Amsterdam Office
Singel 468 D
1017 AW Amsterdam
The Netherlands
+31 (0) 20 5304488

www.geant.org
info@geant.org

TCS Model Subscriber Agreement

Version 3 rev 03

Preamble

The Trusted Certificate Service (TCS), which is managed by the GÉANT Association's Amsterdam office (formerly TERENA) for the community of the association's Members, provides publicly trusted and community-specific Public Key Infrastructure credentials to Subscribers. Its operations and practices are governed by the contract between the GÉANT Association and the CA Operator (DigiCert, Inc. of Lehi, Utah, USA), by the TCS Certification Practice Statement (TCS CPS), and its ancillary documents. In particular, the contract between the GÉANT Association and DigiCert stipulates a number of Required Contractual Terms that must be included in the agreement between GÉANT and its Members, and the agreement between Members and Subscribers.

A *Member* is a National Research and Education Networking organization (NREN) that has entered into an agreement with GÉANT Association to provide TCS Server and Code Signing CA services to its Subscribers.

Subscribers are Research and/or Educational organization and/or non-commercial members of an NREN requesting a Certificate through an Account at the CA Operator.

Applicants are individuals from the constituency of a Subscriber that - through applying via that Subscriber - are allowed to apply for a Certificate on behalf of the Subscriber.

Some Member organisations may already have more general contracts in place with each of their connected institutions and may want to add the stipulations of the Subscriber Agreement to that contract. Other national GEANT Association member organisations may wish to have separate Subscriber Agreements with their Subscribers. It is to be expected that in most cases these contracts will be in the local language. As regards the Subscriber Agreements, there will therefore be a lot of

variety between countries. Nevertheless, the following issues should in any case be incorporated in the contracts that serve as Subscriber Agreements:

- that the Subscriber will abide by the Required Contractual Terms
- that the Subscriber will abide by the TCS Certificate Practice Statement (TCS CPS);
- that the Subscriber will follow the applicable Certificate Practice Statement in issuing and using the Certificates;
- that the Subscriber will review each certificate prior to use;
- that the Subscriber will obey the applicable law with respect to each certificate;
- that the Subscriber will ensure the accuracy of all information provided;
- that the Subscriber will maintain its private keys as confidential information;
- that the Subscriber will cease using the certificate if it is revoked;
- that the Subscriber gives the GÉANT Association and the relevant Member the right to revoke a certificate on the basis of the stipulations in the TCS Certificate Practice Statement.

The following formulations can be used by Members when drafting the Subscriber Agreements to be signed by them and their Subscribers, although adaptations to national law may be necessary. Members may want to add additional conditions.

Model Subscriber Agreement

By participating as a Subscriber and Registration Authority in the GÉANT Trusted Certificate Service (TCS), you:

- shall agree to abide by the TCS Consolidated Required Contractual Terms, the relevant section of which is replicated herein, including any updates and addenda thereto;
- shall agree to abide by the TCS Certificate Practice Statement (CPS), including the pertinent ancillary documents, Practice Statements, Policies, and Certificate Terms of Use;
- are responsible that staff and representatives involved with the TCS read and understand the terms and conditions in the TCS Certificate Practice Statement (CPS) and associated policies that are published in the TCS repository at http://www.terena.org/activities/tcs/repository-g3/. The Subscriber agrees with these terms and conditions;
- shall follow the practices and procedures described in the TCS CPS, and shall act in accordance with the conditions imposed on Subscribers by the CPS;
- are responsible to use TCS certificates only for legal and authorised purposes in accordance with the suggested usages and practices in the TCS CPS;
- are responsible to provide correct and accurate information in its communications with the Member. Subscriber is responsible to alert the member if at any stage while a certificate is valid, any information originally submitted has changed since it had been submitted to the Member.

Subscriber is aware that certificates issued to Subscriber may be revoked by the Member or TERENA according to the conditions indicated in the TCS CPS.

As a Registration Authority, the Subscriber hereby agrees to the following terms:

1. Applicability. The terms cover each digital certificate issued to a Subscriber under the agreement with GÉANT Association, regardless of (i) the digital certificate type (email, code signing, or TLS/SSL), (ii) when the Subscriber request the digital certificate, or (iii) when the digital certificate actually issues. The Subscriber may not request a certificate with contents that infringe on the intellectual property rights of another entity.
2. Private Key Generation. The Subscriber must keep all Private Keys confidential and use reasonable measures to protect the Private Key from disclosure. The Subscriber must request revocation of the Certificate within one working day of any suspected misuse or compromise of a Certificate or Private Key. The Subscriber must generate its key pair using one of the following methods: (i) inside a secure hardware token, (ii) using trustworthy cryptographic software on a local computer system where it is the sole user and administrator, (iii) on a computer system administered by its sponsor or a third party if (a) the key material is generated using trustworthy cryptographic software, (b) access is limited to designated individuals, who are subject to and aware of applicable privacy rules and a professional code of conduct, (c) the private key and pass phrase are not sent in clear text over a network, (d) the encrypted private key file is not sent over the network unprotected, (e) the system is located in a secure environment, where access is controlled and limited to only authorized personnel, and (f) a system does not persistently keep pass phrases or plain text private keys for longer than 24 hours.
3. IGTF Private Key Storage. Subscribers of Certificates issued as a 'Grid Certificate' must store and protect Private Keys in accordance with the applicable and current Grid policy.
4. Certificate Transparency. To ensure Certificates function properly throughout their lifecycle, the Subscriber must permit DigiCert to log SSL Certificates with a public certificate transparency database. Because this will become a requirement for Certificate functionality, Subscribers cannot opt out of this process and expressly agree to log their Certificates. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.
5. **Restrictions.** Subscribers may not (a) share their Certificate or Private Key with another user except where permitted by the CPS, (b) use a Certificate or Private Key to operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring failsafe operation whose failure could lead to injury, death or environmental damage, (c) modify, sub license, reverse-engineer or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key, (d) use or make representations about a Certificate except as allowed in the CPS, (e) impersonate or misrepresent your affiliation with any entity or use a Certificate in a manner that could reasonably result in a civil or criminal action being taken against the Subscriber or DigiCert, (f) use a Certificate to send or receive unsolicited bulk correspondence, sign or distribute any files, software, or code that may damage the operation of another's computer or that is downloaded without a user's consent, or breach the confidence of a third party, (g) attempt to use a Certificate to issue other Certificates, except that a Subscriber may use the Certificate to create proxy certificates as defined in RFC 3820, or (h) intentionally create a Private Key that is substantially similar to a DigiCert or third party Private Key. Subscribers are solely responsible for ensuring your Certificates are renewed prior to their expiration.
6. Revocation. DigiCert may revoke a Subscriber's Certificate without notice for the reasons stated in the CPS, including if DigiCert believes that (a) the Subscriber or **the Certificate's** Subject requested revocation of the Certificate or did not authorize the Certificate's issuance,

(b) the Subscriber or the Certificate's Subject breach its obligations under the agreement with the GÉANT Association or an NREN or fail to comply with the CPS, (c) a provision of this agreement containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid, (d) the Subscriber or the Certificate's Subject are added to a government prohibited person or entity list or are operating from a prohibited destination under the laws of the United States, (e) the Certificate contains inaccurate or misleading information, (f) the Certificate was used outside of its intended purpose or used to sign malicious software; (g) the Private Key associated with a Certificate was disclosed or compromised, (h**)** the agreement between the GÉANT Association and Digicert terminates, (i) the Certificate was used or issued, directly or indirectly, contrary to law, the CPS, or industry standards, (j) industry standards or DigiCert's CPS require revocation, or (k) revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

7. Relying Party Warranties. DigiCert's Relying Party Warranty (**http://www.digicert.com/docs/agreements/DigiCert_RPA.pdf)** is only for the benefit of entities other than the Subscriber that act in reliance on a Certificate or a Digital Signature. Subscribers do not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty.

8. Remedy. A Subscriber's sole remedy for a defect in a Certificate is to have DigiCert use reasonable efforts to correct the defect. DigiCert is not obligated to correct a defect if (i) the Certificate was misused, damaged, or modified, (ii) the Subscriber did not promptly report the defect to DigiCert, or (iii) Subscriber has failed to abide by the GÉANT Association agreement.

9. Software and Equipment. Subscribers are solely responsible for their own conduct, software, website maintenance, operation, development, security and content, and all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to access and use the Certificates.

10. Warranty Disclaimers. THE CERTIFICATES, AND ANY RELATED SOFTWARE, PRODUCTS, AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO THE ACCOUNT WILL BE TIMELY OR ERROR-FREE. Use of a SHA-1 Certificate will result in errors displayed by Application Software Vendors.

11. Limitation on Liability. The agreement is not required to limit a party's liability for (i) death or personal injury resulting from the negligence of a party or (ii) fraud or fraudulent statements made by a party. EXCEPT AS STATED ABOVE, THE SUBSCRIBER MUST AGREE TO LIMIT DIGICERT'S MAXIMUM LIABILITY RESULTING FROM THE CERTIFICATE TO THE AMOUNT OF $ 530.000. SUBSCRIBER MUST AGREE THAT DIGICERT IS NOT LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. The limitations must apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement were breached or proven ineffective.

12. Indemnification. To the extent permitted by law, Subscriber must indemnify, hold harmless, and defend DigiCert against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from Subscriber's breach of these terms.