TCS Generation 5 Technical Addendum to the CPS v2.2

TCS Generation 5 Certification Practice Statement TA

Version TA-G5-01
Published 2024-12-22
http://www.geant.org/tcs/

Table of Contents

1. Introduction

This Technical Addendum (TA) augments the Certification Practice Statement (CPS) for the Trusted Certificate Service (TCS), managed by the GÉANT Association's Amsterdam office for the community of its Members, applicable to the Issuing Authorities for the TCS Certificate Profiles – hereafter collectively referred to as 'TCS CAs'.

Starting January 2025, the TCS adds its 5th generation certification authority partner, HARICA (www.harica.gr) as the issuing authority for both public and private trust certificates. The scope of Generation 5 TCS includes

- public trust Server,
- joint-trust public and IGTF Server,
- private-trust (IGTF) Client Authentication,
- public-trust S/MIME email,

and other contracted products that are part of the HARICA-GEANT agreement that are beyond the scope of this CPS and are entirely covered by the HARICA Certification Policy and pertinent HARICA Certification Practice Statements.

Under the structure of the GEANT Trusted Certificate Service, the TCS is operated on behalf of the GÉANT Association by a contracted CA Operator. Under this Technical Addendum for the 5th generation TCS, the TCS is operated by the Greek Universities Network (GUnet) doing business as the Hellenic Academic & Research Institutions Certification Authority (HARICA).

This Technical Addendum complies and shall comply with the CA Operator's Certificate Policy, and must be interpreted in conjunction with the CPS of the CA Operator and the GEANT TCS CPS. This TA augments, details, and profiles the CA Operator's CPS for the TCS service. Where no further stipulations are made in this TA, the stipulations of the GEANT TCS Personal CA CPS, the GEANT TCS Server CA CPS, and the CA Operator's CPS apply.

1.1 Overview

The TA relates to the following certificate type issued by the CA Operator:

- Server – organisation-validated certificates in compliance with the CABF OV baseline requirements
- IGTF Server - organisation-validated certificates in compliance with the CABF OV baseline requirements and in addition with the IGTF Classic profile by using the subject distinguished name prefix assigned to the GEANT TCS (the sequence of domainComponents dc=org, dc=terena, dc=tcs)

- S/MIME Sponsor-validated Client Certificate ("Email") - verified email, organisation and name of the individual
- S/MIME organisation-validated Client Certificate ("Email") – verified email and organisation

- 13 month Personal Authentication private trust certificate – IGTF MICS and Classic profile certificates containing an RA-validated name, email address, and unique identifier
- 13 month Personal Automated Authentication and Robot Email private trust certificates – IGTF MICS and Classic profile certificates used for machine-to-machine communication

This addendum does not cover any other certificates types or products available in or via the GEANT TCS.

1.2 Document Name and Identification

This document is the TCS Technical Addendum TA-G5-01, which was published on 2024-12-22 by the TCS Policy Management Authority.

1.3 PKI Participants

1.3.1 Certification Authorities

This TA adds HARICA as a Certification Authority provider for the 5th generation TCS.

Server Certificate services

For the *Server Certificate* services, both OV web-public trusted and joint OV and IGTF Classic (OV) certificates are issues by the "HARICA OV TLS RSA" (2021) and "HARICA OV TLS ECC" (2021) issuing CAs:

- https://repo.harica.gr/certs/HARICA-OV-TLS-Sub-R1.txt
- https://repo.harica.gr/certs/HARICA-OV-TLS-Sub-E1.txt

the difference between the OV and IGTF Classic (OV) certificates is solely in the profile of the end-entity certificates, where IGTF Classic (OV) profiles are prefixed with the domainComponent sequence assigned by GEANT to the TCS ("dc=org,dc=terena,dc=tcs", in encoding-order).

The root of trust for all Server certificates are the "HARICA TLS RSA Root CA 2021" and the "HARICA TLS ECC Root CA 2021":

- https://repo.harica.gr/certs/HARICA-TLS-Root-2021-RSA.txt
- https://repo.harica.gr/certs/HARICA-TLS-Root-2021-ECC.txt

For transitional compatibility purposes, cross-signed certificates exist to the 2015 trust roots.

Personal Certificate service

For the *Personal (also known as email or S/MIME) Certificate* service, certificates are issued by the "HARICA S/MIME RSA SubCA R3":

- https://repo.harica.gr/certs/HaricaSmimeSubCAR3.txt

The root of trust for Personal certificates is the "Hellenic Academic and Research Institutions RootCA 2015"

- https://repo.harica.gr/certs/HaricaRootCA2015.txt

Authentication Certificate services

The *Personal Authentication, Personal Automated Authentication, and Organisation Authentication (Robot Email) Certificate* services, are issued by the "GEANT TCS Authentication RSA CA 5" and "GEANT TCS Authentication ECC CA 5":

- https://repo.harica.gr/certs/...
- https://repo.harica.gr/certs/...

The root of trust for Authentication certificates is a private (enterprise specific) trust root for the GEANT TCS Research and Education community: "ToBeDefined":

- https://repo.harica.gr/certs/...

Other Certificate Services

Other certificate services, including Organisation validated S/MIME, OV and EV Code Signing, Qualified Certificates, and any IV certificates are not covered by this technical addendum.

1.3.2 Registration Authorities

No stipulation.

1.3.3 Subscribers

No stipulation.

1.3.4 Relying Parties

No stipulation.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

No stipulation.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This CPS and any related documents, agreements, or policy statements referenced herein are maintained and administered by the TCS Policy Management Authority.

1.5.2 Contact Person

Trusted Certificate Service
GÉANT Association
Hoekenrode 3
1102 BR Amsterdam
The Netherlands

E-mail: tcs-pma@lists.geant.org

1.5.3 Person Determining CPS Suitability for Policy

No stipulation.

1.5.4 CPS Approval Procedures

No stipulation.

1.6 Definitions and Acronyms

No stipulation.

2. Publication and Repository Responsibilities

This TA is one of a set of documents relevant to the TCS services. Relevant documents and/or references thereto are made available through the TCS Repository. The TCS Repository can be found at https://wiki.geant.org/display/TCSNT/.

2.1 Repositories

Policies, Practices, and ancillary documents managed by the CA Operator are held in the Repository of the CA Operator, which can be found at https://harica.gr/en/About/Policy.

Root and intermediate certificates are published at https://repo.harica.gr/

2.2 Publication of Certificate Information

No stipulation.

2.3 Time or Frequency of Publication

No stipulation.

2.4 Access Controls on Repositories

No stipulation.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The name forms for Server Certificate end-entity certificates that are joint CABF OV and IGTF Classic OV trusted will be prefixed with a sequence of domainComponent names “DC=org”, “DC=terena”, “DC=tcs”.

The name forms of end-entity Authentication Certificates (private trust hierarchy) will be prefixed with a sequence of domainComponent names “DC=org”, “DC=terena”, “DC=tcs”.

For Authentication Certificates, neither locality nor stateOrProvinceName shall be part of the subject DN for any and-entity. The subject name construction shall be based on the TCS distinguishing prefix (domainComponent based as specified in 3.1.1), the Country (C) name, the OV validated organizationName (O), and the commonName (CN) of the certificate subject, post-fixed with the unique identifier of the user including the organisational scope (i.e. *identifier@scope*).
The latter shall constitute any disambiguation needed for differentiating similarly-named organisation within a single Country.

There are no stipulations for the name forms of other certificate profiles beyond those specified by the issuing CA.

3.1.2 Need for Names to be Meaningful

No stipulation.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

Server Certificates may use either locality (L) or stateOrProvinceName (ST) in the subject naming of end-entity certificates, in accordance with CACABF requirements. Under this technical addendum, there shall be no constraint on the name forms used herefore.

3.1.5 Uniqueness of Names

The Subject Distinguished Name of a TCS Authentication CA-issued Certificate is unique for each Applicant by including an Identifier that uniquely and persistently represents the Applicant in the IdP of its Subscriber.

The unique persistent identifier for the 5th generation TCS authentication CA can be either the eduPersonPrincipalName, or the subject-id as defined by the SAML V2.0 Subject Identifier Attributes Profile Version 1.0.

Common-name uniqueness and consistency between 4th and 5th generation TCS subject names is ensured by having the same identity providers and organisations provide the unique identifier (and displayname), and the identifier being omnidirectional.

When eduPersonPrincipalName is provided by the IdP of the subscriber together with the eduPersonEntitlement urn:mace:terena.org:tcs:personal-user, the subscriber guarantees that the eduPersonPrincipalName is never re-assigned and remains persistently bound to the human entity for which it was first released.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

No stipulation.

3.4 Identification and Authentication for Revocation Requests

No stipulation.

4. Certificate Life-Cycle Operational Requirements

No stipulation.

5. Facility, Management and Operational Controls

No stipulation.

6. Technical Security Controls

No stipulation.

7. Certificate, CRL and OSCP Profiles

7.1 Certificate profile

The public trust root for Server and IGTF Server certificates shall be the “C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA TLS RSA Root CA 2021”

7.1.1 Version number(s)

No stipulations.

7.1.2 Certificate extensions

No stipulations.

7.1.3 Algorithm object identifiers

No stipulations.

7.1.4 Name forms

The subject name of the GEANT Authentication CA certificates are as specified in section 1.3.1.

The structure of subject distinguished names of TCS Authentication End Entity Certificates remains unchanged by this TA.

There are no further stipulations beyond those set forth by the CA Operator

7.1.5 Name constraints

No stipulations.

7.1.6 Certificate policy object identifier

No stipulations.

7.1.7 Usage of Policy Constraints extension

No stipulations.

7.1.8 Policy qualifiers syntax and semantics

No stipulations.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulations.

7.2 CRL profile

7.2.1 Version number(s)

No stipulations.

7.2.2 CRL and CRL entry extensions

No stipulations.

7.3 OCSP profile

There are no further stipulations beyond those set forth by the CA Operator.

8. Compliance Audit and Other Assessments

No stipulations.

9. Other Business and Legal Matters

No stipulations.