers, Server Signing Application (SSA as defined in [CEN/TS 419241]), HSMs enjoy the same controls described in Sections 5 and 6 for physical, personnel, procedural, and technical se-

curity. The location and construction of the facility housing the CAs and equipment is consistent with facilities used to house high value, sensitive information.

1.3.2 Registration authorities

A Registration Authority (RA) works on behalf of a CA. Trans Sped operates an in-house Registration Authority but may as well make use of external service providers as subsidiary RAs responsible for verifying both business information and personal data contained in a subscriber's certificate.

Any subsidiary RA is contractually bound to Trans Sped. A subsidiary RA is registered as registration service provider. The Registration Officers of such a subsidiary RA are individually identified; they are equipped with special Registration Officer (RO) certificates. Only data signed by one of the RO certificates will be accepted by the CA system.

Personal identification of end users applying for a certificate may take place at Trans Sped or at any of the subsidiary RAs used for this purpose.

Personal identification of end users applying for a certificate may also be performed by mobile identification officers operating on behalf of Trans Sped.

1.3.3 End entities

In the context of this document, end entity (or end user) is a synonym for subscriber (or person). It refers to natural persons who use qualified certificates issued by Trans Sped.

1.3.4 Applicability

Technically, all applications in the areas of electronic signatures and secure Internet communication are suitable for use with qualified certificates issued under the terms of this CPS/CP.

This CPS/CP supports certificates:

a) which meet the requirements laid down in [eIDAS];

b) are issued by Trans Sped in compliance with the requirements laid down in [eIDAS];

c) which are for use only with secure signature creation devices (SSCD) which meet the requirements of [eIDAS];

d) are issued to the public.

1.4 Contact details

1.4.1 Specification administration organization

This CPS/CP is administered by Trans Sped's Policies and Practices Board.

Contact person

CPS/CP Administrator
SC Trans Sped SRL
38 Despot Vodă
020656 Bucharest
Romania
Phone:+40 21 210 87 02

Fax: +40 21 211 02 07
E-mail: office@transsped.ro

Person determining CPS suitability

Trans Sped's Policies and Practices Board consisting of Trans Sped executives determines the CPS/CP's suitability.

2 General Provisions

This chapter describes obligations and liability of Trans Sped'sCAs, RAs, subscribers and relying parties. The obligations and liability are governed by eIDAS Regulation, the Romanian Law and mutual agreements made by the parties mentioned above.

2.1 Obligations

2.1.1 CA obligations

Trans Sped provides its certification services for qualified certificates in compliance with this CPS/CP and in compliance with the Romanian Electronic Signature Act and [eIDAS].

Trans Sped implements measures and procedures for providing certification services for qualified certificates as described in § 4 and § 5 of this CPS/CP.

The primary purpose of any Certification Authority is to provide certificate management services (generation, operational use, revocation and expiry) for customers within their respective policy domain(s).

Trans Sped's CAs uses their own key pairs. The private key of CA is used to sign certificates to subscribers.

Trans Sped's CA's keys for the issuance of qualified certificates are generated in a FIPS 140-1/2 Level 3 certified Hardware Security Module (HSM) in a physically secure facility.

Trans Sped's CAs for qualified certificates perform the following functions:

1. Generate its own keys.
2. Operate in an efficient and trustworthy manner and in accordance with this CPS/CP, the Romanian Electronic Signature Act and [eIDAS].
3. Establish subordinate Registration Authorities if necessary.
4. On the receipt of an authenticated certificate application, issue qualified certificates that meet the X.509 certificate standard, the eIDAS and ETSI EN 319 401 requirements, and the requirements of the request.
5. Ensure that the certificates are free from data entry errors and factually correct based on the information known to the CA at the time of issuance.
6. Inform the applicant of the measures needed to increase the security of qualified electronic signatures and to test them reliably.
7. Inform the applicant that a qualified electronic signature has the same effect in legal transactions as a handwritten signature unless otherwise specified by law.
8. Revoke certificates on receipt of authenticated revocation requests, or in compliance with § 3.4 or § 4.5 of this CPS/CP.
9. Post revocation information to its directory services and issue CRLs.
10. Promptly notify the owner of the certificate about the revocation.

In addition, Trans Sped reserves the right to investigate compromise and suspected compromises of private keys, non-compliance or suspected non-compliance with the stipulations

of this CPS/CP in order to protect the integrity of the community of all subscribers, and take actions it deems appropriate based on its findings.

Investigations may include, but are not limited to:

1. Interviews with operational staff of RAs;
2. A review of applicable system logs, operational records and other related files or documents, including e-mails;
3. An audit of operational procedures;
4. An audit of security controls, procedures, and measures;
5. Request for information.

These rights and obligations may be addressed in greater detail in contractual agreements with Subscribers.

2.1.2 RA obligations

An RA is associated with one or more CAs and acts on behalf of its CAs. An RA is responsible for registering applicants. It performs identity proofing and the verification of all certificate data.

In particular the tasks of an RA are:

- Forwarding checked and complete data for certificate issuance and certificate revocation to the CA.
- Identification and authentication of appliants and third parties.
- Information of subscribers about the proper use of qualified certificates.
- Handing over secure signature creation device (SSCD) to applicants and activating certificates.
- Tracking logistics of certificate lifecycle.
- Validation of revocation requests.

Personal identification of applicants for a qualified certificate may take place at any of the subsidiary RAs used for this purpose. Mobile RA Officers may identifiy and authenticate persons at the customer's premises.

An RA Officer must not use his/her private RA keys for any other purpose than those associated with its RA function without the express permission of Trans Sped. The RA must comply with the provisions in this CPS/CP, those in ETSI EN 319 401, and those in the Romanian Electronic Signature Act and eIDAS; this includes, but is not limited to: ensuring that the requirements specified in § 4 CPS/CP are met, and that the controls defined in § 5 and § 6 CPS/CP are provided; keeping subscriber information confidential according to § 2.8 CPS/CP; and performing the authentication procedure as defined in § 3 CPS/CP.

Any RA must have properly qualified and trustworthy employees that are authorized to perform the RA duties. The workstation used for submitting registration information to Trans Sped must not be publicly accessible, and the communication via insecure channels must be properly protected.

Trans Sped reserves the right to prohibit performing RA services on behalf of Trans Sped, if an RA does not conform to the provisions set forth by Trans Sped.

2.1.3 Subscriber obligations

The obligations of the subscribers can be derived from eIDAS or from the Romanian Electronic Signature Act.

It is recommended that subscribers use signature-application components that clearly indicate the production of a qualified electronic signature and enable the subscriber to identify the data to which the signature refers. To check signed data signature-application components are needed that will show:

- To which data the signature refers,
- Whether the signed data are unchanged,
- To which signature-code owner the signature is assigned to,
- The contents of the qualified certificate on which the signature is based, and
- The results of the subsequent validity check of certificates.

2.1.4 Relying party obligations

A relying party shall:

- verify the validity or revocation of the certificate using current revocation status information,
- take account of any limitations on the usage of the certificate indicated to the relying party in the certificate,
- take any other precautions prescribed in agreements or elsewhere.

2.1.5 Repository obligations

Trans Sped will update its repository, consisting of the relevant policies, the directory of downloadable certificates, and the certificate status checking service, within a reasonable amount of time, at least once in 24 hours, to reflect new information concerning the validity and reliability of the certificates issued.

Revocation status information is publicly and internationally available 24 hours per day, 7 days per week. Upon system failure, service, or other factors which are not under the control of Trans Sped, Trans Sped makes best efforts to ensure that the revocation status service is not unavailable for longer than inevitable.

Trans Sped protects the integrity and authenticity of all systems providing certificate status information.

2.2 Liability

2.2.1 CA liability

As a Trust Service Provider issuing qualified certificates to the public, Trans Sped is liable as specified in the Romanian Electronic Signature Act and eIDAS Regulation.

As a Trust Services Provider under the Romanian Electronic Signature Act and eIDAS Regulation, Trans Sped is obliged to make appropriate cover provisions to ensure to be able to meet the statutory obligations for reimbursement of damages caused by an infringement.

2.2.2 RA liability

Like Trans Sped, the RA is only liable for matters that lie in its sphere of influence and responsibility. Any RA operating on behalf of Trans Sped has a contractual agreement with Trans Sped. An entity intending to make claims against an RA should first turn to Trans Sped because

(1) a subscriber has a contractual agreement with Trans Sped, not with the RA, which only acts on behalf of Trans Sped.

(2) a relying party will, in general, not know the RA that committed the act leading to the claim that is made by the relying party.

Trans Sped will investigate facts and, should Trans Sped come to the conclusion that no fault can be attributed to Trans Sped, refer the party making claims to the relevant RA.

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

For both kinds of relying parties, contractual and non-contractual relying parties, the regulations of indemnification of Romanian Law are binding.

2.3.2 Fiduciary relationships

No fiduciary relationship between RA, CA, subscriber or relying party is represented by Trans Sped. Trans Sped does not represent, or act as agent, fiduciary, or trustee of a subscriber or relying party. Trans Sped cannot be bound to any obligation in any way by subscribers or relying parties, and Trans Sped shall make no contradicting representation in any way.

2.3.3 Administrative processes

A certified public accountant performs an audit of Trans Sped's balance once a year to ensure financial integrity and proper business management.

2.4 Interpretation and Enforcement

2.4.1 Governing law

The eIDAS and laws of Romania shall govern the enforceability, construction, interpretation, and validity of this CPS/CP and of the related contracts.

Regulations for providing certification services for qualified certificates are especially defined in [eIDAS] and in the Romanian Electronic Signature Act (Law No. 455/2001).

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

If parts of any of the provisions in this CPS/CP are inoperative or void, this will not affect the validity of the remaining provisions.

2.4.2.2 Survival

Despite the fact that this CPS/CP may eventually no longer be in effect, the following obligations and limitations of the CPS/CP shall survive: § 2.1 (Obligations), § 2.2 (Liability), § 2.3.3 (Administrative processes), § 2.4 (Interpretation and Enforcement) and § 2.8 (Confidentiality).

2.4.2.3 Merger

In case of a merger, Trans Sped shall ensure the continuity and stability of the CA operation with all reasonable means.

2.4.2.4 Notice

Whenever any party wishes to or has to notify any other party with respect to this CPS/CP, such a notice shall be given by digitally signed e-mail or in writing. The latter must be delivered either by certified mail (including return receipt request), or by a courier service confirming the delivery in writing, and it must be addressed to:

SC Trans Sped SRL
38 Despot Vodă
020656 Bucharest
Romania

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

2.4.3 Dispute resolution procedures

It is in the interest of Trans Sped as a Trust Service Provider and trusted third party to resolve any dispute promptly and efficiently. Therefore, any party intending to make claims should contact Trans Sped first, regardless of the nature of the claim.

Dispute resolution procedures relating to disputes between Trans Sped and Customers can be set forth in the agreements between the parties. Dispute resolution procedures relating to disputes between Trans Sped and Subscribers can be set forth in contractual agreements with Subscribers.

In any case of dispute, claim, or controversy in connection with or relating to this CPS/CP or any qualified certificate issued by Trans Sped, Trans Sped can be contacted by e-mail to: office@transsped.ro.

Disputes may also be reported to:

SC Trans Sped SRL
38 Despot Vodă
020656 Bucharest
Romania

2.5 Fees

Trans Sped charges fees for the use of certain services that Trans Sped offers to its Subscribers. An up-to-date list of current fees is available from Trans Sped web site: http://www.transsped.ro/.

2.6 Publication and Repository

2.6.1 Publication of CA information

Trans Sped will publish this CPS/CP at http://www.transsped.ro/repository. Trans Sped's CAs certificates are accessible from the repository as well.

The directory of all accessible and downloadable qualified certificates issued by Trans Sped is available at http://ca.transsped.ro. Qualified certificates are accessible for download only if the certificate holder has agreed to the publication of the certificate.

Certificate Revocation Lists (CRLs) for qualified certificates are available at http://www.transsped.ro/repository.

2.6.2 Frequency of publication

This CPS/CP and any subsequent changes are made publicly available after approval by Trans Sped's Policies and Practices Board.

The CRLs are updated every twenty-four (24) hours. The database providing status information for qualified certificates is updated every time a certificate is released or revoked. Any other information listed in § 2.6.1 is updated every time it is modified.

2.6.3 Access controls

Only authorized personnel is able to publish or modify any information referred to in § 2.6.1.

2.6.4 Repositories

For the location of the certificate repository and the CPS/CP please refer to § 2.6.1.

2.7 Compliance audit

Trans Sped is subject to external audits. Audits are conducted every two years with compliance review in between the compliance audits according to eIDAS Regulation. These include audits pursuant to eIDAS, ETSI EN 319 401 and the Romanian Electronic Signature Act compliance audit. All of these audits require demonstration of a maximum level of security and conformity to documented policies and practices.

In addition, Trans Sped performs internal self-audits. Topics covered by these audits include checks of proper implementation of Trans Sped's certificate policies and extensive checks on key management policies, security controls, operations policy and comprehensive checks on certificate profiles.

Trans Sped reserves the right to perform periodic inspections and audits of any RA facilities to validate that the RA is operating in accordance with the security practices and procedures laid out in the present CPS/CP and in internal documents.

2.8 Confidentiality

Trans Sped keeps information confidential.

Trans Sped's directory of certificates transmits the data stated in the certificate to all requesting entities. Qualified certificates can be retrieved only if the certificate holder has agreed to the publication of the certificate.

Trans Sped collects, processes, and utilizes the personal and organization-related data only as appropriate and necessary for the issuance of a qualified certificate.

Trans Sped will not transmit data contained in certificates to third parties for advertising purposes. Trans Sped does not make any further commercial use of the data obtained in connection with an application for a certificate.

Trans Sped protects all personal and organization-related data which is not included in the certificate against unauthorized access. Trans Sped reserves its right to mention an organization as a customer.

2.9 Intellectual Property Rights

Key pairs corresponding to certificates of Trans Sped's CAs are the property of Trans Sped.

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

This CPS/CP is the intellectual property of Trans Sped.

3 Identification and Authentication

3.1 Initial Registration

In order to obtain a qualified certificate, any subscriber must apply for a certificate, and identify and authenticate himself to Trans Sped.

Trans Sped ensures that subscribers are properly identified and authenticated; and that subject certificate requests are complete, accurate, and duly authorized.

Before a qualified certificate is issued, Trans Sped informs the subscriber of the terms and conditions regarding use of the certificate as regulated in the eIDAS Regulation and the Romanian Electronic Signature Act.

Details of the identification are regulated by the eIDAS Regulation and the Romanian Electronic Signature Act. Submitted documents may be in the form of either paper or electronic documentation.

Trans Sped verifies at time of registration by appropriate means and in accordance with eIDAS, ETSI EN 319 401 and national legislation the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued.
Trans Sped records all the information necessary to verify the subject's identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity as well as the signed agreement with the required content.
Trans Sped collects a physical address or other attributes which describe how the subject may be contacted.

3.1.1 Types of names

The subject and issuer fields of the certificate must be populated with a unique Distinguished Name (DN) in accordance with X.500 standard, with the attribute type as further constrained by RFC 5280.

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

3.1.2 Need for names to be meaningful

Trans Sped will determine the subscriber's DN to make it compliant with common standards, practices and other regulations.

The name should have commonly understood semantics (first and last name, company's name, Internet e-mail address) for the relying party to determine identity of the person and / or organization.

However, the applicant can choose a pseudonym instead of the clear name in the qualified certificate. Trans Sped will issue such pseudonymized certificates; the use of a pseudonym is indicated by the suffix ":PN" in the Common Name field of the certificate.

3.1.3 Rules for interpreting various name forms

Any X.509 certificate issued for private use will have absent Organization and Organizational Unit fields. If one (or both) of these fields are present, the certificate is either intended for commercial use or sponsored by that organization.

3.1.4 Uniqueness of names

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

3.1.5 Name claim dispute resolution procedure

Trans Sped is not responsible for resolving name claim disputes among subscribers. Trans Sped may add, at its own discretion, additional information to a name in order to make it unique among the names of certificates issued by Trans Sped.

3.1.6 Recognition, authentication and role of trademarks

Trans Sped will honor trademark claims that are documented by a subscriber.

3.1.7 Method to prove possession of private key

Prior to the issuance of a qualified certificate CA must ensure and make sure that the requester owns and has it under his control the private key belonging to the public key of the certificate.

If the Subscriber named in a qualified certificate generates its own keys, the Subscriber must use its private key to sign a value and provide that value to the CA issuing the certificate. The CA must then validate the signature using the Subject's public key.

If Trans Sped generates within its premises the private key belonging to the qualified certificate of the Subject – typically on Qualified Electronic Signature Creation Device or on Hardware Security Module, then proof of possession is not required.

3.1.8 Authentication of organization identity

If the applicant is a person who is identified in association with a legal person or other organizational entity in addition to the data in § 3.1.9 evidence shall be provided of its existence. This verification may be carried out by a presentation of a copy of a document, which proves the existence of the organization (current extract of a competent official register in which the organization is listed or a comparable document).

Governmental or administrative authorities must supply documents which reflect their relationship to the next higher entity (e.g. a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer.

The documentation must include:

– full name and legal status of the associated legal person or other organizational entity,

– relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.

3.1.9 Authentication of individual identity

The authentication of an individual entity is performed in compliance with eIDAS, the Romanian Electronic Signature Act, ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

Evidence of the identity of an applicant is checked against an official ID document in combination with the personal appearance of the applicant. Trans Sped may use, with the applicant's consent, personal data collected at an earlier date. The ID document must contain:

– full name (including surname and given names),

– date and place of birth,

– a serial number or other attributes which may be used to distinguish the person from others with the same name.

It is also permitted to check the identity of the applicant indirectly using means which provide equivalent assurance to physical presence (for example if the applicant already possesses a qualified certificate, which implies that the applicant has been identified with personal presence).

If the applicant is a person who is identified in association with a legal person or other organizational entity in addition to the data in § 3.1.8 evidence shall be provided of:

– evidence that the subject is associated with the legal person or other organizational entity,

– authorization from the legal person or other organizational entity to act for the legal person or other organizational entity.

3.1.10 **Non-verified Subscriber Information**
Information that is not verified shall not be included in Certificates.

3.2 Routine Rekey

Rekey means changing the public key for an existing certificate by issuing a new certificate with a *different* public key. The certificate name stays the same. It is different from renewal, which means issuing a new certificate, with an extended validity period, for the *same* public key. (See [RFC4949].) Renewal for qualified certificates is not supported.

Expiration warnings will be issued to subscribers when rekey time arrives. Rekey of certificates before the expiration can be requested by an on-line procedure, which checks the validity of the subject's certificate. The new certificate is issued after the request is approved by Trans Sped. Rekey of the SSCD certificate requires proving the possession of current private key by sending a signed S/MIME e-mail or by performing client-authenticated TLS. Rekey of Server based certificate requires authentication to the Signature Creation Device (See [CEN/TS 419241] for definition) using the same factors as required to activate use the private key.

Rekey of expired certificates follows the same rules as an initial registration. The entire registration process has to be repeated.

If the new certificate is to contain data about an organization new legal documents as indicated in § 3.1 must be presented before rekeying.

3.3 Rekey after Revocation

After a certificate has been revoked, the subscriber must reapply for a new certificate in accordance with § 3.1, since the revoked key pair is ineligible to sign and authenticate a rekey request (see § 3.2).

3.4 Revocation Request

Requests for suspension or revocation of a certificate issued by Trans Sped are authenticated according to one of the following methods:

- personal appearance at the RA;
- with a handwritten signature on a suspension/ revocation form;
- providing possession of the private key;
- successful login to on-line certificate services provided by Trans Sped.

4 Operational Requirements

4.1 Certificate Application

A subscriber submits a certificate application to Trans Sped and follows the procedure described in this CPS/CP or in Trans Sped's descriptions for certificate applications.

Certificate applications are submitted to Trans Sped for processing, the result being either approval or denial.

The key pair may be generated by CA, RA or subscriber. In any case, key generation shall take place in a secure environment. Keys for qualified electronic signatures are always created in secure signature creation devices which are approved to be used for such purposes. Private keys shall not be exportable from such devices.

The subscriber shall sign an agreement with Trans Sped that includes:

- statement that the information provided are correct;
- agreement to the subscriber's obligations;
- consent to the publication of the certificate in repository.

4.2 Certificate Issuance

Trans Sped verifies the accuracy and validity of all data necessary for the issuance of a qualified certificate (compare § 3.1.8 and § 3.1.9). Trans Sped will verify the data contained in the application according to the Romanian Electronic Signature Act and eIDAS Regulation. Trans Sped will either issue the subscriber's certificate upon successful completion of this process or inform the subscriber about any problems or inconsistencies.

Trans Sped generates qualified certificates using the appropriate certificate format, and sets validity periods and extension fields in accordance with relevant standards and legal regulations.

The maximum validity period for an end-user qualified certificate is 3 years from the date of its issuance.

4.3 Certificate Acceptance

On receiving a certificate, subscriber is committed check its contents. If the certificate has any faults that cannot be accepted by the subscriber, the subscriber must inform Trans Sped without any delay. Trans Sped will then revoke the certificate and take the appropriate measures either to refund the certificate price to the subscriber or to reissue a new certificate.

If a certificate is not rejected within 7 day of the reception of the certificate, the certificate is considered accepted.

4.4 Certificate Dissemination

Qualified certificates are made available for retrieval from Trans Sped's certificate repository by third parties only if the subscriber has declared his consent.

4.5 Certificate Suspension and Revocation

A certificate can either be suspended or revoked. If it is not certain whether the corresponding private key has been lost or compromised, the subscriber must suspend the certificate until matters have been clarified. If the private key has been compromised or lost for sure, or if subscriber data represented in the certificate has changed substantially, the certificate must be revoked and the subscriber must reapply.

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

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

Trans Sped provides revocation status information through distribution of Certificate Revocation Lists (CRLs) through repository or using on-line certificate status service (OCSP).

4.5.1 Circumstances for revocation

A certificate is revoked in case:

1. The subscriber or an authorized third party has submitted a revocation request;
2. Trans Sped has learned about false information having been supplied in the certificate application that invalidate the certificate;
3. The Supervisory Body instructs Trans Sped to revoke a certificate in accordance with eIDAS;
4. Trans Sped ceases operation and no other certification service provider continues Trans Sped's certification services.

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

4.5.2 Who can request revocation

The subscriber or his substitute can request revocation.

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

Any entity or third party that confirmed any information contained in a certificate has the right to revoke the affected certificate.

Everybody can inform Trans Sped about the fact that information in a certificate is not or no longer correct. Trans Sped will then check whether a revocation in accordance with § 4.5.1, 2 is adequate.

4.5.3 Procedure for revocation request

There are several ways to submit a revocation request:

1. The subscriber or an authorized third party may request a certificate to be revoked by filling in and signing a revocation form in front of a Registration Officer. Authentication is then provided by the handwritten signature.
2. The subscriber or an authorized third party may request a certificate to be revoked by sending a revocation request in electronic form to Trans Sped. Authentication is then provided by the qualified electronic signature.
3. Using on-line services provided by Trans Sped.

Trans Sped confirms a request for revocation by e-mail or sends a written confirmation, within reasonable amount of time, no later than twenty-four (24) hours after receiving the request.

4.5.4 Revocation request grace period

Trans Sped processes the revocation request, upon confirming that it originated from an authorized entity, as promptly and efficiently as possible. The time needed to revoke the certificate does not exceed twenty-four (24) hours.

4.5.5 Circumstances for suspension

A certificate is suspended in case:

1. The subscriber or an authorized third party has submitted a suspension request;
2. Trans Sped suspects that false information has been supplied in the certificate application that might invalidate the certificate;
3. The certificate has not been paid in respect with the contractual provisions.

4.5.6 Who can request suspension

The subscriber or his substitute can request suspension.

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

Any entity or third party that confirmed any information contained in a certificate has the right to suspend the affected certificate.

Everybody can inform Trans Sped about the fact that information in a certificate might not be correct. Trans Sped will then check whether a suspension in accordance with § 4.5.5, 6 is adequate.

4.5.7 Procedure for suspension request

There are several ways to submit a suspension request:

1. The subscriber or an authorized third party may request a certificate to be suspended by filling in and signing a suspension form in front of a Registration Officer. Authentication is then provided by the handwritten signature.
2. The subscriber or an authorized third party may request a certificate to be suspended by sending a suspension request in electronic form to Trans Sped. Authentication is then provided by the qualified electronic signature.
3. Using on-line services provided by Trans Sped.

Trans Sped confirms a request for suspension by e-mail or sends a written confirmation, within reasonable amount of time, no later than twenty-four (24) hours after receiving the request.

4.5.8 Limits on suspension period

A certificate is suspended for maximum seven (7) days following the suspension request. A certificate may be suspended twice; a third suspension or exceeding the suspension period will result in the certificate being revoked.

The request for certificate reinstatement must not be authenticated using the certificate that is suspended, revoked, expired or is otherwise invalid.

4.5.9 CRL issuance frequency

The CRL issuance frequency shall be at least every twenty-four (24) hours. Trans Sped signing CAs issue CRL every 18 hours with next update of 24 hours. Offline CAs (e.g., Root CA) issue CRLs that have next update of 60 days or less.

4.5.10 CRL checking requirements

Relying parties must, when working with qualified certificates issued by Trans Sped, verify these certificates at all times. This includes the use of CRLs, in accordance with the certification path validation procedure specified in RFC 5280.

4.5.11 On-line revocation / status checking availability

The certificate status can be checked on-line at the certificate status information system. Any changes committed to the status information system are immediately available to any subscriber and / or relying party.

4.5.12 On-line revocation checking requirements

It is the responsibility of the relying party to check the revocation status on-line.

4.5.13 Other forms of revocation advertisements available

None.

4.5.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.5.15 Special requirements regarding key compromise

Depending on whether the subscriber suspects or knows for sure that his private key has been compromised, he is required to request revocation as soon as possible. A subscriber is not relieved from his obligations as a subscriber until he has been notified by Trans Sped of the revocation of the certificate.

5 Physical, procedural, and personnel security controls

Trans Sped is committed to establishing and maintaining state of the art security controls required from CAs and RAs. This chapter provides an outline of such a security controls framework, which reflects the provisions of the Romanian Electronic Signature Act, eIDAS and the ETSI EN 319 401. The respective provisions supplement one another and serve to enhance the overall security controls. All of them require the highest standards of security controls.

For security reasons, however, Trans Sped will not disclose any specific details about the specific measures taken. The documents describing Trans Sped's implementation of security controls are considered non-public.

5.1 Physical Controls

Several layers of physical security controls restrict access to sensitive hardware and software systems used for performing critical CA operations, which take place within a physically secure facility. These systems are physically separated from the organization's other systems so that only authorized employees can access them.

Physical access to the CA systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes access cards in combination with passwords for access. A log is maintained, listing all physical entries to restricted areas.

Private keys used for issuing certificates or signing certificate status responses are not vulnerable to physical penetration. These keys are stored in tamper-resistant secure signature creation devices which are confirmed to fulfill the requirements of the Romanian Electronic Signature Act and eIDAS Regulation. The device is protected from unauthorized access while installed and activated. Physical access controls are implemented to reduce the risk of device tampering even when is not installed and activated. Regular security checks are made to ensure that all these controls function properly.Access to any physical area where information or equipment sensitive to CA operations is located is restricted and monitored by the integrated alarm system.

In addition, sensitive areas are monitored by video cameras.

Any sensitive computer system with regard to certificate issuance runs a secure B1 operating system and cannot be operated through a LAN or WAN, but only from the console. The computer systems providing the directory and repository services may only be administered from the console or via a secure network protocol. Access to sensitive systems requires two persons to be present (or log on) simultaneously.

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment. All CA systems have reasonable precautions taken to minimize the impact of water exposure. All CA systems have industry standard fire prevention and protection mechanisms in place.

Off-site backups are stored in a physically secure manner by a bonded third-party storage company.

Any RA confirming subscriber information and forwarding this information to Trans Sped must provide a secure physical facility for storing registration records and tokens needed to

access RA components. If an RA keeps confidential subscriber information the RA's physical security controls must match those of Trans Sped.

An RA never stores subscriber key information.

5.2 Procedural Controls

Operating procedures are documented and maintained. Procedural controls ensure that no single person acting by him/herself will be able to circumvent the security measure taken.

Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures. Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. This is achieved, for example, by defining different roles so that performing certain essential tasks requires multiple individuals. This "dual control" prevents single persons from being able to forge a certificate.

The following are the trusted roles implemented by the CA:

- Manager - individual with overall responsibility for the CA systems;
- Security Officer - individual with overall responsibility for the security of the service. These individuals manage and monitor events logs and archives discussed in Sections 5.4 and 5.5. They do not hold any other roles;
- System Administrator - individual authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys;
- System Operator - individual authorized to perform system backup and recovery;
- Registration Officer - individual authorized to request or approve certificates, or certificate revocations. These individuals do not hold any other roles;

Auditor - individual authorized to view and maintain CA audit logs. Development and testing facilities are physically separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective action is taken. Users of CA systems are required to note and report observed or suspected security weaknesses and threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are always available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

5.3 Personnel Controls

Trans Sped ensures that all personnel involved in issuing, managing, suspending and revoking qualified certificates, and managing related data and information is integer, trustworthy, and loyal. This includes, but is not limited to, requiring a certificate issued by the police, stating that the individual in question has no criminal record whatsoever. All personnel must

have proper knowledge and experience related to CA operations and must have demonstrated security consciousness and awareness regarding its duties at Trans Sped. Periodic reviews occur to verify the continued trustworthiness of all personnel.

No unauthorized users have access to systems storing sensitive data. All systems storing such data are located inside a protected area. In addition, access to rooms inside the protected area is controlled by an access control system; access to systems is permitted for authorized persons only.

Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. All employees of the organization and, where relevant, third-party users receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. Trans Sped's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

5.4 Audit Logging Procedures

Trans Sped keeps audit trails and system log files that document actions taken as part of Trans Sped's certification services.

At a minimum, each audit record include the following:

- the time of the event;
- the type of the event;

a success or failure indicator for the event, and the identity of the entity that caused the event.

Trans Sped manually or automatically logs the following significant events:

- changes to the audit parameters (e.g. audit frequency, type of event audited);
- attempts to delete or modify audit logs;
- successful logins, unsuccessful login attempts for trusted roles;
- the change of the number of permitted unsuccessful attempts;
- reaching the limit of the permitted number of the unsuccessful login attempts;
- readmission of a user blocked because of the unsuccessful login attempts;
- all events for the entire life cycle of CA keys (generation, loading, saving, etc.);
- events related to the generation and managing of user keys;
- every request related to certificate issuance, re-key, suspension and revocation;
- events related to the request processing;
- certificate issuance or status change;
- generation of a new CRL;
- generation of an OCSP response;

- change of the settings of any component of the CA;
- changing the user roles, rights;
- changing the certificate profile;
- changing the CRL profile;
- security policy settings changes
- installing, clearing (resetting), removing, disposing, an HSM;
- uploading keys, certificates to the HSM.
- access to a CA system component;
- security sensitive files or records read, written or deleted
- system crashes, hardware failures and other anomalies
- firewall and router activity
- CA facility visitor entry/exit

Events in audit logs are time-stamped and digitally signed. Trans Sped uses GPS time signal and a set of NTP servers as time source.

Audits logs and event journals are reviewed regularly and archived to assist in future investigations of security-related incidents. In addition, the summaries of reviews are also archived.

As part of the scheduled system back up procedures, audit trail files are backed up to WORM media. Audit trail files are archived by the system administrator on a regular (at least) weekly basis. Event journals are reviewed at least on a weekly basis by the internal auditors.

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted. These provisions are implemented using the features of a secure B1 operating system requiring the simultaneous login of two persons.

For further details upon internal and external audit requirements and procedures, see § 2.7.

5.5 Records Archival

Audit trails and system log files (see § 5.4) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. Archived audit data concerning qualified certificates are retained as required by the Romanian Electronic Signature Act.

Trans Sped uses internal and external archival to prevent loss of important documents and digital data. The archives are located in separate (internal or external) locations and protected by access-control systems. In general, records concerning qualified certificates are retained at least ten (10) years as required by the Romanian Electronic Signature Act. No single person is able to modify or even destroy archived material, and access to it is strictly restricted.

5.6 Key changeover

Upon the end of the CA's private key's lifetime, a new CA signing key pair and a new CA certificate is generated and all subsequently issued certificates are signed with the new private signing key.

The older, but still valid, CA certificate will be available to verify old signatures until all of the certificates signed using the associated private key have expired. The old private key is also used to sign CRLs and OCSP Responder certificates. Thus, due to rekey a CA can create multiple CRLs, the list on all these CRLs is identical.

Changing CA keys enables Trans Sped to adjust key parameters and cryptographic algorithms, taking into account the suitability of algorithms and parameters in order to compensate advances in science and / or technology. Any new CA key is available by request via e-mail or from Trans Sped's repository at http://www.transsped.ro/repository.

5.7 Compromise and Disaster Recovery

To restore business operations in a reasonably timely manner following interruption to, or failure of critical business processes, business continuity plans have been developed. The business continuity plan defines the period of time that is an acceptable system outage time in the event of a major natural disaster or CA private key compromise. This tolerated outage time depends on the requirements on the availability of a specific service and may range from one hour up to 12 hours.

Backups of essential business information and CA system software are performed daily. Disaster recovery procedures are tested regularly. Documentation concerning details of these procedures is considered confidential.

5.8 CA Termination

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.

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

CA private keys used for issuing qualified certificates and the private keys used for signing revocation status information (CRL, OCSP) are generated in FIPS 140-1/2 Level 3 certified hardware security modules (HSM).

The entire key generation procedure is done under dual control. In addition, the key generation is witnessed and signed off by a third person not involved in the actual key generation.

At no point during the generation process does the private key leave the HSM in unencrypted form, and no unencrypted private key material leaks out.

No copy of any private key is kept permanently on magnetic media in unencrypted form. No private key material is temporarily stored on magnetic media because keys for qualified certificates are generated inside the HSM.

6.1.1.2 Subscriber key pair generation

If the subscriber's key pair generation is done by CA or RA the keys are stored on PIN protected secure signature creation device (SSCD) or HSM. This process takes place in secured premises. No copy of subscriber's private keys is kept by CA or RA so that their misuse is not possible.

If key generation is done by the Subscriber and the certificate request sent to CA, Trans Sped gives then no guarantee on the key generation. Key pairs must be generated on PIN protected secure signature creation device (SSCD) approved by Trans Sped. The PIN protecting the SSCD is strictly personal.

6.1.2 Private key delivery to entity

Private keys generated by CA or RA on SSCDs are delivered to the subscriber by certified personal mail with return receipt. The PIN codes are distributed separately from SSCDs.

Alternatively, the subscriber may collect his SSCD with the private key at CA or RA office.

On subscriber's request the SSCD may also be delivered by any other acceptable form of secure delivery.

6.1.3 Public key delivery to certificate issuer

Subscribers submit their generated public key as an electronic request whose format has to comply with PKCS#10 Certification Request Syntax. Subscriber's requests must be signed using the private key corresponding to the public key to be indicated on the Certificate.

Binding between the certificate request and identity proofing is approved as follows:

- For the initial identity proofing for SSCD, the subscriber appears in person and certificate creation and identity proofing is done at the same time.
- For rekeying for SSCD, the TLS session or S/MIME message use the current private key for subscriber authentication and include the PKCS#10 request.
- For the initial identity proofing as well as rekeying for Secure Server Application, the subscriber must authenticate to their account using the same multiple factor used to invoke the private key.

6.1.4 Public key delivery to users

Methods for CA certificates delivery to relying parties include:

- the publication of the CA certificates on a national Trusted List of Qualified Trust Service Providers;
- the publication of CA certificates on Trans Sped's repository, and by the delivery of a hash of the certificate through a trusted channel at the request.

The subscriber's public key is delivered on the same SSCD used for storing the subscriber's private key if the key pair is generated by CA or RA.

If the subscriber has agreed that his public key certificate being published in Trans Sped's certificate directory, it is available for download as well.

6.1.5 Key sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

Trans Sped's CAs have 2048 bit RSA key pairs. Any key generated on a SSCD and used for a qualified certificate is at least 2048 bit in size. Qualified certificates that are issued after 01/01/2013 shall use 2048 bit key pairs.

No certificates, CRLs or OCSP responses will be signed using RSA 2048 bit that extend beyond 12/31/2030. Also all certificates issued for 2048 bit RSA keys will expire by12/31/2030, otherwise will be revoked.

6.1.6 Public key parameters generation

Permissible algorithms and key parameters for key pairs used for qualified certificates are published by the eIDAS and ETSI. Trans Sped uses only such algorithms and key parameters for qualified certificates that are defined to be adequate.

All current CA keys for the issuance of qualified certificates are RSA keys with 2048 bit and use the hash algorithm SHA-256.

6.1.7 Parameter quality checking

Key pairs should be generated only on approved smart cards or HSMs. Smart cards in use at Trans Sped are formatted to allow only 2048 bit key sizes. The online-application and / or certification mechanisms will check for properly generated certificate requests and their correct format.

6.1.8 Hardware / software key generation

Keys for qualified certificates shall be generated only on secure signature creation devices (SSCD).

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

Qualified certificates issued by Trans Sped must be used according to the X.509 v3 key usage field as set by Trans Sped (see also § 7.1). Qualified certificates may be used for electronic signatures.

6.2 Private Key Protection

Trans Sped ensures the secure management of the CA private keys used for issuing qualified certificates and the private keys used for signing revocation status information (CRL, OCSP) and prevents the private keys disclosure, copy, deletion, modification and unauthorized usage. The CA private keys are stored at a physically secure location, in a secure Hardware Security Modules (HSM).

Access to both the facility and the private keys is protected by access control mechanisms. The private keys can only be activated by two persons and are stored in a FIPS 140-1/2 Level 3 certified HSM. It is never written to any permanent or magnetic storage media.

6.2.1 Standards for cryptographic module

For issuing qualified certificates a FIPS 140-1/2 Level 3 certified HSM (or equivalent) is used.

Also for storing other types of keys Hardware Security Modules (HSM) are used. These modules are certified to be FIPS 140-1/2 Level 3 compliant. Physical access to the HSM is restricted by an access control system. The HSM are used in the FIPS 140-1/2 Level 3 mode.

The HSM can only be activated by two persons simultaneously (dual login).

Unencrypted private keys cannot be extracted from the hardware security module at any point.

6.2.2 Private key (n out of m) multi-person control

The private CA keys are stored in a FIPS 140-1/2 Level 3 certified HSM (or equivalent). In order to activate the private CA keys, two persons are required (see § 6.2.1). No single person has all the activation data needed for accessing any of the private CA keys.

6.2.3 Private key escrow

Trans Sped will not keep end users' private signature keys for qualified certificates.

For certificates issued in compliance with the Romanian Electronic Signature Law any form of key escrow is explicitly prohibited.

6.2.4 Private key backup

CA keys are generated in a FIPS 140-1/2 Level 3 certified HSM.. Trans Sped makes secure copies before putting the CA keys into service. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can only be restored into another mod-

ule. The encrypted keys are copied on WORM media and can only be activated under dual control in a physically secure site.

Keys for end users are generated and stored on a SSCD. These keys cannot be extracted from the smart card and are therefore not backed up.

6.2.5 Private key archival

Key backup (see § 6.2.4) is used for archival purposes. The stipulations on private key back-up apply.

Archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site. Archived keys are never put back into production.

6.2.6 Private key entry into cryptographic module

CA private keys are generated and stored in a FIPS 140-1/2 Level 3 certified HSM. The CA private keys do not exist in plain text outside the cryptographic module. Trans Sped only exports the private key from the HSM for the purpose of making a secure copy. The export and loading of the CA private keys is performed according to section § 6.2.4.

The HSMs are secure handled and tampering protected during shipment, storage and usage.

6.2.7 Method of activating private key

Activating private CA keys used for issuing qualified certificates requires authentication via pass phrases and / or PINs and can only be done under dual control, since the authentication secret is split into two or more shares.

6.2.8 Method of deactivating private key

The private CA key is automatically deactivated after issuing certificates has been completed and the certification application exits or closes the connection to the HSM. Before it can be used again, the HSM must be reactivated.

6.2.9 Method of destroying private key

The destruction of any private CA key must be authorized by the management. It is done under dual control, and it is witnessed and signed off by a third person not involved in the actual destruction of the key.

All copies and fragments of the private key are destroyed at the end of the key pair life cycle.

For private keys used in conjunction with an HSM, the magnetic storage space that carried the private key is wiped multiple times to erase any remaining trace and the hardware token (smart card) needed to activate the key is completely erased or physically destroyed, unless it is needed to activate other private keys. If the storage medium itself is replaced (for example, due to hardware failure), it is physically destroyed.

If a secure cryptographic device is accessible and known to be permanently removed from service, all private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.

If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device. If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

If a private key is stored on an SSCD, the SSCD is destroyed by physically destroying the smart card.

There are no copied or fragments of key material which need to be destroyed because the use of an SSCD guarantees that private keys can never be exported from the SSCD.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Any qualified certificate issued by Trans Sped is stored in the certificate repository and on backup media of the systems that host the certificate repository. In addition, any qualified certificate issued by Trans Sped is stored on the CA system and on the audit files created for the CA system.

6.3.2 Usage periods for the public and private keys

Public and private keys may be used for as long as the validity period of certificate and/or the repository indicate. Once this period has expired, keys are no longer valid.

The use of CA private keys is limited to the period of time in which the used algorithms are regarded as suitable for use; the usage will be stopped after that time.

6.4 Activation Data

Business requirements for access control are defined and documented in an access control policy which includes identification and authentication process for each user, segregation of duties, and number of persons required to perform specific CA operations (meaning, m out of n rule). Activation (and access) data for sensitive keys and assets is under dual control and/or split between at least two disjoint groups of employees.

A formal user registration and deregistration procedure for granting access to activation data for CA information systems and services is followed, and the allocation and use of activation data and privileges is restricted and controlled. Users' access rights are reviewed at regular intervals, and are required to follow defined policies and procedures in the selection and use of passwords.

6.5 Computer Security Controls

A general information security policy document (security policy) is approved by management, published, and communicated, as appropriate, to all employees. This policy is supplemented by detailed policies and procedures for personnel involved in certificate and key management.

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and gives an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.

The Policies and Practices Board (see § 8.1) ensures there is clear direction and visible management support for security initiatives. It is responsible for maintaining the security policy and coordinates the implementation of information security measures.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The development is carried out in accordance with systems development and change management standards.

Trans Sped only uses applications and devices that:

- are commercial off-the-shelf hardware and software, designed and developed by a documented design methodology, or;
- custom hardware and software developed by a reliable party in a controlled environment using structured development methods, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and validation.

New components are first tested within the testing environment before being used in production environment. Production and development environments are totally uncoupled.
Hardware is procured and shipped in a manner to reduce the likelihood of tampering. The hardware is dedicated to PKI and PKI related operations.

6.6.2 Security management controls

Trans Sped has mechanisms and policies in place to control and monitor the configuration and integrity of its systems.

6.7 Network Security Controls

Trans Sped has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.). Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.

Access to all servers is subject to authentication. Users are provided direct access only to the services that they have been specifically authorized to use.

Trans Sped uses GPS time signal and a set of NTP servers as time source for all CA components. Time derived from the trusted time sources is used to establish the time of:

- initial validity time of a subscriber's certificate
- revocation of a subscriber's certificate
- posting of CRL updates
- OCSP responses

6.8 Cryptographic Module Engineering Controls

SSCDs used for storing key material are certified according to ITSEC Level “E4 high” (or equivalent).

The Hardware Security Modules used for storing other CA key material are certified to be FIPS 140-1/2 Level 3 compliant (see § 6.2.1).

7 Certificates, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

Trans Sped issues X.509 version 3 certificates in accordance RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.1.2 Certificate extensions

Trans Sped uses standard X.509v3 extensions. Qualified certificates issued by Trans Sped include the following extension fields, according to ETSI EN 319 412-2 and ETSI EN 319 412-5:

- `basicConstraints` is a critical extension and has the value `false`.
- `keyUsage` is a critical extension and has the value `digitalSignature, nonRepudiation`
- `subjectAltName` is a non critical extension that allows additional identities to be bound to the subject of the certificate such us e-mail address or UPN.
- `authorityKeyIdentifier` is a non critical extension that identifies the CA public key that must be used to verify the subscriber’s certificate.
- `qcStatements` is a non critical extension and has the values:
  id-etsi-qcs-QcCompliance
  id-etsi-qcs-QcSSCD
  id-etsi-qcs-QcPDS pointing to the PKI Disclosure Statement.

7.1.3 Algorithm object identifiers

For qualified certificates Trans Sped only supports such hash function/digital signature algorithm combination which are permissible for the use in qualified certificates.

Current CA keys for the issuance of qualified certificates are RSA keys with 2048 bit and use the hash algorithm SHA-256.

7.1.4 Name forms

See § 3.1.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy Object Identifier

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

Trans Sped QCA G2 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

SAFE CA OID

1.3.6.1.4.1.39965.2.1.1 mediumAssuranceHardware

trans sped (1.3.6.1.4.1.39965) safe (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) safe (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

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued by Trans Sped may contain policy qualifiers such as user notice, policy name, and CPS pointers.

7.1.9 Processing semantics for the critical certificate policy extension

If this extension is critical, the certificate path validation software must be able to interpret this extension (including the optional qualifier), or must reject the certificate.

7.2 CRL Profile

7.2.1 Version number(s)

Trans Sped issues X.509 version 2 CRL's in accordance with RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Certificate status information is also provided via OCSP.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

OCSP requests and responses shall be in accordance with RFC 6960.

Specific administration
Contact information:

TRANS SPED SRL
38 Despot Vodă
020656 Bucharest
Romania
Phone: +40 21 210 87 02
Fax: +40 21 211 02 07
WWW: http://www.transsped.ro
E-Mail: office@ transsped.ro

7.4 Specification change procedures

Trans Sped's Policies and Practices Board has final authority and responsibility for specifying and approving Certification Policy and Certification Practice Statement. It is responsible for performing a (continuous) assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the Certification Policy and Certification Practice Statement.

Trans Sped makes available its public Certification Practice Statement (CPS/CP) to all appropriate subscribers and relying parties. Revisions to this CPS/CP that have significant impact on the users of this CPS/CP must not be made retroactively and shall be published at least two weeks prior to coming into effect.

Revisions to this CPS/CP which are considered to have minimal or no impact on subscribers and relying parties using certificates and certificate status information issued by Trans Sped may be made and posted to the repository without notice to users of the CPS/CP and without changing the version number or date of this CPS/CP.

This version of the CPS/CP is dated April 2017.

7.5 Publication and notification policies

Any time this CPS/CP is amended, and the modified version is approved by Trans Sped's Policies and Practices Board, it is posted to the repository.

7.6 CPS approval procedures

The CPS/CP document is reviewed by and accredited by Trans Sped's Policies and Practices Board before being published in the repository.

8 References

CEN/TS 419241 Security Requirements for Trustworthy Systems Supporting Server Signing

[ETSI] ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319411-1: Electronic Signatures and Infrastructures (ESI);

Policy and security requirements for Trust Service Providers issuing certificates;

Part 1: General requirements

ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;

Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI);

Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412 -5 Electronic Signatures and Infrastructures (ESI);

Certificate Profiles; Part 5: QCStatements

[eIDAS]

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[SB] Supervisory Body

[RESA] Romanian Electronic Signature Act (Law No. 455/2001)

[RFC4949] Internet Security Glossary.

[RFC5280] Internet X.509 Public Key Infrastructure

Certificate and Certificate Revocation List (CRL) Profile

[RFC6960] Internet X.509 Public Key Infrastructure

Online Certificate Status Protocol – OCSP, 2013

[X509] ISO/IEC 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T X.509 Recommendation. See the edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied for X.509v3 certificates.

9 Certificate Profiles

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

9.1 Trans Sped Root CA G2

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	CN	Trans Sped Root CA G2
	OU	Trans Sped CA
	O	Trans Sped SRL
	C	RO
Validity	2016 – 2031	
Subject	Attribute	Value
	CN	Trans Sped Root CA G2
	OU	Trans Sped CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	[RSA Key, 2048 Bit]	
Extension	Critical	Value
basicConstraints	yes	cA: TRUE pathLenConstraint: none
keyUsage	yes	keyCertSign cRLSign
subjectKeyIdentifier	no	automatic

9.2 Trans Sped QCA G2

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	= Subject of Trans Sped Root CA G2	
Validity	2016 - 2026	
Subject	Attribute	Value
	CN	Trans Sped QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	[RSA Key, 2048 Bit]	
Extension	Critical	Value
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G2
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl

9.3 Trans Sped Mobile eIDAS QCA G2

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	= Subject of Trans Sped Root CA G2	
Validity	2016 - 2026	
Subject	Attribute	Value
	CN	Trans Sped Mobile eIDAS QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	[RSA Key, 2048 Bit]	
Extension	Critical	Value
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1] 0.4.0.194112.1.2 [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 G2
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl

9.4 End User QC

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	= Subject of Trans Sped QCA G2	
Validity	Up to 3 years	
Subject	Attribute	Value
	CN	<Common Name = First name + Last name>
	G	<First name>
	SN	<Last name>
	SERIALNUMBER	<Personal Identification Code>
	OU	<Organizational Unit> **optional**
	O	<Organization> **optional**
	C	<Country Code>
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)
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository
qcStatement	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcPDS (location of PKI Disclosure Statements = http://www.transsped.ro/repository)
subjectAltName	no	Other Name / rfc822-Name = <Email Address>
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped QCA G2
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation:

		URL=http://www.transsped.ro/cacerts/ts_qca_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_qca_g2.crl

9.5 End User Mobile QC

Data Field	Value	
Version	v3	
Serial Number	automatic	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	= Subject of Trans Sped Mobile eIDAS QCA G2	
Validity	Up to 3 years	
Subject	Attribute	Value
	CN	<Common Name = First name + Last name>
	G	<First name>
	SN	<Last name>
	SERIALNUMBER	<Personal Identification Code>
	OU	<Organizational Unit> **optional**
	O	<Organization> **optional**
	C	<Country Code>
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)
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository
qcStatement	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcPDS (location of PKI Disclosure Statements = http://www.transsped.ro/repository)

subjectAltName	no	Other Name / rfc822-Name = <Email Address>
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Mobile eIDAS QCA
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_mobile_eidas_qca_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_ mobile_eidas_qca_g2.crl

9.6 OCSP responder certificate

Trans Sped QCA G2 OCSP Signer

Data Field	Value	
Version	v3	
Serial Number	Allocated automatically	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	CN	Trans Sped QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Validity	No longer than 60 days from date of issue	
Subject	Attribute	Value
	CN	Trans Sped QCA G2 OCSP Signer
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	[RSA Key, 2048 Bit]	
Extension	Critical	Value
basicConstraints	yes	Subject Type=End Entity Path Length Constraint=None

keyUsage	yes	Digital Signature (80)
subjectKeyIdentifier	no	Allocated automatically
Authority Info Access	yes	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.transsped.ro/cacerts/ts_qca_g2.crt
OCSP no revocation checking	no	05 00
Enhanced Key Usage	yes	OCSP Signing (1.3.6.1.5.5.7.3.9)
Thumbprint algorithm	no	Sha1
Thumbprint	no	Allocated automatically

9.7 Trans Sped QCA G2 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_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

Field	**Content**
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	

10 Glossary

A

ACTIVATION DATA

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e. g., a PIN or a passphrase).

ASYMMETRIC ALGORITHM

Unlike symmetric algorithms, asymmetric (or public key) encryption algorithms use two different keys for encryption and decryption, where the private key cannot be computed from the public key.

AUTHENTICATION

Authentication refers to the process of confirming either a person's identity or the integrity of information (or both).

B

BLOCK CIPHER

A block cipher is a symmetric algorithm that encrypts larger blocks of text of fixed size, usually 64 bits (equal to eight characters). Examples of block ciphers are IDEA, DES and Triple-DES. See also stream cipher.

C

CA

See Certification Authority.

CERTIFICATE

A certificate is a public key that is signed by a Certification Authority. It binds a public key to the entity named in the certificate (the subject) that holds the corresponding private key. A certificate can be thought of as an electronic ID card. It also identifies the Certification Authority that issued the certificate. The certificate formats most widely used today are PGP and X.509.

CERTIFICATE APPLICATION

In the context of this document, the term "certificate application" refers to all the information a subscriber submits to the Certification Authority in applying for a certificate. This information includes, but may not be limited to, the (digital) certificate request, personal data, a photocopy of his ID card etc. See also certificate request.

CERTIFICATE POLICY

A named set of rules that indicates the applicability of a certificate to a particular community and / or class of applications with common security requirements. While a CPS is prepared by a Certification Authority, any organization may define a Certificate Policy.

CERTIFICATE POLICY DEFINITIONS

The Certificate Policy Definitions (CPD) is a document describing a set of certificate policies that a Certification Authority supports for the issuance of advanced certificates. It is usually available from the repository.

CERTIFICATE REQUEST

In the context of this document, the term “certificate request” refers to the digitally self-signed public key of the subscriber, which may either be encoded in binary or text form. The information such as the Subject DN and public key in the certificate request is to create and sign the certificate. See also certificate application.

CERTIFICATE REVOCATION LIST

A list that contains revoked certificates which the CA has issued. If a CA issues certificates under different Certificate Policies, with a different signing key being used for each policy, multiple CRLs for key will be generated. However, the list of revoked certificates will be identical on all the CRLs.

CERTIFICATION AUTHORITY

A Certification Authority is trustworthy institution that certifies public keys, i. e. issues certificates. For this purpose, the information contained in the public key, in particular the key holder's identity, is verified.

CERTIFICATION PATH

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

CERTIFICATION PRACTICE STATEMENT

A statement of the practices which a Certification Authority employs in issuing certificates. See also Certificate Policy.

CERTIFICATION SERVICES PROVIDER

A Certification Services Provider is a third party that manages any of the services that a Certification Authority generally provides, such as issuing certificates, a directory service, an online certificate status responder or end entity registration.

CERTIFY

To digitally sign another entity’s public key by using one’s own private key.

CIPHER

A cipher is a cryptographic algorithm used for encryption.

CONFIRM

To ascertain through appropriate inquiry and investigation.

CONVENTIONAL ALGORITHMS

See symmetric algorithms.

CORRESPOND

To belong to the same key pair.

CPD

See Certificate Policy Definitions.

CPS

See Certification Practice Statement.

CRL

See Certificate Revocation List.

CRYPTANALYSIS

Cryptanalysis deals with the breaking of encryption algorithms, i. e. decrypting coded messages.

CRYPTOGRAPHY

Cryptography is the science of keeping messages secret.

CRYPTOLOGY

Cryptology is the area of mathematics that combines cryptography and cryptanalysis.

CSP

See Certification Services Provider.

D

DECRYPTION

The process of unscrambling encrypted data.

DH

See Diffie-Hellman.

DIFFIE-HELLMAN

Diffie-Hellman is a secure public key exchange algorithm invented by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman patent expired in 1997.

DIGITAL CERTIFICATE

See certificate.

DIGITAL SIGNATURE (USING RSA ALGORITHM)

A digital signature is a small block of data (hash value) that is encrypted using the sender's private key and appended to the signed data to provide authenticity and integrity. The digital signature is checked using the sender's public key.

DISTINGUISHED NAME

Strictly speaking, a Distinguished Name (DN) is a path through an X.500 directory information tree which uniquely identifies an entity. An X.500 directory tree is a hierarchical structure, and because information like an e-mail address follows no such hierarchy, it should not be part of a DN. Most DNs do, however, contain an e-mail address, and a DN is commonly understood to be comprised of the collection of data fields that make up a standard X.509, i. e., Country (C), State / Province (SP), Locality (L), Organization (O), Organizational Unit (OU), Common Name (CN) and Email. A DN following this scheme might look like the following: /C=US/SP=Washington/L=Seattle/O=My Company, Inc. /OU=Internet Services/CN=John Doe/Email=jdoe@mycompany.com.

DN

See Distinguished Name.

DSA

A public key signature algorithm proposed by NIST for use in DSS that uses a variable key size from 1024 to 3072 bits.

DSS

DSS (Digital Signature Standard) is a digital signature standard proposed by NIST. DSS is used, for instance, by PGP version 5.0 and above.

E

ENCRYPTION

The process of scrambling and rendering data useless for anyone other than the intended recipient.

ENTITY

See person.

G

GENERAL TERMS AND CONDITIONS

Certification Authority services and offers are provided on the basis of the General Terms and Conditions. These are available from the repository.

GTC

See General Terms and Conditions.

H

HASH FUNCTION

A hash function generates a short extract of fixed length (MD5: 128 bits = 16 characters, SHA-256: 256 bits), the hash value, from any given data in such a way that the original data cannot be derived from the extract, and that it is infeasible to construct other data that produces the same hash value. For example, the hash value derived by applying the hash function to the body (the message text) of an e-mail is then used along with the private key in order to digitally sign the e-mail.

I-J

IDEA

IDEA (International Data Encryption Algorithm) is a 64 bit block cipher that uses a 128 bit key. IDEA is considered to be one of the most secure encryption algorithms. It is used (among others) by PGP. Commercial users of PGP that use IDEA as the symmetric cipher have to pay a license fee to the Swiss company ASCOM; non-commercial use is free of charge.

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

ISSUE A CERTIFICATE

The process of a CA signing an end user's public key, thus creating the certificate, and notifying the subscriber of its contents.

K

KEY

A digital code used to encrypt, decrypt, create and verify digital signatures. Keys used for asymmetric algorithms come in pairs, where private key is used to sign the data and the public key is used to verify the data. Symmetric algorithms, however, use the same key for both encryption and decryption, and there is no concept of a digital signature.

KEY PAIR

The set of keys used for asymmetric algorithms. See also key.

KEY RING

The key ring is the file PGP keeps the public (or private) keys in.

L

LAN

Local Area Network.

LDAP

A protocol for accessing on-line directory services. LDAP was defined by the IETF in order to encourage adoption of X.500 directories. The Directory Access Protocol (DAP) was seen as too complex for simple Internet clients to use. An LDAP directory entry is a collection of attributes with a name, called a distinguished name (DN). The DN refers to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "CN" for common name, or "mail" for e-mail address. The values depend on the type. For example, a mail attribute might contain the value "john.doe@company.com". LDAP directory entries are arranged in a hierarchical structure that reflects political, geographic, and / or organizational boundaries.

M

MD5

MD5 is a 128 bit hash function developed by Ron Rivest. It is widely used, and PGP uses it in conjunction with the RSA algorithm..

N

NIST

The NIST (National Institute for Standards and Technology) is a branch of the US Department of Commerce that proposes open interoperability standards.

NSA

The NSA (National Security Agency) is a cryptologic organization of the US government that deals with the development and the cryptanalysis of encryption algorithms.

O

ONE-WAY FUNCTION

See hash function.

P

PASS PHRASE

A pass phrase, just like a pass word, is used to deny unauthorized access to confidential data. A pass phrase consists of several words, punctuation marks and numbers to provide

better security than a simple pass word. A pass phrase is used, for instance, to protect the private key.

PERSON

A human being or any organization capable of signing a document, either legally or as a matter of fact.

PGP

PGP (Pretty Good Privacy), developed by Phillip Zimmermann, is a popular and very widely used application for exchanging secure e-mail and encrypting files. Non-commercial use is free, commercial users will have to obtain a license from PGP Inc.

PIN

Personal Identification Number.

PRIVATE KEY

Of the key pair used in asymmetric algorithms, the private key is the one that must be kept secure by its owner. No one else must have access to this key. Usually, the private key is protected by a pass word or a pass phrase. It is used for decrypting messages sent to the owner of the corresponding public key and for generating digital signatures.

PUBLIC KEY

Of the key pair used in asymmetric algorithms, the public key is the one that is made publicly available, e. g. on a public key server. Its purpose it to encrypt messages sent to the key owner and to verify digital signatures that the latter has made using the corresponding private key. A public key certified by a Certification Authority is a called a certificate.

PUBLIC KEY ENCRYPTION ALGORITHM

See asymmetric algorithm.

PUBLIC KEY EXCHANGE ALGORITHM

A public key method for exchanging session keys. Most public key algorithms are simply used for exchanging secret keys for symmetric encryption algorithms, not for encryption of data. Diffie-Hellman is suitable for key exchange only, while RSA is a public key encryption algorithm.

PUBLIC KEY SERVER

A public key server is a public key directory, much like a public telephone book, which lists user names and their public keys for easy access.

Q-R

QUALIFIED CERTIFICATE

A qualified certificate is a certificate issued in compliance with eIDAS and in compliance with the Romanian Signature Act. A signature produced using a qualified certificate is deemed to be legally equal to a handwritten signature.

RA

See Registration Authority.

REGISTRATION AUTHORITY

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates, i. e., an RA is delegated certain tasks on behalf of a CA.

RELYING PARTY

A recipient of a certificate who acts in reliance on that certificate and / or digital signatures verified using that certificate.

REPOSITORY

A collection of databases for storing and retrieving certificates, CRLs and any other information related to certificates and digital signatures, for example this CPS.

REVOCATION

Revocation is the process of declaring one's public key as no longer valid. This is normally done because its owner can no longer guarantee that he has sole access, and that his private key has not been compromised. By revoking the corresponding public key certificate one aims to prevent others from doing any damage by pretending to be the key's owner. Revoking the public key certificate lets people know that the public key should no longer be used to encrypt any messages or files, and that digital signatures made using this key should no longer be accepted. The revoked public key certificate serial number is then placed on a CRL (Certificate Revocation List) by a Certification Authority so that anyone can check whether a public key certificate is still valid.

RSA

Rivest-Shamir-Adleman (encryption algorithm) **S**

SECRET KEY

See private key.

SECRET KEY ALGORITHM

See symmetric algorithm.

SELF-SIGNED

A public key is referred to as self-signed if it is digitally signed using the corresponding private key.

SESSION KEY

The key used for the symmetric encryption algorithm and exchanged via the public key algorithm. The session key is randomly generated for each exchange of data, i.e. for each session.

SET OF PROVISIONS

A collection of practice and / or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS.

SHA-2

SHA-2 is a hash function developed by NIST that is used in the DSS.

SHA-256

S/MIME

S/MIME (Secure Multipurpose Internet Mail Extension) is a standard suggested by a group of software developers lead by RSADSI that provides encryption and digital signatures for exchanging secure e-mail. S/MIME certificates are based on the X.509 format.

SSL

SSL (Secure Socket Layer) is a protocol developed by Netscape that aims to provide secure data exchange over the Internet. SSL is supported and used by all modern Internet browsers in order to protect the communication and the transfer of sensitive data on the world wide Web through encryption. Unfortunately, the export versions of these applications that are available outside of the United States are limited to a weak 40 bit encryption (instead of 128 bit) due to export restrictions. SSL certificates are based on the X.509 format.

SUBSCRIBER

A person that is the subject named in a certificate and holds the private key corresponding to the public key listed in the certificate.

SUSPENSION

Suspension is the process of placing one's certificate on hold, i. e., declaring it as temporarily invalid. This is normally done because the subscriber suspects that his private key has been lost or compromised. By suspending the corresponding public key certificate one aims to prevent others from doing any damage by pretending to be the key's owner. Suspending the public key certificate lets people know that, for the time being, the public key should not be used to encrypt any messages or files, and that digital signatures made using the corresponding private key should not be accepted at the moment. A suspended public key certificate must either be revoked upon confirming that the private key has indeed been lost or compromised, when it is placed on a CRL (Certificate Revocation List) by the issuing Certification Authority, or the suspension may be lifted, if, for example, the private key has been recovered (i. e., is not lost).

SYMMETRIC ALGORITHM

In contrast to asymmetric algorithms, the key used for decryption (or encryption) can be computed from the other key in a symmetric (or conventional) encryption algorithm. Most of the time both keys are the same.

T

TIME-STAMP

An indication of (at least) the date and time a document was signed and by whom.

TRIPLE-DES

A variant of the DES algorithm where DES (key size 56 bits) is used three times with three different keys. The effective key size is only 112 bits (and not 168 bits, as one might expect).

U-V

USER ID

A PGP data structure containing the key owner’s identity. The commonly used format is “Full name <e-mail address>”, e. g. “John Doe <jdoe@company.com>".

W-Z

WAN

Wide Area Network.

X.509

X.509 is a standard certificate format of the ITU-T (International Telecommunication Union-Telecommunication). It contains the name of the issuer, usually a Certification Authority, information about the key owner's identity and the digital signature of the issuer. Both SSL and S/MIME use X.509 certificate format.