TERENA Academic CA Repository (TACAR)

Issuing date:

Version: 2.0

Authors: L. Florio, R. Karlsen-Masur, M. Sova

Document Revision History

Version	Date	Description of change	Person
1.4.4	July 2008	Latest version issued	L Florio
2.0	01. September 2011	Draft version for approval	L. Florio, R. Karlsen-Masur, M. Sova

TACAR Details

TACAR is a TERENA trademark.

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

Contact: tacar-admin@terena.org

TERENA Address:
TERENA
Singel 468 D,
1017 AW Amsterdam, the Netherlands.
Telephone: +31 20 530 44 88
Fax: +31 20 530 44 99
http://www.terena.org

1 Table of Contents

1 Introduction

This document defines the TACAR Policy that is the set of procedures to gather Trust Anchors, to store them, publish them and securely download them.

2 TACAR Purpose

The TERENA Academic CA Repository (TACAR) is a trusted repository, operated by Transeuropean Research and Education Network Association (TERENA) to support, securely store and distribute cryptographic public keys used for digital signing (e.g. Certification Authority (CA) certificates), also called Trust Anchors (TA). TACAR offers three main functionalities:

- reliable distribution of TAs,
- identification of TAs' owners and
- classification of TAs into categories of equivalent policies

TAs accepted by TACAR are:

- those managed by a National Research and Education Network (NREN);
- those operated to support non-profit research projects, in which the academic and/or the eScience community is directly involved.
- those TAs needed to support the building of certificate validation paths from above TAs to a root CA certificate

3 TACAR Definitions, Roles and Responsibilities

This section describes the roles foreseen in TACAR and their related responsibilities.

3.1 Trust Anchor

Trust Anchors (TAs) are cryptographic public keys used for digital signing of other public keys and some additional meta data associated with those public keys (e.g. X.509 digital certificates of Certification Authorities (CAs)) or other data.

3.2 Relying Party (Consumer)

A Relying Party (RP) is an entity that relies on certificates and/or digital signatures issued by the TAs, which are registered with TACAR, for authentication or signature verification purposes.

3.3 TA Owner

A TA Owner is a person authorised to:

- register one or more TAs with TACAR;
- modify the information related to his/her published TA(s);
- request that his/her own TA(s) are removed from TACAR.

3.4 Trust Profile

A Trust Profile (TP) is a set of requirements from RPs in regards to the quality of identity assertions and vetting procedures as well as the supporting assertion infrastructure; TPs are defined by the CA-coordination bodies (see section 3.5) TACAR works with.

3.5 CA-coordination body

A CA-coordination body, typically a Policy Management Authority (PMA), is a body that defines TPs on behalf of RPs and accredits CAs under these TPs. A CA-coordination body nominates Trusted Introducers, see section 3.6 and Category Managers, see section 3.8.

3.6 Trusted Introducer

A Trusted Introducer (TI) is a person appointed by TERENA based on the nomination put forward by the CA-coordination bodies or organisations that use TACAR.

TIs are responsible to securely relay verified authentication information (such as PGP public keys, X.509 user certificates or samples of handwritten signatures) about TA Owners to the TACAR Administrator.

3.7 TACAR Category

TACAR Categories map TP and are used to classify and list the registered TAs that are accredited under such specific Trust Profile.

3.8 Category Manager

A Category Manger (CMs) is a person appointed by TERENA based on the nomination put forward by the CA-coordination bodies TACAR works with. CMs are responsible for:

- assigning TAs to the appropriate TACAR Category, typically as a result of an accreditation process performed by a CA-coordination body;
- adding a new TACAR Category, whenever CA-coordination bodies request a new one;
- renaming existing category whenever CA-coordination bodies request to do so.

3.9 TACAR Administrator

A TACAR Administrator is a person appointed by TERENA to operate TACAR. The TACAR Administrator is responsible for:

- registering/resigning TA Owners;
- registering/resigning TIs;
- registering/resigning CMs;
- registering/deleting TACAR Categories;
- deleting TAs from TACAR;

4 TA Owner Registration and Resignation

Any new TA Owner is required to register himself/herself with TACAR. The registration process involves the following steps:

- registering the TA Owner's authentication details (e.g. PGP public key or X.509 user certificate) during a face-to-face meeting with the TI or with the TACAR Administrator;

- filling in the registration letter (see Annex I) and deliver it to the TACAR Administrator;

The TACAR Administrator will:

- verify that the TA Owner is listed in the registration letter; and
- create an entry in TACAR for that TA Owner.

Once TA Owners are registered, then they can access the TACAR website to register/update their TA(s) and the related information.

A TA Owner will be resigned:

- if requested by the TA Owner, or
- per request of his/her employer.

For a TA that has no TA Owner associated with it, the TACAR Administrator removes that TA from TACAR.

5 Registration, Modification and Deletion of a TA in TACAR

If TA Owners are new to TACAR, then the TA Owners are requested to register themselves with TACAR, see section 4.

A registered TA Owner can:

- identify himself/herself to the TACAR website[1] to enter the data related to his/her TAs or update the information related to his/her TAs;
- use his/her pre-registered authentication information to sign the emails that are automatically generated by the TACAR system in the TA Owner's email client;
- send the digitally signed email to the TACAR Administrator;

The TACAR Administrator will

- validate the digital signature to authenticate the TA Owner's request;
- approve or deny the request based on the authentication;

To delete an existing TA from TACAR, the TA Owner should send a request to the TACAR Administrator in the form of a signed email; the TACAR Administrator upon successful verification of the request will proceed to remove the TA.

6 Category Manager Registration and Resignation

The CMs are appointed by a CA-coordination body. Each CA-coordination body can nominate a number of CMs. It is recommended to have a reasonable but low number of CMs to cover for absence or unavailability of a single CM. The the TIs and TACAR Administrators are also CMs. CMs have (authenticated) access to the TACAR system to assign the matching TACAR Category to TAs.

CMs will be resigned:

- upon CM's request,
- on request by the main stakeholder of the TACAR Category, i.e. the CA-coordination body,
- upon TERENA's request.

[1] https://www.tacar.org/user/identify

7 Trusted Introducer Registration and Resignation

TIs are appointed by TERENA based on the nomination put forward by the CA-coordination body or organisation that use TACAR.

There shall be a reasonable low number of TIs per designated CA-coordination body which best fit the geographic distribution and presence of the CA-coordination body.

The first time a new TI is appointed, the TI and TACAR Administrator will exchange validated authentication information (e.g. PGP public key or X.509 user certificate) at the earliest opportunity a face-to-face meeting can be organised.

TIs will be resigned:

- upon TI request,
- on request by the main stakeholder of the TACAR Category, i.e. the CA-coordination body,
- upon TERENA's request.

The list of the TI is maintained on the TACAR website.

8 TERENA Obligations

TERENA, as responsible of TACAR, shall follow the identification/authorization procedure described in this document and shall ensure that TACAR website is reachable at any moment.

TERENA will decide on the base of the information got 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 Trust Anchors were 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, and interruption of the service that might happen because of the use of TACAR or to relying parties.

9 TACAR Policy Update Procedures

Updates to this document will only be made by 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 TACAR contact email address as indicated in this document;
2. Update proposals will be discussed through email and/or face-to-face meetings among the TACAR Administrator and the CA-coordination bodies that use TACAR;
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 - Registration Letter

The TA Owner can deliver this letter:

- via postal mail sent to the TERENA Address; or
- as a PDF document attached to a signed email sent to the TACAR Administrator, after the TA Owner's authentication information has been registered with the TACAR Administrator or with the TI.

This document is meant to bind TA Owners to a TA; if a TA Owner owns more TAs then he/she is expected to fill in a letter for each TA he/she owns.

TA Owner Details

(copy this section for every TA Owner associated with the TA(s) listed below)

a) **TA Owner Name:**

b) **Affiliation Name:**

c) **Affiliation Website:**

d) **TA Owner email address:**

e) **TA Owner PGP Key details:**

User-ID:

Key-ID:

Fingerprint:

Direct Responsible Person

(the person the TA Owner(s) report to)

a) **Name:**

b) **email address:**

Trust Anchor(s) Details

(copy this section for each TA associated with the TA Owners listed above)

a) **Legal CA Name:**

b) **Trust Anchor website:**

c) **SHA1 TA fingerprint:**

Final Statement

The TA Owner(s) named above and the TACAR Administrator have verified each other's names and each other's identity and authentication information (e.g. PGP public key or X.509 user certificate).

The TA Owner(s) agree with the policies and procedures defined by TACAR regarding the certificate store.

Date:

Signatures:

<Firstname Lastname TA Owner 1> ……

<Firstname Lastname TA Owner 2> …….