

Déclaration des pratiques de certification

Version	1.1
Date	20 Janvier 2013
Rédigé par	Ambroise Ismael Kabore
Relu par	
Approuvé par	

MISES À JOUR

Version	Date	Modifications réalisées
0.1	19/12/2012	Création
1.1	20/01/2013	Après relecture par Magali Bardet

Table des matières

1	Introduction	4
1.1	Contexte Général	4
1.2	Délégation d'autorité d'enregistrement	4
1.3	Souscripteur	4
2	Pré requis pour les demandes	4
2.1	Enregistrement d'un souscripteur	4
2.2	Vérification	4
3	Pratiques et procédures	4
3.1	Demande de certificats	4
3.2	Validation des demandes	5
3.3	Révocation des certificats	5
3.4	Expiration	5
3.5	Renouvellement	5
4	Conservation et Protection des données	5

1 Introduction

1.1 Contexte Général

La PKI mise en place pour le projet de chat sécurisé fournit des certificats (Durée : 2 ans) aux utilisateurs sécurisés du chat. Ces certificats sont utilisés sur le chat pour s'authentifier.

1.2 Délégation d'autorité d'enregistrement

Pas de délégation du rôle d'Autorité d'Enregistrement dans notre cas. La PKI assurera ce rôle.

1.3 Souscripteur

Le souscripteur est l'utilisateur du chat souhaitant se connecter au chat sécurisé. Le souscripteur est identifié dans chaque certificat. Une fois acceptée, l'adhésion au service pour le souscripteur est valable pour la totalité de la période de validité du certificat sauf révocation.

2 Pré requis pour les demandes

2.1 Enregistrement d'un souscripteur

- Le souscripteur fournit à la RA toutes les informations nécessaires à son enregistrement.
- Le souscripteur s'engage à fournir des informations correctes et précises et avertir la RA 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.

2.2 Vérification

L'AE doit :

- Vérifier le remplissage correct de tous les champs par le souscripteur en respectant les conventions.
- Enregistrer le souscripteur.
- Transmettre la demande à la CA.

L'AE a le droit de refuser toute demande.

3 Pratiques et procédures

3.1 Demande de certificats

Lorsque l'utilisateur fait une demande de certificat, la RA vérifie si les informations respectent les conventions, si les données respectent, la demande est automatiquement envoyée à l'autorité de certification pour génération du certificat. La demande se fait via un formulaire disponible sur l'application cliente du chat. L'utilisateur doit aussi se présenter physiquement chez l'administrateur pour s'authentifier.

Dans le cas où un serveur veut faire une demande de certificat à la PKI, c'est l'administrateur du serveur qui fait la demande en suivant la procédure normale.

3.2 Validation des demandes

Le délai moyen entre la réception des demandes complètes et la délivrance d'un certificat est de 1 jour. En cas de non validation des informations, la RA 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. La RA vérifie que la demande de révocation est :

- Soit faite par l'utilisateur ayant fait la demande de certificat : la demande de révocation sera traitée.
- Soit faite par une entité disposant des droits nécessaires : la RA révoquera le certificat. La demande de révocation et l'identité de l'entité seront conservées.

3.4 Expiration

La PKI doit s'efforcer de prévenir le souscripteur par email, 30 jours avant l'expiration de son certificat.

3.5 Renouvellement

Idem que pour demande de certificat.

4 Conservation et Protection des données

La PKI conserve les données relatives aux certificats pendant 2 ans minimum après expiration ou révocation des certificats. La PKI garde des copies des certificats quel que soit leur statut et conserve les logs pendant une période de 2 ans ou pour une période conforme à la loi.

La PKI respecte les règles applicables sur la protection des données personnelles jugées par la loi comme confidentielles.

Acronymes

CA	Certification Authority
AE	Registration Authority
DPC	Déclaration des Pratiques de Certification
PKI	Public Key Infrastructure
CNRS	Centre National de la Recherche Scientifique
TCS	Terena Certificate Service

Documents applicables et de référence

- PC (Politique de certification)
- Déclaration des pratiques de certification TCS (CNRS)