



Unité Réseaux du C.N.R.S. (UPS 836)

## Déclaration des Pratiques de Certifications TCS

Auteurs : Équipe TCS (CNRS/UREC)

### Référence du document :

CPS CERTIFICAT TCSV2.0.DOC

### Table des matières :

1	Introduction .....	2
1.1	Contexte général .....	2
1.2	Délégation d'Autorité d'Enregistrement .....	2
1.3	Souscripteur TCS .....	2
2	Pré requis pour les demandes .....	2
2.1	Enregistrement d'un souscripteur .....	2
2.2	Vérification administrative .....	3
3	Pratiques et procédures .....	3
3.1	Demande de certificats .....	3
3.2	Validation des demandes .....	4
3.3	Révocation des certificats .....	4
3.4	Expiration .....	4
3.5	Renouvellement .....	4
4	Conservation et protection des données .....	4

# 1 Introduction

---

## 1.1 Contexte général

1. Le service « TERENA Certificate Server » (TCS) opéré par TERENA fournit des certificats serveurs (durée: 1, 2, 3 ans) et des certificats serveurs eScience (durée: 13 mois)
2. L'utilisation de ces certificats est possible pour tout type de transaction sauf les transactions financières
3. Un certificat peut couvrir 100 noms de domaine maximum
4. Un certificat « wildcard » peut couvrir plusieurs sous domaines

## 1.2 Délégation d'Autorité d'Enregistrement

Le rôle d'Autorité d'Enregistrement de RENATER est délégué pour le CNRS à l'Unité Réseaux du CNRS - UREC. L'AE du CNRS :

1. Maintient un registre des unités approuvées pour les demandes de certificats
2. Accepte, évalue, approuve ou rejette les demandes de certificats
3. Vérifie l'exactitude et l'authenticité des informations fournies par le *souscripteur* au moment de la demande conformément à la CPS
4. Utilise des documents officiels ou autres documents autorisés pour évaluer une demande faite par un *souscripteur*
5. Vérifie l'exactitude et l'authenticité des informations fournies par le *souscripteur* au moment du renouvellement conformément à la CPS

## 1.3 Souscripteur TCS

Le *souscripteur* est l'unité du CNRS souhaitant souscrire au service TCS. Le *souscripteur* est identifié dans chaque certificat TCS et est le titulaire de la clé privée du certificat.

Chaque *souscripteur* doit signer et cacheter la *Lettre d'Engagement* et la transmettre à l'AE pour bénéficier du service.

Une fois acceptée, l'adhésion au service pour le *souscripteur* est valable pour la totalité de la période du marché TCS

# 2 Pré requis pour les demandes

---

## 2.1 Enregistrement d'un souscripteur

1. Le *souscripteur* fournit à l'AE tous les documents ou informations nécessaires à son enregistrement auprès de l'AE. Ces documents incluent une preuve d'identité de l'unité.
  - a. Obligatoire : la *Lettre d'Engagement* signée par un représentant légal de l'unité (Directeur de l'unité).

- b. Obligatoire : Le *souscripteur* désigne un ou plusieurs contacts administratifs autorisés à faire des demandes de certificats ou des demandes de révocation de certificats au nom du *souscripteur*.
  - c. Obligatoire : une liste des noms de domaine ou zones du domaine cnrs.fr utilisés par le *souscripteur* dont le *Centre National de la Recherche Scientifique* ou le *souscripteur* est titulaire (cf. §2.2).
  - d. En option : une liste des adresses IP assignées à l'unité demandeur.
2. Le *souscripteur* s'engage pour toute action engagée par les contacts administratifs.
  3. Les contacts administratifs doivent se conformer au document « *TCS Certificate Practice Statement (CPS)* » et autres documents TCS.
  4. Le *souscripteur* s'engage à fournir des informations correctes et précises et avertir l'*AE* en cas de mise à jour nécessaire de ces informations tout au long de la période de validité du certificat par le moyen de communication le plus adapté (cf. *Lettre d'Engagement*).

## 2.2 Vérification administrative

L'*AE* doit :

1. Vérifier l'identité du *souscripteur* automatiquement ou manuellement en vérifiant particulièrement les informations suivantes à partir des bases de référence du CNRS :
  - a. Intitulé de l'unité (public)
  - b. Le code Labintel (public)
  - c. Rue, code postal, ville (public)
  - d. Nom du directeur de l'unité
  - e. Si nécessaire : délégation de signature pour les marchés et commandes nécessaires à l'approvisionnement et au fonctionnement de l'unité
  - f. Numéros de décision au Bulletin Officiel du CNRS
  - g. Contacts administratifs (nom complet, email, téléphone)
  - h. L'existence des Contacts administratifs dans le référentiel Janus
2. Vérifier la propriété des noms de domaine :
  - a. soit le titulaire du nom de domaine dans les bases « whois » est le *Centre National de la Recherche Scientifique* (par exemple : *CNRS, CTRE NAT DE LA RECHERCHE SCIENTIFIQUE*)
  - b. soit le titulaire du nom de domaine dans les bases « whois » est le *souscripteur*
  - c. et pour une zone du domaine cnrs.fr, le titulaire dans les bases de l'UREC est le *souscripteur*.
3. Vérifier tous les documents (*Lettre d'Engagement*) : notamment vérifier la *Lettre d'Engagement* signée avec cachet et signature du responsable légal, original envoyé par courrier postal, ou copie par courrier électronique signé numériquement par certificat d'une autorité du CNRS.
4. Enregistrer le *souscripteur*.
5. Autoriser le *souscripteur* à demander des certificats serveurs.
6. Confirmer les informations sur un *souscripteur* par l'utilisation possible des services d'un tiers.

L'*AE* a le droit de refuser toute demande.

## 3 Pratiques et procédures

---

### 3.1 Demande de certificats

Lorsque le contact administratif fait une demande de certificat et l'approuve, le système de l'AE vérifie si les requêtes sont conformes aux données enregistrées pour l'unité (nom, DNS, adresses IP). Si les données correspondent, la demande est automatiquement envoyée à l'autorité de certification pour émission.

La demande se fait via un formulaire en ligne disponible sur le site de l'AE.

### 3.2 Validation des demandes

Le délai moyen entre la réception des demandes complètes et la délivrance d'un certificat est de 5 jours. En cas de non validation des informations, le système de l'AE rejette la demande. Le demandeur peut refaire sa demande suite à un rejet.

### 3.3 Révocation des certificats

La révocation entraîne la fin de validité du certificat avant la date de fin initialement prévue. Le système de l'AE vérifie que la demande de révocation est :

- Soit faite par le *souscripteur* ayant fait la demande de certificat
  - a. Automatiquement auprès du système de l'AE (une demande authentifiée faite par un contact administratif du *souscripteur* sera automatiquement acceptée). La demande de révocation et l'identité du contact administratif seront enregistrées.
  - b. Explicitement par un Contact administratif du *souscripteur* auprès du personnel de l'AE. L'AE peut demander confirmation par téléphone ou fax. La demande de révocation et l'identité du contact administratif seront enregistrées. Le personnel de l'AE commandera alors la révocation du certificat ; son identité ainsi que la raison de la révocation seront enregistrées.
- Soit faite par une entité pouvant prouver la propriété de la clé privée associée au certificat => en cas de preuve, l'AE révoquera le certificat. La demande de révocation et la preuve de la bonne clé privée seront conservées.

### 3.4 Expiration

TCS doit s'efforcer de prévenir le *souscripteur* par email, 30 jours avant l'expiration de ses certificats.

### 3.5 Renouvellement

Idem que pour demande de certificats.

## 4 Conservation et protection des données

---

TERENA conserve les données relatives aux certificats pendant 3 ans minimum après expiration ou révocation des certificats. TERENA garde des copies des certificats quelque soit leur statut : enregistrement au format électronique, papier ou autre format approprié. TERENA conserve les logs pendant une période de 3 ans ou pour une période conforme à la loi.

TCS respecte les règles applicables sur la protection des données personnelles jugées par la loi ou le CPS comme confidentielles.

Informations jugées confidentielles:

1. *Lettre d'Engagement* signée.

2. Traces des demandes de certificat et documents soumis pour les demandes de certificats acceptées ou rejetées.
3. Traces des transactions et des audits financiers.
4. Traces et enregistrements des opérations de l'infrastructure de TCS, management des certificats, services des inscriptions et données.

L'AE conserve les traces conformément à la note : « Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS » du Fonctionnaire de Sécurité de Défense du CNRS. Le personnel de l'AE doit se conformer à la loi sur la protection des données personnelles.