

Policy of the TERENA Academic CA Repository (TACAR)

Version 1.4.4 – 18 July 2008

Editor: Licia Florio (TERENA)

**Reviewers: EuGridPMA
TF-EMC2**

Abstract

This document defines the policy to join TACAR. This version of the document has been modified to redefine the role of the Trusted Introducer, introduced in the previous version of this document.

Document Log

Version 1.4.4:

- Redefinition of TI role

Version 1.4.3:

- Added Trusted Introducer (TI) role
- Improved structure of whole document

Version 1.1/1.2/1.3:

- Improved version of the original TACAR policy

Version 1.0x:

- Original TACAR policy

TACAR Details

TACAR website: <http://www.tacar.org>

TERENA Address: Singel 468 D, 1017 AW Amsterdam, the Netherlands.

Telephone Number: +31 20 530 44 88

Fax: +31 20 530 44 99

<http://www.terena.nl>

Table of Contents

Abstract	2
TACAR Details	2
1 Goal of this Document	4
2 What is TACAR	4
3 Definitions	4
4 Certificates Accepted in TACAR	4
5 How to Join TACAR	4
5.1 Accreditation Process	5
5.2 Registration Process	5
6 Trusted Introducer for TACAR	5
6.1 Who can become the Trusted Introducer?	5
6.2 What are the obligations of a Trusted Introducer?	5
7 Registration of CA Certificates in TACAR	6
8 Updates of the Information in TACAR	7
8.1 Updates of the Accredited People	7
9 Update of the CA Certificates	7
10 Integrity Verification of the CA Certificates and Policies	8
11 Level of Trust to Be Put on the Certificates	8
12 Distribution of the CA Certificates	8
13 TACAR Participant Obligations	8
14 TERENA Obligations	8
15 Policy Update Procedures	9
Annex I: Template Letter of Registration	10
Annex II: Template Letter of Accreditation	15

1 Goal of this Document

One of the key problems linked to the cross-domain use of Public Key Infrastructures (PKI) is how to import the different root CA certificates in user's browsers and other applications in a practical and cost-effective manner. A possible solution that is being applied within the academic community is the use of a process for gathering and verifying academic root-CA certificates, allowing them to be published in one easily downloadable and importable trusted file.

This document defines the procedures to gather the certificates, to store them, publish them and allow for a secure download.

2 What is TACAR

The TERENA Academic CA Repository (TACAR) offers a trusted and centralised location where root CA certificates can be stored and safely downloaded for installation in users' browsers, mailers or other tools where roots certificates are needed.

TACAR does not evaluate the policies adopted by CAs and therefore does not enforce compliance with any particular CA policy or technical minimum requirements in order for a candidate CA to be accepted in, and remain a part of, TACAR.

The only requirement to be part of TACAR is that the applying CA operates for the research and academic community (see Section 4).

3 Definitions

TERENA Officer: A person appointed by TERENA to maintain TACAR.

Trusted Introducer (TI): A person appointed by TACAR community to perform some tasks on the behalf of TERENA Officer.

TACAR Representative: TERENA Officer or Trusted Introducer.

Direct Responsible Person: A person appointed by the applying CA or the applicants CA Host-Organization or the accreditational body to appoint CA administrators

CA Administrator: A person approved to request modification of published CA information.

CA Representative: A CA administrator accredited by the CA to represent the CA in TACAR.

4 Certificates Accepted in TACAR

The root CA certificates that are accepted by TACAR are:

- those directly managed by the TERENA member NRENs;
- or those belonging to a National Academic PKI in the TERENA member countries (NPKIs);
- or those issued by a CA set-up and running to support not-for-profit research projects, in which the academic community is directly involved.

5 How to Join TACAR

The first time the root certificate of the applying CA is to be included into TACAR, the applying CA must provide, during a face-to-face meeting, two copies of:

- the **Registration Letter** (template provided in **Annex I**) ;
- the **Accreditation Letter** (template provided in **Annex II**) .

If PGP personal public keys are provided (see **Accreditation Process**), updated versions of the CP/CPS or a re-generated root CA certificate can be submitted electronically to the TERENA Officer.

5.1 Accreditation Process

The Accreditation letter (see Annex II), which initially must be provided and validated **via a face-to-face meeting between the representatives of the applying CA and a TACAR representative** (see Section 7) designates the direct responsible person who will be in charge of maintaining and updating the accreditation information and at least two CA administrators, who will be in charge of registering, maintaining and updating the root certificate information on behalf of the applicant.

The Accreditation Letter shall contain information about the identity of the contributors and responsible people for the applicant CA. If the applying CA intends to provide updates electronically, PGP personal keys of the people appointed in the Accreditation letter must also be provided.

The accreditation letter must be stamped and signed by all the designated individuals listed in the Accreditation Letter.

5.2 Registration Process

The Registration letter (see Annex I), which also must be submitted and validated **at the initial face-to-face meeting between the representatives of the applying CA and a TACAR representative** (see Section 7) provides information about the CA, its root certificates and its policy.

The Registration Letter shall also be signed and stamped by the CA representatives and by the TACAR representative that collects the information during the first face-to-face meeting.

6 Trusted Introducer for TACAR

To make the entrance into TACAR faster for new applying CAs, a more scalable solution has been agreed upon. This mechanism uses the concept of a Trusted Introducer (TI).

The process of using a Trusted Introducer relies on TERENA's ability to delegate authority for identification and verification to a small number of accredited individuals (the Trusted Introducers).

These individuals will undertake the verification process normally undertaken by the TERENA Officer(s) in charge of TACAR and pass the verified information back to TERENA in a secure manner for inclusion in TACAR.

6.1 Who can become the Trusted Introducer?

Trusted Introducers shall be appointed by TERENA based on an approval by a majority of the existing TACAR community, i.e. those organizations with certificates hosted in TACAR at the time of appointment.

There shall be no more than one Trusted Introducer per designated CA-coordinating body or organisation.

The Trusted Introducer should be a person that regularly meets CA representatives (e.g. at events such as the IGTF, OGF, TERENA meetings).

Once the Trusted Introducer has been appointed, he/she and the TERENA Officer(s) in charge of TACAR will mutually identify themselves and will exchange and sign each others PGP Keys.

TERENA will remove individuals from the list of Trusted Introducers if they are unable to fulfill their role or by request of a majority of the TACAR community or at their own request.

TERENA will keep the list of the Trusted Introducers on the TACAR Website.

6.2 What are the obligations of a Trusted Introducer?

The Trusted Introducer will act on behalf of TERENA, whenever a new applying CA requests to join TACAR and TERENA Officer is not able to attend the face-to-face meeting.

The tasks that the Trusted Introducers will have to follow are:

- Verifying that the representative of the applying CA is entitled to hold such a role.
- Verifying the identity of the representative of the applying CA;
- Gathering and signing the PGP keys of the representatives of the applying CA; the keys must be either published on a PGP server or emailed to the TERENA Officer responsible for TACAR.
- Optionally the TI might also collect all the other documentation; this material can be delivered to

TERENA either via mail or using signed email or during a face-to-face meeting.

7 Registration of CA Certificates in TACAR

A face-to-face meeting between a representative of the applying party and a TACAR representative (either the TERENA Officer or the TI) must be arranged the first time the root CA is provided.

In this meeting:

1. if PGP keys are used, the representative of the applying CA is only required to provide his/her PGP keys; in this case the TI will:
 - a. verify the identity of the applicant (using photo-id documents if needed);
 - b. sign the PGP keys with his/her PGP keys;
 - c. either publish the signed keys or deliver them to the TERENA Officer(s);

The applying CA must then:

- a. post two paper copies of the Registration Letter to TERENA Officer, one of copies will be signed by the TERENA Officer and returned to the applying CA.
- b. mail (using PGP signed email) to the TERENA Officer the following:
 - pdf version of both the Registration Letter and Accreditation Letter (including their detached signatures);
 - CA Root Certificates (PEM format¹) and related detached signature;
 - A PDF version of the Certificate Policy (CP) and its detached signature;
 - A PDF copy of the Certificate Practice Statement (CPS), if available and its detached PGP signature,

Optionally, the applicant may choose to provide all the documentation during the face-to-face meeting with the TI.

2. If no PGP keys are used by the representative of the Applying CA, then:
 - a. the TI will verify the identity of the applicant (using photo-id documents if needed);

The applying CA must then provide the TI with:

- a. Two paper copies of both the registration and accreditation letters; the TI will sign one of each of the copies and give these back to the applying CA.
- b. A CD-ROM containing:
 - CA Root Certificates (PEM format²) included in the Registration Letter and its detached PGP signature by the CA representative (if the PGP method is followed for future electronic updates)
 - A PDF version of the Certificate Policy (CP), if available, and its detached PGP signature by the CA representative (if the PGP method is followed for future electronic updates)
 - A PDF copy of the Certificate Practice Statement (CPS), if available, its detached PGP signature by the CA representative (if the PGP method is followed for future electronic updates)³.
 - A PDF version of the Registration Letter (and its detached PGP signature if the accreditation process is followed and PGP keys are provided).
 - A PDF version of the Accreditation Letter (and its detached PGP signature if the accreditation process is followed and PGP keys are provided).

This process must be repeated for each CA certificate the contributor wishes to include in the repository.

1 **.pem**: With OpenSSL, built with: *openssl x509 -outform PEM -inform DER -in cert.der -out cert.pem*

2 **.pem**: With OpenSSL, built with: *openssl x509 -outform PEM -inform DER -in cert.der -out cert.pem*

3 Note that either the CP or the CPS is mandatory.

8 Updates of the Information in TACAR

A CA registered with TACAR might have several updates in the course of time. Typical updates related to the new CP/CPS documents, regenerated root certificates, different accredited people or more rarely legal changes of the CAs.

8.1 Updates of the Accredited People

There are different cases that might require an update to the Accreditation Letter.

1. If the changes are related to the accredited people, then the Direct Responsible Person as indicated in the Accreditation Letter will be able to add or remove people from the list of accredited individuals for the corresponding CA. In this case:

- a. either a new paper version of the Accreditation Letter must be delivered to the TERENA Officer by the CA representative;
- b. or a PGP signed email with the PDF version of the new Accreditation Letter must be sent to the TERENA Officer.

2. If the changes are about the Direct Responsible Person (i.e. a new person has been appointed), this can only be done sending a new paper version of the Accreditation Letter to the TERENA Officer, signed by the new Direct Responsible Person.

3. If the update involves handing out new PGP keys, then this update must be done during a face-to-face meeting at any meeting where:

- a representative of the CA and a TERENA Officer are present. In this case the TERENA Officer and the owner of the PGP key mutually identify themselves and signed their PGP keys.
- a representative of the CA and the Trusted Introducer are present. In this case the Trusted Introducer and the owner of the PGP key mutually identify themselves and signed their PGP keys. The Trusted Introducer will then deliver the newly received keys to the TERENA Officer(s).

The new accreditation information invalidates any previous accreditation.

9 Update of the CA Certificates

An update of a CA certificate must be done if either:

- The CA certificate in the repository has been revoked, or
- Any data submitted with the CA certificate registration has changed, or
- The organization that manages the CA is abandoning the service, or
- A new certificate for the CA in the repository has been generated.

To update a certificate and/or a CP/CPS, any of the accredited CA administrators must send to the TERENA Officer:

- either a signed e-mail message (using the previously PGP key provided to the TERENA Officer in the accreditation process) to the TERENA Officer indicating the following information, according to the subject of the update:
 - In the case of a CA certificate update: their new certificates and their related SHA-1 and MD5 fingerprints.
 - In the case of a CP/CPS update: Subject and fingerprint of the document(s) to be updated, and the related fingerprint and location of the new one.
 - e-mail message must include the reason for the update. One single e-mail message can include both certificate and policy updates.
- or a CD-ROM containing the following information, according to the subject of the update:
 - In the case of a CA certificate update: new certificates and related SHA-1 and MD5 fingerprint.

- In the case of a CP/CPS update: Subject and fingerprint of the document(s) to be updated, and the related fingerprint and location of the new one.
- The CD-ROM shall be accompanied by a letter signed by one the accredited people which explains the reason for the update.

If not critical, the update can also be performed at any meeting where the representative of the CA and TACAR representative are both present (ie, TF-EMC2/IGTF/OGF etc). In this case the TERENA Officer will collect a CD-ROM by the representative of the CA already registered in TACAR. The CD-ROM shall be accompanied by a printed letter that explain the reason for the update and signed by the representative of the CA that provides the information.

The TERENA Officer will then proceed to update the information on-line.

In case of changes of the CA details such as CA name or CA address or CA telephone number a new version (electronic version digitally signed or paper version) of the Registration Letter must be provided.

10 Integrity Verification of the CA Certificates and Policies

TERENA will provide at the TACAR website the list of all the CA root certificates and their related fingerprints in the repository.

TERENA will also provide a list of MD5 and SHA-1 fingerprints of the CP or CPS linked to each CA certificate included in the repository.

11 Level of Trust to Be Put on the Certificates

As TERENA will provide a copy to any CP/CPS (English version) associated to any CA root certificate in the repository, it is the TACAR user's responsibility to check the respective CA policies before using the CA root certificate.

12 Distribution of the CA Certificates

TERENA shall provide a Web page allowing access to:

- the certificates stored into the repository and their MD5 and SHA-1 fingerprints;
- the CP/CPS associated to any CA certificate in the repository and the MD5 and SHA-1 fingerprints of the policies;
- and the links to the PKI sites if available.

The TACAR certificate Web page shall be publicly available, and the download of the root CA certificates and the related SHA-1/MD5 fingerprint will take place in a secure way.

The secure download makes use of a server X.509 certificate, generated and maintained by the exclusive purpose of securing access to the repository.

13 TACAR Participant Obligations

Any organisation contributing to the TACAR is obliged to timely inform the TERENA Officer of any update in its CA certificates, CP/CPS or any other information related to them in the repository (for example the link to the PKI site, the certificate download location, etc..).

14 TERENA Obligations

TERENA, as responsible of the TACAR, is obliged to follow the identification/authorization protocol described in this document and to make certificates/policies and their updates publicly available.

TERENA will also be obliged to check once a year if the information in the repository is still correct by mailing the contributors.

TERENA will decide on the basis of the information received whether to add or remove certificates to or from

TACAR.

Compliance with the TACAR does not imply that the submitting body has passed any evaluation of its policy, but merely that the root-CA was submitted to TERENA by a bona-fide member of that organisation who identified him or herself to TERENA with a legally-recognised means of personal identification.

TERENA makes no warranty, express or implied, including the warranties of fitness for a particular purpose, or assumes any legal liability or responsibility for the information hosted in the repository.

TERENA refuses any whatsoever responsibility for any (not only monetary) damage, loss, interruption of the service that might happen because of the use of TACAR or to relying parties.

15 Policy Update Procedures

Updates to this document will only be made by unanimous agreement of the organisations participating in the TACAR at the moment of update proposal is presented, according to the following rules:

1. Proposals for update will be sent to the TERENA's contact as indicated on the TACAR website
2. Update proposals will be discussed through e-mail and/or face-to-face meetings among TACAR participants.
3. Once consensus has been reached, the new version of the policy will be circulated among the participant organisations.
4. If no objections to the new version are received within a period of two weeks, it will be considered approved by the TACAR member community. Otherwise, process will be restarted at step 2.

Annex I: Template Letter of Registration

This document is the core of the TACAR procedures. It is the starting point for the inclusion of a CA into the repository. For the first time, it must be delivered, validated, and signed by representatives of both parties (TERENA and the applicant) during a face-to-face meeting. Subsequent updates can be made electronically, as described by the TACAR in the policy.

If this document is accepted by TERENA, all formerly released Letters Of Registration issued by the applying CA are invalid.

If no accredited PGP key is used to sign the electronic versions of this and attached documents the printed paper versions of these documents are the relevant versions. In this case paper versions signed by an accredited signature of all related documents must be provided.

Once the initial *Letter Of Registration* is accepted by TERENA, updates can be send to TERENA via PGP signed e-mail or postal mail as long as the updated document is signed by any currently accredited person for the applying CA. TERENA will verify the signatures against the last received and accepted *Letter Of Accreditation*. TERENA will return signed copy of the received document.

Note: For TERENA's convenience a copy of this as word-processor source and PDF file should be provided on the CD-ROM and if accredited PGP keys are available a detached PGP signature should be placed on the CD-ROM as well.

Letter of Registration

The following institutional organisations, companies and persons hereby announce the following [updated] information to the TERENA Academic CA Repository by way of [electronically signed email | personal meeting with the TERENA Officer]:

Authorisation Information

a. TACAR Representative

TACAR representative can be either a TERENA Officer or one of the Trusted Introducer.

TACAR website: <http://www.tacar.org>

a.1 TERENA Officer Details

Name

Licia Florio

Affiliation

TERENA

PGP key fingerprint: C4EF BC37 9E0F 8A21 9B92 D473 1800 4F4A 2777 07CC

TERENA Address: Singel 468 D, 1017 AW Amsterdam

Phone number: +31 20 530 44 88

Fax number: +31 20 530 44 99

TERENA website: <http://www.terena.nl>

a.2 Trusted Introducer Details

Name:

Affiliation:

PGP key fingerprint:

b. CA Representative

Name

<Firstname Lastname, Position>

Affiliation

<e.g. CA Name>

Meeting Location and Date

Name

<Meeting description>

Date

<date>

Location

<Location name>

Organisation and Applying CA

Organisation Name

(The name of the organisation the CA belongs to or is managed by)

<Organisation Name>

Applying CA

(Legal name of the CA)

Name CA is known under

<CA Name>

Address

<full postal address>

<full physical address>

Phone / Fax

Phone: <+999999999999>

Fax: <+999999999999>

Website

<http://www.ca.net/>

E-Mail Address

<ca@ca.net>

Administrative Contact Person(s) (within the CA)

<Firstname Lastname, Position>

<Firstname Lastname, Position>

Registered Root Certificates

The following list of certificates is a complete list of all X.509 root certificates belonging to the named applying CA that are presented in the TERENA Academic CA Repository. If this document is updated **all** certificates that are going to be listed in the root cert store have to be listed in the sections below. [To add more than one root certificate duplicate the complete following section and change as needed.]

Root Certificate 1 – <CA certificate hierarchy name / ID>

Certificate Download Points

List of URLs to download certificate and related information.

Type: <X.509v3>

- Mime-Type: <application/x-x509-ca-cert>
<http://www.ca.net/...../ca.der>
- Overview page for this certificate (optional)
<http://www.ca.net/.../ca.html>

Subject (DN)

(add/remove components as needed)

C=

ST=

L=

O=

OU=

CN=

Email=

Validity

(e.g. date and time, timezone)

Valid not before:

Valid not after:

Fingerprint

SHA-1:

MD5:

Key Type

(e.g. RSA)

<type>

Key Size

(e.g. 1024 bit, 2048 bit)

<length>

CRL Distribution Points (optional)

CRL download URL:

- Mime-Type: <application/pkix-crl>
<http://www.ca.net/...../ca-crl.crl>
- Overview page
<http://www.ca.net/...../crls.html>

OCSP (optional):

<OCSP responder URL>

Directory Service (optional)

LDAP (optional): <LDAP server and DIT entry point>

HTTP (optional): <URL>

[Either a policy (CP) or a certification practice statement (CPS) are mandatory to provide]

Policy (CP)

Name

<policy name or ID>

URL (HTML)

<http://www.ca.net/...../policy.html>

URL (PDF)

<http://www.ca.net/...../policy.pdf>

Fingerprint (of PDF)

SHA-1:

MD5:

Certification Practice Statement (CPS)

Name

<CPS name or ID>

URL (HTML)

<http://www.ca.net/...../cps.html>

URL (PDF)

<http://www.ca.net/...../cps.pdf>

Fingerprint (of PDF)

SHA-1:

MD5:

Final Statement

The information given above is correct and in conformance with the latest TERENA Academic CA Repository policy as of today. The representative of the applying CA is an accredited staff member as of the latest *Letter of Accreditation* issued by the applying CA.

The following items are attached to this document:

(all electronic versions of the documents are provided for TERENAs convenience)

- 1 CD-ROM medium with the following documents / files regarding this letter:
- Root Certificate 1. **At least one of the following formats (and the corresponding detached signature) shall be included, although including all of them is strongly recommended.**
 - ca-cert.pem X.509 certificate file (PEM format)
 - ca-cert.pem.sig detached PGP signature for ca-cert.pem (if PGP keys are provided)
 - policy.pdf policy (CP)
 - policy.pdf.sig detached PGP signature for policy.pdf.sig (optional)
 - cps.pdf certification practice statement (CPS) (if available)
 - cps.pdf.sig detached PGP signature for cps.pdf.sig (optional)
- Letter-Of-Registration.doc
- Letter-Of-Registration.doc.sig detached PGP signature of Letter-Of-Registration.sxw (optional)
- Letter-Of-Registration.pdf (optional, recommended)
- Letter-Of-Registration.pdf.sig detached PGP signature of Letter-Of-Registration.pdf (optional)

For the applying CA:

Location:

Date:

Signatures:

<Firstname Lastname CA Representative>

Applying CA Organisational crest:

For TERENA:

I, the TACAR representative checked the identity documents of the bearer of this letter, <Firstname Lastname>, the applying CA's representative. The identity documents and signature matches the ones stated in the most current *Letter Of Accreditation*.

Location:

Date:

Trusted Introducer Signature:

<Firstname Lastname>
.....

TERENA Officer Signature:

<Firstname Lastname>
.....

TERENA Organizational crest:

Annex II: Template Letter of Accreditation

This document names the complete list of accredited persons for the applying CA. No other or formerly accredited person if not named in the this *Letter Of Accreditation* shall be accredited any longer for the applying CA.

If this document is accepted by TERENA, all formerly released Letters Of Registration issued by the applying CA are invalid.

If no accredited PGP key is used to sign the electronic versions of this and attached documents the printed paper versions of these documents are the relevant versions. In this case paper versions signed by an accredited signature of all related documents must be provided.

Once the initial *Letter Of Accreditation* is accepted by TERENA, updates of CA administrators must be send to TERENA via postal mail. The updated document shall be signed by any currently accredited person for the applying CA. TERENA will return signed copy of the received document.

Note: For TERENA's convenience a copy of this letter as word-processor source and PDF file should be provided on a CD-ROM and if accredited PGP keys are available a detached PGP signature should be placed on the CD-ROM as well.

Letter of Accreditation

The following institutional organisations, companies and persons are hereby accredited to the TERENA root certificate collection schema. The applying party is completely responsible for the accuracy of this information and for maintaining and updating this record with the responsible TERENA officer. The applying party is especially responsible to add or remove people from the list of accredited people in regards to the applying CA. If the applying party fails to these mandatory procedures, TERENA or TERENA's officer shall not be responsible for any loss, damage or costs arising through this fact in any case to any individual or organisation.

Organisation and Applying CA

Organisation

(The name of the organisation the CA belongs to or is managed by, e.g. NREN, Ministry or Assocoation, etc.. Not to mix up with the 'Hosting Organisation", see below)

Name

<Organisation Name>

Address

<full postal address>

<full physical address>

Phone / Fax

Phone:

Fax:

Website

<<http://www.nren.net/>>

Administrative Contact Person

(in e.g. the NREN)

<Firstname Lastname, Position>

Applying CA

(Legal name of the CA)

Name

<CA Name>

Address

<full postal address>

<full physical address>

Phone / Fax

Phone:

Fax:

Website

<http://www.ca.net/>

E-Mail Address

<ca@ca.net>

Administrative Contact Person(s) (within the CA)

<Firstname Lastname, Position>

Applying CA Host-Organisation

(The host organization of the applicant CA)

Name

<Organisation Name>

Address

<full postal address>

<full physical address>

Phone / Fax

Phone: <+999999999999>

Fax: <+999999999999>

Website

<<http://www.ca-host-org.net/>>

Administrative Contact Person

(person the CA staff reports to, head of CA)

<Firstname Lastname, Position>

Accreditational Body

(The person/people on whose order the CA staff are performing their jobs, e.g. teamlead, project leader, head of department etc, person the CA staff reports to)

Name

<Organisation name>

Address

<full postal address>

<full physical address>

Phone / Fax

Phone:

Fax:

Website

<<http://www.accreditation-body-org.net/>>

Direct Responsible Person

(the person the head of CA reports to)

Name

<Firstname Lastname, Position>

E-Mail address

<mail@domain>

PGP-Key (optional)

User-ID: <Name <mail@domain>>

Key-ID: <0x99999999>

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: <Alg> / <Length>

Fingerprint: <Hex Fingerprint>

Preferred PGP-server URL (optional): <<http://keyserver.net:11371/>>

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: <Name>

Certifying CA (optional)

User-ID: <CA Name <ca@domain>>

Key-ID: <0x99999999>

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: <Alg> / <Length>

Fingerprint: <Hex Fingerprint>

Preferred PGP-server URL (optional): <<http://keyserver.net:11371/>>

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: <Name>

Accredited CA Staff

(people responsible for maintaining the information in the repository)

The following list is the complete and entire list of all accredited CA staff. The accreditation body is defined in Section *Accreditational Body*.

People

(all CA staff including head of CA if not already the direct responsible person, person who is meeting with the TERENA Officer)

CA Administrator 1 - <FirstName Lastname>

Name

<Firstname Lastname, Position>

E-Mail address

<mail@domain>

PGP-Key (optional)

User-ID: <Name <mail@domain>>

Key-ID: <0x99999999>

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: <Alg> / <Length>

Fingerprint: <Hex Fingerprint>

Preferred PGP-server URL (optional): <http://keyserver.net:11371/>

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: <Name>

Certifying CA (optional)

See certifying CA from above.

CA Administrator 2 – <Firstname Lastname>

Name

<Firstname Lastname, Position>

E-Mail address

<mail@domain>

PGP-Key (optional)

User-ID: <Name <mail@domain>>

Key-ID: <0x99999999>

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: <Alg> / <Length>

Fingerprint: <Hex Fingerprint>

Preferred PGP-server URL (optional): <http://keyserver.net:11371/>

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: <Name>

Certifying CA (optional)

See certifying CA from above.

Final Statement

The person named above, i.e. <List of Firstname Lastname> are affiliated to the applying CA. They are commissioned, authorised and mandated to maintain and update the accreditation information as stated in this letter for the applying CA as well as register, maintain and update the root certificate information as stated in the *Letter Of Registration* presented to TERENA. Above named persons cross checked all information given in this letter, especially names, identity proof numbers, PGP-key IDs and fingerprints. We have read and understood the policies and procedures defined by TERENA's root certificate collection schema regarding the certificate store and we are adhering to them. The above information is correct as of signing date of this letter.

The following items are attached to this document:

- 1 CD-ROM with the following documents / files regarding this letter:
 - PGP keys (optional)
 - <file-name.asc> <Firstname Lastname> of all accredited persons
 - <file-name.asc> CA for above key(s)
 - <Letter-Of-Accreditation.doc>
 - <Letter-Of-Accreditation.sxw.sig> detached PGP signature of <Letter-Of-Accreditation.sxw> (optional)
 - <Letter-Of-Accreditation.pdf> <Letter-Of-Accreditation.pdf.sig> detached PGP signature of <Letter-Of-Accreditation.pdf> (optional)

For the applying CA:

Location:

Date:

Signatures:

<Firstname Lastname Direct Responsible Person>
<Firstname Lastname CA Administrator 1>
<Firstname Lastname CA Administrator 2>

Organizational crest:

For TERENA:

I, the TACAR representative, checked the identity documents of the bearer of this letter, <Firstname Lastname>, the applying CA's accredited representative. The identity documents matches the ones stated above.

Location:

Date:

Trusted Introducer Signature:

<Firstname Lastname>
.....

TERENA Officer Signature:

<Firstname Lastname>
.....

TERENA Organizational crest: