Agence Nationale de Certification Electronique

Politique de Certification et Déclaration des pratiques de certifications de l'autorité Tunisian Root Certificate Authority

Mise à jour

Rev	Date	Nature de la révision	Page
Rev 00	01/06/2015	Première Rédaction	Toutes les pages
Rev 01	28/07/2015	Mise à jour	Mise à jour des profiles
Rev 02	27/11/2017	Mise à jour	Section 7.2

	Elaboré par	Validé par	Approuvé par
Fonction :	ANCE	Comité de pilotage	Directeur Général
Date :	19/02/2017	22/11/2017	27/11/2017

Sommaire

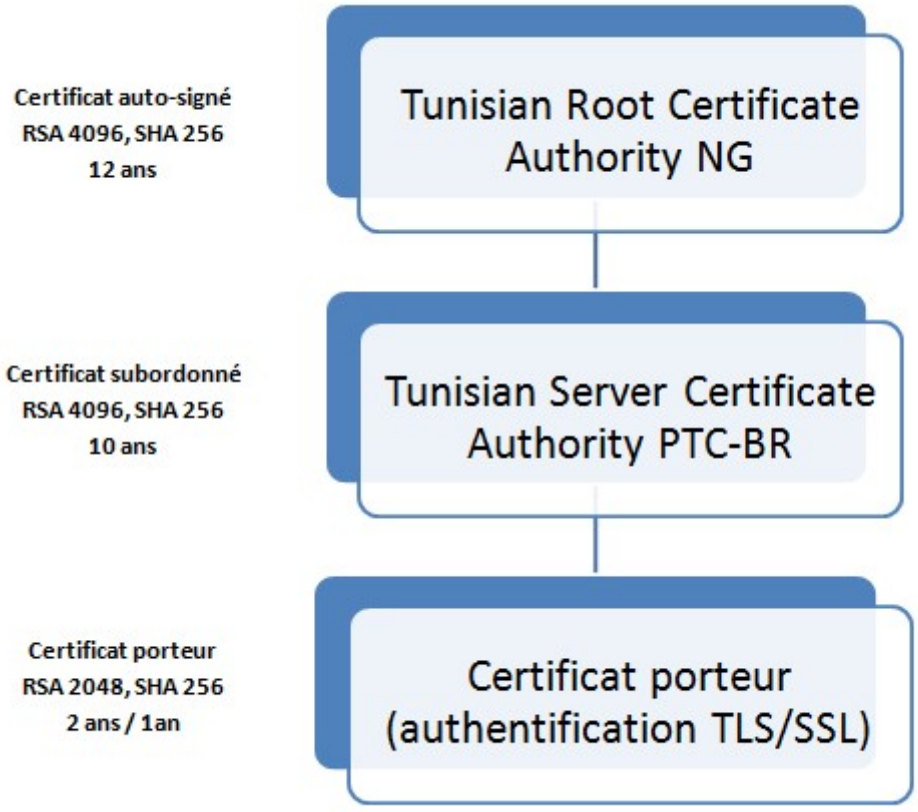
1 INTRODUCTION

1.1 Généralités

L'ANCE, l'Agence Nationale de Certification Electronique, est dépositaire en Tunisie de la confiance électronique. L'ANCE est notamment en charge de la création et de l'opération de l'Autorité Racine de Certification Nationale tunisienne.

Dans cette optique, l'ANCE met en œuvre son IGC, structurée en Autorité Racine et Autorités subordonnées, spécialisées par populations cibles ou usages (personnes physiques, serveurs, équipements VPN, signature de code…).

La hiérarchie de l'IGC de l'ANCE concernée dans le présent document est structurée de la façon suivante :



L'Autorité de Certification « **Tunisian Root Certificate Authority NG**», ou « **AC Racine** » dans la suite du document a pour charge de délivrer les certificats d'Autorités de certification déléguées de l'ANCE ou d'Autorités de FSCE externe à l'ANCE.

Le présent document a pour objectif la description des exigences applicables aux pratiques de certification devant être mises en place par l'AC Racine pour l'émission de certificats destinés aux autorités de certification.

Le présent document est établi de façon à respecter de manière générale le plan de la RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement

Framework » de l'IETF. En revanche, aucune exigence de conformité n'est établie vis-à-vis de cette RFC directement dans le présent document. La conformité retenue est vis-à-vis de la norme ETSI TS 102 042 pour la PC/DPC AC Racine ;

Dans la suite du document, le terme générique « AC » peut être utilisé pour remplacer « AC Racine (de l'ANCE) ».

1.2 Nom du document et identification

Le présent document PC/DPC appelé « Politique de certification et déclaration des pratiques de certification de l'autorité Tunisian Root Certificate Authority NG» est à la propriété de l'ANCE.

Il est identifié de façon unique par l'identifiant OID suivant : 2.16.788.1.2.6.1.7.

1.3 Entités intervenant dans l'IGC

L'AC s'appuie sur les composantes et sous-composantes suivantes :

- **service d'enregistrement :** ce service est aussi appelé « Autorité d'Enregistrement » (AE) assurée par l'ANCE pour gérer les demandes de certificats et de révocation,
- **service de production des certificats, des LAR :** ce service est assuré par l'ANCE qui génère les certificats électroniques des autorités de certifications à partir des informations transmises par le service d'enregistrement après les avoir préalablement vérifiées et validées ;
- **service de publication :** ce service met à disposition des utilisateurs de certificat (UC) au moyen de site internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, PC/DPC publiées par l'AC, certificats d'AC, …), ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations (LAR, avis d'information, …) ;
- **service de gestion des révocations :** ce service traite les demandes de révocation des certificats subordonnés. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats ;
- **service d'information sur l'état des certificats :** ce service fournit aux utilisateurs de certificats (UC) des informations sur l'état des certificats. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers sous la forme de Listes des Autorités Révoquées (LAR)
- **service de journalisation :** ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC. Il est assuré par l'ANCE. Il permet de collecter l'ensemble des données utilisées et/ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audits consultables.
- **service d'audit :**ce service est assuré par l'entité d'audit interne à l'ANCE qui a pour charge l'application des contrôles réguliers et récurrents pour assurer la conformité des pratiques avec les PC /DPC.

1.3.1 Autorité de Certification (AC)

L'ANCE assure le rôle d'AC et elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité de l'AC est composé de la Politique de Sécurité des Systèmes d'Information, et de la présente PC/ DPC, des Conditions Générales d'Utilisation (CGU) et l'ensemble des procédures mises en œuvre par les composantes de l'IGC.

L'ANCE valide le référentiel de sécurité et elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et/ou contrôle de conformités effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

L'AC a pour responsabilité de garantir le lien entre l'identifiant d'une autorité et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par une clé privée de l'AC.

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. En plus des services de gestion du cycle de vie des certificats, L'AC met en œuvre les services de journalisation et d'audit.

La PC/DPC, les clés publiques et les LAR émis par l'AC sont la propriété de l'AC.

1.3.2 Les Autorité d'Enregistrement (AE)

L'ANCE joue le rôle de l'autorité d'enregistrement (AE). Elle est chargée

- l'enregistrement pour les demandes de certificats d'Autorités ;
- la révocation des certificats d'autorités ;
- la délivrance des certificats d'autorités pour les FSCE.

1.3.3 Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre de la publication des documents tels que les PC /DPC (plus de précisions sont fournies dans la section §2).

1.3.4 Utilisateur de Certificats (UC)

Les Utilisateurs de Certificat (UC) doivent se conformer à toutes les exigences de la présente PC/DPC. Ils s'engagent notamment à :

- Déclarer à l'AC les usages prévus des certificats émis selon la présente PC/DPC, via le formulaire de demande, et respecter ces usages par la suite, dans le respect de la législation en vigueur ;
- Respecter les termes des CGU ;
- Utiliser des logiciels qui sont à même de vérifier que le certificat :
  - n'est en dehors de sa période de validité au moment de son utilisation,
  - n'est pas révoqué,
  - est effectivement utilisé selon l'usage prescrit dans le certificat.

1.4 Usage des certificats

1.4.1 Utilisation appropriée des certificats

1.4.1.1 Certificat de l'AC

La clé de l'AC Racine sert à signer son propre certificat et les Listes de Autorités Révoquées (LAR).

1.4.1.2 Certificats de l'AC subordonnées

La présence PC/DPC permet d'émettre des certificats à destination des AC subordonnées. La clé de l'AC Racine sert à signer les certificats d'Autorités subordonnées et les Listes des Autorités Révoqués (LAR). Grâce à ces certificats l'UC peut vérifier l'authenticité des AC subordonnées.

1.4.2 Utilisation interdite des certificats

Toute utilisation non spécifiée dans la présente PC/DPC est interdite.

Ainsi, l'ANCE ne peut en aucun cas être tenue responsable de l'utilisation des certificats émis selon cette PC/DPC à des fins et selon des modalités autres que celles prévues dans la présente PC/DPC.

1.5 Gestion de la PC/DPC

1.5.1 Organisme responsable de la présente PC/DPC

L'ANCE est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC/DPC.

1.5.2 Point de contact

Les remarques concernant cette PC/DPC sont à adresser à :

Titre de l'entité responsable	Adresse email	Adresse courrier
Agence Nationale de Certification Electronique	ance@certification.tn	Parc Technologique El Ghazala Route de Raoued, Km 3.5 2083 Ariana, Tunisie

1.5.3 Entité déterminant la conformité de l'implémentation de la présente PC/DPC

L'ANCE procède à des analyses / contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC d'émettre des certificats.

1.5.4 Procédures d'approbation de la présente PC/DPC

L'ANCE possède ses propres méthodes pour approuver le présent document. L'ANCE approuve les résultats de revue de conformité par les experts nommés à cet effet conformément à la procédure de mise à jour de la PC/DPC.

1.6 Définitions et Acronymes

1.6.1 Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AEC	Autorité d'Enregistrement Centrale
AED	Autorité d'Enregistrement Déléguée
ANCE	Agence Nationale de Certification Electronique
ARL	Authority Revocation List
ARLDP	Authority Revocation List Distribution Point
CGU	Conditions Générales d'Utilisation
CN	Common Name
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CRLDP	Certificate Revocation List Distribution Point
DPC	Déclaration des Pratiques de Certification
DN	Distinguished Name
ETSI	EuropeanTelecommunications Standards Institute
HTTPS	HyperText Transfer Protocol Secure
IGC	Infrastructure de Gestion de Clés
ISO	International Organization for Standardization
LAR	Liste des Autorités Révoquées
LCR	Liste des Certificats Révoqués
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OID	Object Identifier
PC	Politique de Certification
PC/DPC :	Politique de Certification et Déclaration des pratiques de certifications
PSSI	Politique de Sécurité des Systèmes d'Informations
RFC	Request For Comments
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SP	Service de Publication
SSL	Secure Socket Layer
TLS	Transport Layer Security

UC	Utilisateur de Certificats
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.6.2 Définitions

Audit : contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.

Autorité de Certification (AC) : entité responsable de garantir le lien (infalsifiable et univoque) entre l'identifiant d'une autorité subordonnée et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par une clé privée de l'AC.

Autorité d'Enregistrement (AE) : entité responsable de la délivrance des certificats aux RCS. L'AE traite en outre, les demandes de certificat. L'AE est un terme générique utilisé pour désigner l'AEC au niveau du Guichet de l'ANCE ou une AED au niveau des guichets des partenaires.

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettre en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat électronique : fichier électronique attestant qu'une clé publique est liée au nom de domaine identifié dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat par sa clé privée, l'AC valide le lien entre l'identifiant du nom du domaine et la bi-clé et garantit son authenticité.

Certificat d'AC : certificat pour une AC émis par une autre AC. [X.509].

Certificat d'AC auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification :(ou chaîne de confiance, ou chaîne de certification) chaîne constituée de plusieurs certificats nécessaires pour valider un certificat vis-à-vis d'un certificat d'AC auto-signé.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique.[ISO/IEC 9798-1].

Composante :plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte,

le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de cette clé privée.

Confidentialité : la propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus non autorisés.

Déclaration des Pratiques de Certification (DPC) :document qui identifie et référence les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Demande de certificat : message transmis par une entité AE à l'AC pour obtenir l'émission d'un certificat d'AC.

Disponibilité : propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation : valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie ;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1] ;
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de gestion de clés (IGC) : ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques utilisés par des services de confiance.

Infrastructure à Clé Publique (ICP) : IGC dédiée à la gestion de clés asymétriques. C'est l'infrastructure requise pour produire, distribuer, gérer des clés publiques et privées, des certificats et des Listes de Certificats Révoqués.

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste des Autorités Révoqués (LAR) : liste signée numériquement par une AC et qui contient des identités de certificats d'Autorités qui ne sont plus valides.

Module cryptographique : ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) Standard mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'ICP après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR : entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles, identifié par un nom (OID), définissant (a) les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes (b) les obligations et exigences portant sur les autres intervenants, notamment les autorités subordonnées et les utilisateurs de certificats.

PC et DPC : fusion de la Politique de Certification (PC) et la Déclaration des Pratiques de Certification (DPC)

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Autorité subordonnée de secret : personne qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Qualificateur de politique : informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

RSA : algorithme de cryptographie à clé publique inventé par Rivest, Shamir, et Adleman.

Signature numérique : somme de contrôle cryptographique générée en utilisant une fonction de hachage et une clé privée et vérifiable en utilisant une clé publique.

Utilisateur de Certificats (UC) : application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat d'autorité conformément à la présente PC/DPC.

Validation d'un certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenues dans le chemin de certification. Elle inclut également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat auto-signé qui sera pris comme référence.

2 Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Le Service de Publication (SP) est le service en charge de la publication du présent document et des autres documents ou informations dont la publication est nécessaire afin d'assurer la bonne utilisation des certificats délivrés au titre de la présente PC/DPC.

Le SP est chargé de mettre à disposition les informations, citées ci-après, sur le site web de l'ANCE.

2.2 Informations devant être publiées

L'AC s'assure que les termes et conditions applicables à l'usage des certificats qu'elle délivre sont mis à la disposition des autorités subordonnées et des UC.

L'AC, via le SP, rend disponibles les informations suivantes :

- La présente PC/DPC (http://www.certification.tn/sites/default/files/documents/politiqueRACINE-NG-02.pdf);
- Le certificat de l'AC (http://www.certification.tn/pub/TunRootCA2.crt);
- La Liste de Autorités Révoquées (LAR) valide et à jour (http://www.certification.tn/pub/TunRootCA2.crl)

Toutes ces informations sont disponibles sur le site internet de l'ANCE, accessible à l'adresse http://www.certification.tn.

2.3 Délais et fréquences de publication

La présente PC/DPC et les certificats de l'AC racine de l'ANCE sont disponibles en permanence selon un taux de disponibilité 24h/24 7j/7 et mises à jour selon les besoins.

Une nouvelle LAR est publiée tous les ans suivant un taux de disponibilité de 24h/24 7j/7.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sur le site web, détaillées dans la section § 2.2, sont accessibles publiquement en lecture seule.

L'accès en écriture des informations publiées est strictement limité aux personnes habilitées de l'ANCE. Les administrateurs s'authentifient au moyen d'une authentification forte. La communication établie entre les administrateurs et les serveurs est chiffrée pour en assurer la confidentialité.

3 Identification et Authentification

3.1 Nommage

3.1.1 Types de noms

Dans chaque certificat X.509, l'AC (*Issuer*) et l'autorité subordonnée (*Subject*) sont identifiés par un nom distinctif, en anglais « Distinguished Name » (*DN*). Les identifiants utilisés dans ces certificats sont conformes à la norme X.500.

3.1.1.1 Certificat de l'AC Racine

Les identifiants utilisés dans le certificat de l'AC racine sont les suivants :

Champ de base	Valeur
Issuer DN	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority - TunRootCA2
Subject DN	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2

3.1.1.2 Certificat de l'Autorité

L'identité du certificat de l'autorité est la suivante :

Champ de base	Valeur
Issuer DN	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
Subject DN	C=(Exigé) O= (Exigé) OU= (Optionnel) CN=(Exigé)

3.1.2 Nécessité d'utilisation de noms explicites

Les identités incluses dans les certificats émis conformément à la présente PC/DPC sont toujours explicites et nominatives.

3.1.3 Pseudonymisation des autorités subordonnées

La présente PC/DPC n'autorise pas de pseudonymes et de noms anonymes dans les certificats émis.

3.1.4 Règles d'interprétations des différentes formes de noms

L'identification de l'autorité est basée sur son nom.

3.1.5 Unicité des noms

Les DN des certificats d'autorités sont uniques au sein du domaine de certification de l'AC qui émet le certificat. Durant toute la durée de vie de l'AC Racine, un DN attribué à une autorité ne peut être attribué à une autre autorité.

3.1.6 Identification, authentification et rôle des marques déposées

Sans objet pour les marques déposées.

3.2 Vérification initiale d'identité

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par l'autorité est réalisée par les procédures de génération de la clé privée correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (Cf. § 6.1).

3.2.2 Validation de l'identité des responsables des autorités subordonnées

Dans le cas d'une demande de FSCE, le dossier d'enregistrement d'Autorité Subordonnée, déposé auprès de l'AE doit comprendre au moins le dossier de demande rempli et complet, contenant notamment les justificatifs requis.

3.2.3 Informations non vérifiées de l'autorité subordonnée

La présente PC/DPC ne formule pas d'exigence sur ce point.

3.2.4 Certification croisée d'AC

La présente PC/DPC ne prévoit pas de certification croisée de l'AC Racine avec d'autres AC.

3.3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'une autorité entraîne la génération et la fourniture d'un nouveau certificat. La procédure est identique à la procédure de génération de certificat.

3.3.1 Identification et validation pour un renouvellement normal

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales (voir § 3.2 ci-dessus).

3.3.2 Identification et validation pour un renouvellement après révocation

Les vérifications relatives au renouvellement d'une bi-clé après révocation du certificat de clé publique correspondant sont effectuées conformément aux procédures initiales (voir § 3.2).

3.3.3 Identification et validation d'une demande de révocation

Si la demande de révocation est due à une compromission ou suspicion de compromission de clé, perte ou vol, l'authentification de la demande de révocation ne peut être effectuée avec la clé compromise. Les demandes de révocation sont authentifiées par l'ANCE. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial (voir § 3.2).

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La demande est effectuée par le responsable de l'autorité de certification cible.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent au moins faire partie de la demande de certificat :

- le nom de l'autorité à utiliser dans le certificat ;
- le nom et prénoms du responsable de l'autorité ;
- Les données personnelles d'identification du responsable de l'autorité dont un document officiel d'identité en cours de validité, comportant une photographie d'identité ;
- Les informations permettant à l'ANCE de contacter le responsable de l'autorité (numéro de téléphone, courriel, …).

Dans le cas de la demande d'un FSCE, les informations suivantes doivent être fournies afin de pouvoir exercer cette activité :

- Une fiche de renseignement fournie par l'Agence dûment rempli et signée par le demandeur de l'autorisation ;
- Un certificat de nationalité datant de moins de 3 mois ;
- Un certificat de résidence datant de moins de 3 mois ;
- Le bulletin n°3 du représentant de l'autorité ;
- Une déclaration sur l'honneur du représentant s'engageant à ne pas exercer une autre activité professionnelle ;
- Les documents justificatifs des moyens matériels, financiers et humains prévus aux articles 2 et 3 du cahier des charges relatif à l'exercice de fournisseur de services de certification électronique susvisé ;
- Les caractéristiques techniques des équipements et des dispositifs à utiliser pour la fourniture des services, accompagnées d'un schéma du dispositif de certification ;
- Un plan du local du fournisseur et une description détaillée des procédures de sécurité adaptées pour la sécurisation du local ;
- Les caractéristiques des dispositifs de sécurisation des réseaux utilisés pour la fourniture des services de certification ;
- Une description détaillée de tous les registres à tenir et les caractéristiques des dispositifs utilisés pour les gérer ;
- Une étude financière du projet à réaliser ;

- Un récépissé de paiement de la redevance d'étude du dossier prévue à l'article 4 du décret n°2001-1668 du 17 Juillet 2001,fixant les procédures d'obtention de l'autorisation d'exercice de l'activité de fournisseur de service de certification électronique.

Le dossier de demande est établi par le responsable de l'autorité.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

Pour les besoins de vérification des identités des personnes physiques, L'AE, effectue les opérations suivantes :

- vérifier la cohérence du dossier d'enregistrement et des justificatifs présentés ;
- vérifier l'exactitude du bon de commande et du paiement ;
- s'assurer que le responsable de l'autorité a pris connaissance des modalités applicables pour l'utilisation du certificat.

Une fois ces opérations effectuées, l'AE transmet la demande aux composantes de l'AC chargées de la production de certificat. L'AE conserve ensuite une copie des justificatifs d'identité présentés sous forme papier ou électronique ayant une valeur légale.

4.2.2 Acceptation ou rejet de la demande

En cas d'acceptation de la demande, l'AE transmet la demande à l'AC.
En cas de rejet de la demande, l'AE en informe le ou les demandeurs en spécifiant la raison du rejet ainsi que la liste des champs incorrects ou incomplets.

4.2.3 Durée d'établissement d'un certificat

La demande de certificat est traitée dès la réception de la demande et du règlement du paiement par l'AE dans les meilleurs délais.

4.3 Délivrance d'un certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à la vérification de l'intégrité de la demande provenant de l'AE et l'authentification de son origine, ou dans le cas d'un FSCE une fois le rapport de constat établi et l'autorisation validée dans le cas d'un FSCE (Décret n° 2001-1668 du 17 juillet 2001, article 5), l'AC déclenche les processus de génération et de production du certificat.

L'ordonnancement des opérations est assuré, ainsi que l'intégrité et l'authentification des échanges entres les composantes en fonction de l'architecture de l'IGC.

Les conditions de génération des certificats, ainsi que les mesures de sécurité à respecter sont précisées dans la présente PC/DPC.

A la fin du processus de production de certificat, l'AC transmet le certificat produit au service de délivrance de l'AE.

La délivrance du certificat au responsable de l'Autorité subordonnée est effectuée par une remise en mains propres par l'AE au guichet de l'ANCE.

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

Les conditions de génération des certificats et les mesures de sécurité sont précisées aux sections 5 et 6 ci-dessous.

4.3.2 Notification par l'AC de la délivrance du certificat à une autorité subordonnée

La notification est effectuée à la fin de la cérémonie des clés de l'AC par remise du certificat d'AC à son demandeur.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Dès que le certificat est reçu par le Responsable de l'autorité subordonnée, l'AC Racine considère le certificat comme accepté.

4.4.2 Publication du certificat

Le certificat de l'AC racine est publié par le SP.

Les certificats des autorités subordonnées de l'ANCE délivrés par l'AC Racine sont également publiés par le SP.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

L'ensemble des composantes de l'IGC est informé de la délivrance du certificat.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisations de la clé privée et du certificat de l'autorité subordonnée

Conformément à la section § 1.4, l'utilisation de la clé privée et du certificat émis par l'AC Racine est strictement limitée à des fins de signature de certificats et de liste des certificats révoqués, conformément à la présente PC/DPC. Le responsable de l'autorité subordonnée a pour obligation de respecter l'usage autorisé de la bi-clé et du certificat. Sa responsabilité peut être engagée dans le cas contraire.

En outre, les usages autorisés doivent figurer dans le certificat lui-même, au travers des extensions concernant les usages de clés (champs « Key Usage » et « Extended Key Usage » de X509 v3).

4.5.2 Utilisation de la clé publique et du certificat par un utilisateur du certificat

Conformément au chapitre précédent et à la section § 0, les utilisateurs de certificats sont tenus de respecter strictement les usages autorisés des certificats émis selon la présente PC/DPC. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

Conformément à la RFC [5280], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seul les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).

Dans le cadre de la présente PC-DPC, il peut y avoir de renouvellement du certificat des autorités subordonnées sans renouvellement de la bi-clé correspondante.

4.6.1 Causes possibles de renouvellement d'un certificat

Le processus de renouvellement de certificat est similaire à celui de la génération de certificats (voir les précédentes sections). L'opération de renouvellement du certificat est indépendante au certificat expiré.

Une bi-clé ou un certificat peuvent être renouvelés parce que le certificat est sur le point d'expirer ou suite à la révocation du certificat d'une autorité subordonnée (cf. § 4.9).

4.6.2 Origine d'une demande de renouvellement

Identique aux dispositions décrites au niveau de la section § 4.1.1.

4.6.3 Procédure de traitement d'une demande de renouvellement

Identique aux dispositions décrites au niveau de la section § 4.2.

4.6.4 Notification à l'autorité subordonnée de l'établissement du nouveau certificat

Identique aux dispositions décrites au niveau de la section § 4.3.

4.6.5 Démarche d'acceptation du nouveau certificat

Identique aux dispositions décrites au niveau de la section § 4.4.1.

4.6.6 Publication du nouveau certificat

Identique aux dispositions décrites au niveau de la section § 4.4.2.

4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Identique aux dispositions décrites au niveau de la section § 4.4.3.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC5280], ce chapitre traite de la délivrance d'un nouveau certificat à une autorité subordonnée liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Une bi-clé et un certificat peuvent être renouvelés parce que le certificat est sur le point d'expirer ou suite à la révocation du certificat de l'autorité subordonnée (cf. § 4.9).

4.7.2 Origine d'une demande d'un nouveau certificat

La demande peut être issue du responsable de l'autorité subordonnée ou le responsable de l'AC Racine.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Se reporter à la section 4.1.

4.7.4 Notification à l'Autorité Subordonnée de l'établissement du nouveau certificat

Se reporter à la section 4.1.

4.7.5 Démarche d'acceptation du nouveau certificat

Se reporter à la section 4.1.

4.7.6 Publication du nouveau certificat

Se reporter à la section 4.1.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Se reporter à la section 4.1.

4.8 Modification du certificat

La modification de certificat n'est pas autorisée dans la présente PC/DPC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats des autorités subordonnées

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'une autorité subordonnée :

- le Responsable de l'Autorité Subordonnée n'a pas respecté les modalités applicables d'utilisation du certificat ;
- la clé privée de l'Autorité Subordonnée est suspectée de compromission, est compromise, est perdue ou est volée ;
- le Responsable de l'Autorité Subordonnée ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat ;

- la cessation d'activité de l'organisation.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC Racine en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat par exemple), le certificat concerné doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LAR) :

- la clé privée de la composante est suspectée de compromission, compromise, perdue ou volée ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans les PC/DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats des Autorités Subordonnées

Le Responsable de l'Autorité Subordonnée ou un représentant légal de l'entité peuvent demander la révocation du certificat d'une Autorité Subordonnée émis selon la présente PC/DPC. L'AC Racine, émettrice du certificat, ou l'une de ses composantes peuvent demander la révocation des certificats émis selon cette PC/DPC.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'AC elle-même.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat d'une Autorité Subordonnée

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre § 3.3.3.

L'AC fournit un moyen de communication rapide pour faciliter la révocation sécurisée et authentifiée de ce qui suit:

a) un ou plusieurs certificats de un ou plusieurs autorités subordonnées;

b) l'ensemble de tous les certificats émis par l'AC basée sur une seule paire publique / clé privée utilisée par une AC pour générer des certificats d'autorités subordonnées; et

c) tous les certificats d'autorités subordonnées délivrés par l'AC, quelle que soit la paire de clés publique / privée utilisée.

Le dépôt de la demande de révocation est disponible au Guichet de l'ANCE. Un formulaire papier est mis à disposition des Responsables des Autorités Subordonnées pour la révocation des certificats.

Les informations suivantes doivent au moins figurer dans une demande de révocation de certificat :

- l'identité du Responsable de l'Autorité Subordonnée ;
- le nom de l'Autorité Subordonnée ;
- éventuellement, la cause de révocation ;

Le formulaire dûment complété et signé par le Responsable de l'Autorité Subordonnée est communiqué à l'ANCE.

L'AE s'assure d'authentifier la source de la demande de révocation et d'effectuer les contrôles adéquats. L'AE transmet la demande aux composantes chargées de la production des certificats et des LAR. Ces composantes effectuent les contrôles nécessaires pour authentifier la source de la demande et vérifier son intégrité. Est effectuée ensuite la révocation effective et génération de la LAR signée par l'AC Racine.

Le SP se charge ensuite de la publication de la LAR contenant l'information de révocation et met à jour le serveur OCSP.

Les causes de révocation ne sont pas publiées ni dans les LAR ni sur le serveur OCSP.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des Autorités Subordonnées concernés que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC sont décrites dans la « procédure de cessation d'activité ou de changement des composantes de l'AC ».

4.9.4 Délai accordé à une Autorité Subordonnée pour formuler la demande de révocation

Dès que le responsable de l'autorité ou le représentant légal de l'entité a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de autorité subordonnée

Le service de révocation est disponible 24heures sur 24 7jours sur 7. Toute demande de révocation d'un certificat d'une Autorité Subordonnée est traitée dans un délai inférieur à 24 heures. Ce délai couvre la réception de la demande de révocation authentifiée jusqu'à la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la LAR de l'AC Racine.

La révocation d'un certificat de signature de l'AC Racine est effectuée immédiatement, en particulier dans le cas de la compromission de la clé.

4.9.6 Exigences de vérification de révocation par les utilisateurs de certificats

L'UC est tenu de vérifier, avant son utilisation et en particulier lorsque les certificats impliquent des effets juridiques, l'état de ces certificats de l'ensemble de la chaîne de certification correspondante. La validité d'une LAR est contrôlée par vérification de sa signature et vérification de la validité du certificat de l'AC Racine.

4.9.7 Fréquence d'établissement des LAR

La fréquence de publication des LAR est annuelle.

4.9.8 Délai maximum de publication d'une LAR

La publication d'une LAR suite à sa génération doit être effectuée dès que possible.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Les informations de révocation des certificats sont disponibles sur le serveur OCSP à l'adresse ocsp.certification.tn.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre 4.9.6 ci-dessous.

4.9.11 Autres moyens disponibles d'information sur les révocations

Aucun autre moyen d'information sur les révocations n'est prévu dans la présente PC/DPC.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC racine fournit aux UC les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LAR et l'état du certificat de l'AC Racine.

Les LAR sont publiées sur le site web de l'ANCE accessible à l'adresse www.certification.tn et sur l'annuaire ldap.certification.tn accessible à travers le protocole LDAP V3.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24heures sur 24 7jours sur 7 sans interruption prévue.

4.10.3 Dispositifs optionnels

Aucun dispositif optionnel n'est disponible.

4.11 Fin de la relation entre l'autorité subordonnée et l'AC

En cas de fin contractuelle, hiérarchique ou réglementaire entre l'AC et le Responsable de l'Autorité Subordonnée avant la fin de validité du certificat, quelle que soit la raison, ce dernier doit être révoqué.

4.12 Séquestre de clé et recouvrement

La clé d'un certificat émis par l'AC Racine n'est en aucun cas séquestrée par une tierce partie ou toute autre entité.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'IGC est installé dans les locaux de l'ANCE. La construction du site respecte les règlements et normes en vigueur, et tient compte des résultats d'une analyse des risques et des exigences spécifiques face à des risques accidentels.

5.1.2 Accès physique

L'infrastructure des composantes de l'IGC est installée dans une enceinte des locaux de l'ANCE dont les accès sont contrôlés et réservés aux seuls personnels habilités. La traçabilité des accès est assurée.

L'ANCE a défini un périmètre de sécurité physique où sont installés les matériels et les logiciels des composantes critiques de l'IGC assurant les opérations de génération des certificats et de gestion des révocations. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans cette PC/DPC.

En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Si des personnes non habilitées doivent pénétrer dans les installations, elles font l'objet d'une prise en charge par une personne habilitée qui en assure la surveillance. Ces personnes doivent en permanence être accompagnées par des personnels habilités.

5.1.3 Alimentation électrique et climatisation

Des systèmes de génération et de protection des installations électriques sont mis en œuvre par l'ANCE pour assurer la disponibilité des systèmes informatiques du site d'exploitation de l'IGC.

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par l'ANCE et leurs fournisseurs. Elles permettent également de respecter les exigences de la présente PC/DPC, ainsi que les engagements pris par l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de prévention contre les dégâts des eaux permettent de respecter les exigences de la présente PC/DPC, ainsi que les engagements pris par l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les mesures de prévention et de lutte contre les incendies mises en œuvre par l'ANCE permettent de respecter les exigences de la présente PC/DPC, ainsi que les engagements

pris par l'AC, en matière de disponibilité de ses fonctions ; en particulier, les fonctions de gestion des révocations, de publication des informations sur l'état de validité des certificats.

5.1.6 Conservation des supports

Les moyens de conservation des supports d'information mis en œuvre par l'ANCE permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC/DPC. Dans le cadre de l'analyse de risque, les supports ainsi que les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis en terme de disponibilité, de confidentialité et d'intégrité des données, notamment celles conservées dans les journaux, les archives et les logiciels utilisées par l'AC. Les détails de classification de ces informations sont établis au niveau de la procédure de classification des biens.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

5.1.7 Mise hors service des supports

Afin d'éviter toute perte de confidentialité, des mécanismes de destruction des supports papiers (tels que des broyeurs) et des supports magnétiques d'information sont mis en œuvre sur le site d'exploitation de l'IGC et mis à la disposition des personnels de confiance.

Les supports de stockage (disque dur) de l'AC ne sont pas réutilisés à d'autres fins avant destruction complète des informations liées à l'AC qu'ils sont susceptibles de contenir.

En fin de vie, les supports sont détruits.

5.1.8 Sauvegardes hors site

L'AC réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services. Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la procédure de sauvegarde.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnes ayant un rôle de confiance de l'IGC sont toutes des personnes habilitées de l'ANCE et elles connaissent et comprennent les implications des opérations dont ils ont la responsabilité. Suite à la séparation des tâches critiques, les rôles de confiance de l'AC sont distingués en cinq groupes :

- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de l'IGC ;
- Les personnels opérationnels, dont la responsabilité est de mettre en œuvre les fonctions d'IGC ;
- Les personnels d'audit, dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de la composante d'IGC ;

- Les personnels de sécurité, dont la responsabilité est de mettre en œuvre la politique de sécurité des systèmes d'informations, en particulier, la gestion des contrôles physiques aux équipements des systèmes des composantes et l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, ou autre évènement ;
- Porteurs de secrets et de données d'activation.

5.2.2 Nombre de personnes requises par tâche

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement participer, peuvent être différents. La procédure de gestion des rôles et des responsabilités de l'ANCE définit le nombre de personnes requises pour chaque opération.

5.2.3 Identification et authentification pour chaque rôle

Avant l'attribution des rôles et les autorisations correspondantes, l'ANCE effectue toutes les vérifications nécessaires des personnels amenés à travailler au sein des entités opérant les composantes de l'AC.

Chaque attribution d'un rôle à un membre du personnel de l'AC est notifiée par écrit. Le responsable de Sécurité est informé de chaque nomination.

Les contrôles et les vérifications effectués sont décrits dans la procédure de gestion des rôles et des responsabilités de l'ANCE et sont conformes à la politique de sécurité des systèmes d'informations.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Les attributions associées à chaque rôle sont décrites dans la procédure de gestion des rôles et des responsabilités de l'ANCE et sont conformes à la politique de sécurité des systèmes d'informations.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

L'ANCE s'assure que les attributions de ses personnels, amenés à travailler au sein de l'IGC, correspondent à leurs compétences professionnelles conformément à la procédure de recrutement.

Chaque personne amenée à travailler au sein de l'AC est soumise à un devoir de réserve et aux clauses de confidentialité vis-à-vis de l'ANCE. Elle est informée de ses responsabilités en lien avec les services de l'IGC et la politique de sécurité des systèmes d'informations en vigueur au sein de l'AC.

5.3.2 Procédures de vérification des antécédents

L'ANCE s'assure de l'honnêteté de ses personnels amenés à travailler au sein de l'IGC en vérifiant lors de leur recrutement qu'ils n'ont pas eu de condamnation de justice en

contradiction avec leurs attributions. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3 Exigences en matière de formation initiale

Le personnel de l'IGC a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité mises en œuvre conformément à la procédure de recrutement.

Le personnel a eu connaissance et est réputé avoir compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures et dans l'organisation, en fonction de la nature de ces évolutions. L'AC établit annuellement un plan de formation conformément à la procédure de formation. L'AC maintient des fiches d'évaluation pour toutes les actions de formation effectuées.

5.3.5 Fréquence et séquences de rotation entre différentes attributions

Toute rotation de personnel de l'AC ne doit pas entraver la continuité et la sécurité des services.

5.3.6 Sanctions en cas d'actions non autorisées

L'ANCE décide des sanctions à appliquer lorsqu'un personnel abuse de ses droits ou bien effectue une opération non conforme à ses attributions conformément au statut du personnel de l'ANCE.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

L'ANCE ne bénéficie pas des services des employés contractuels pour les rôles de confiance définis à la section § 5.2.1.

Dans le cas d'une prestation de service de fournisseurs externes dans les zones de la PKI, la PSSI de l'ANCE décrit la modalité d'accès physique d'une telle prestation.

5.3.8 Documentation fournie au personnel

Le personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales des composantes de l'IGC.

La documentation adéquate, dont doit disposer le personnel en fonction de son besoin d'en connaître pour l'exécution de sa mission, est composée au moins les documents suivants :

- Le statut du personnel de l'ANCE ;
- La charte de sécurité ;
- La PC/DPC ;
- La PSSI ;

- Les procédures internes et les manuels d'exploitation ;
- Les documents techniques relatifs aux matériels et logiciels utilisés.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

5.4.1 Type d'évènements à enregistrer

L'IGC enregistre tous les évènements liés aux services et à la protection de l'AC qu'elle met en œuvre. Les enregistrements des évènements dans un journal contiennent au minimum les informations suivantes :

- le type d'évènement ;
- l'identifiant de l'exécutant et/ou la référence du système déclenchant l'évènement ;
- la date et l'heure de l'évènement ;
- le résultat de l'évènement.

Selon les types d'évènements, les enregistrements comporteront également les champs suivants :

- le destinataire de l'opération ;
- le nom du demandeur de l'opération ou la référence du système effectuant la demande ;
- le nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- la cause de l'évènement ;
- toute information caractérisant l'évènement.

Les opérations de journalisation sont effectuées en tâche de fond tout au long de la vie de l'IGC. L'imputabilité d'une action revient à la personne, à la composante ou au système l'ayant exécutée.

5.4.2 Fréquence de traitement des journaux d'évènements

L'analyse du contenu des journaux d'événements est effectuée de manière régulière par l'AC. La fréquence de traitement des journaux d'évènements est décrite dans la procédure de journalisation des évènements de l'ANCE.

5.4.3 Période de conservation des journaux d'évènements

Des précisions sur la durée de conservation des journaux d'évènements sont fournies dans la procédure de journalisation des évènements de l'ANCE.

5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des

mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. La procédure de journalisation des évènements de l'ANCE et la documentation système précisent les moyens de protection employés.

5.4.5 Procédure de sauvegarde des journaux d'évènements

L'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements, conformément aux exigences de la présente PC/DPC et en fonction des résultats de l'analyse de risque effectuée.

La « procédure de journalisation des évènements » de l'ANCE précise les mesures de sauvegarde des journaux d'évènements.

5.4.6 Système de collecte des journaux d'évènements

Chaque composante de l'IGC est responsable de la collecte des journaux d'évènements la concernant.

5.4.7 Evaluation des vulnérabilités

Toutes les composantes de l'AC sont en mesure de détecter toute tentative de violation de l'intégrité de leur fonctionnement.

Les journaux sont analysés au moins une fois par trimestre. Cette analyse permet de vérifier la concordance entre évènements dépendants et contribuer à révéler toute anomalie. Plus de détails sont à voir dans la procédure de journalisation des évènements de l'ANCE.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données à archiver sont au moins les suivantes :

- la PC/DPC;
- les dossiers complets des demandes de création et de révocation de certificats ;
- les certificats des autorités subordonnées et LAR tels qu'émis ou publiés ;
- les journaux d'évènements des différentes composantes de l'IGC ;
- les fichiers de configuration des équipements informatiques et les logiciels.L'inventaire des données à archiver figure dans la procédure d'archivage.

5.5.2 Période de conservation des archives

Les certificats des autorités subordonnées et d'AC ainsi que les LAR sont archivés 20 ans après leur expiration. Les durées d'archivage des journaux d'évènements sont décrites dans la procédure d'archivage de l'ANCE.

5.5.3 Protection des archives

Les archives sont protégées en intégrité et accessibles aux personnes autorisées pendant tout le temps de leur conservation.

Les moyens et les mesures mis en œuvre pour assurer la protection des archives sont précisés dans la procédure d'archivage de l'ANCE.

5.5.4 Procédure de sauvegarde des archives

Les principes de sauvegarde des archives sont décrits dans la procédure d'archivage de l'ANCE.

5.5.5 Exigences d'horodatage des données

Tous les composants de l'AC sont régulièrement synchronisés avec un serveur Network Time Protocol (NTP).

5.5.6 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (voir § 5.5.3).

5.5.7 Procédures de récupération et de vérification des archives

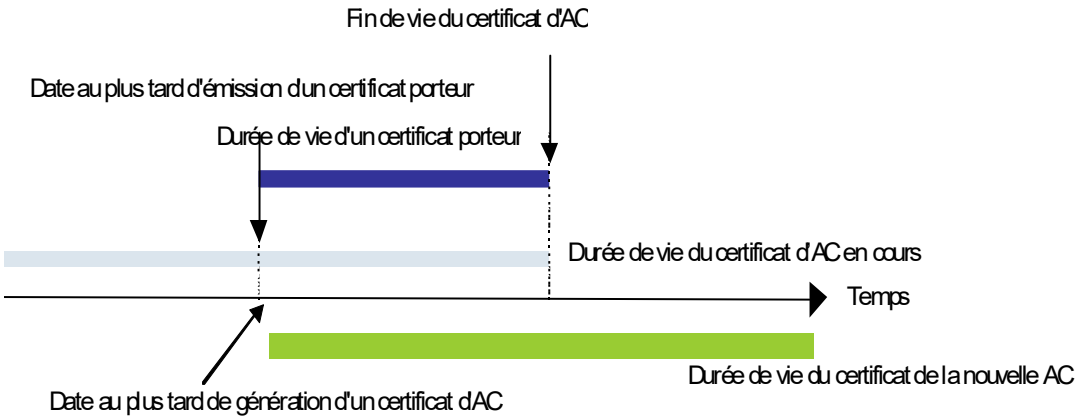
Les archives (papier et électroniques) sont accessibles aux personnes autorisées dans un délai maximum de trois (3) jours ouvrés.

5.6 Changement de clé d'AC

5.6.1 Certificat d'AC

L'AC ne peut pas générer de certificat dont la date de fin de validité serait postérieure à la date d'expiration de la bi-clé de l'AC. Pour cela, la période de validité du certificat de l'AC est supérieure à celle des certificats qu'elle signe.

A partir du moment où une nouvelle clé privée d'AC a été générée pour l'AC et qu'un certificat d'AC a été obtenu par l'AC de niveau supérieur, celle-ci est utilisée dès le début de la période de validité de ce certificat pour générer de nouveaux certificats de autorité subordonnée et les LAR de l'AC pour ces nouveaux certificats. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats autorité subordonnée émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats autorité subordonnée émis à l'aide de cette bi-clé. L'ancienne clé de l'AC sert alors à signer les LAR pour les certificats émis sous cette ancienne clé d'AC.



Une clé d'AC peut être renouvelée par anticipation si :

- la taille d'une clé de l'AC se révèle être insuffisante pour résister aux progrès réalisés pour « casser » les clés ;
- l'algorithme de hachage utilisé pour générer les certificats ou des LAR se révèle être d'une résistance insuffisante pour résister aux collisions.

5.6.2 Certificat de l'autorité subrodonnée

La durée de vie des certificats des Autorités Subordonnées est variable.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Des procédures et des moyens de remontée et de traitement des incidents sont mis en œuvre par l'AC, notamment au travers de l'analyse des différents journaux d'évènements.

Grâce à la sensibilisation et la formation du personnel, ces procédures sont régulièrement appliquées au niveau de chaque composante de l'AC pour détecter l'évènement déclencheur d'un éventuel incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC.

En cas de sinistre, l'IGC dispose d'un plan de reprise d'activité, qui prend en compte les scénarios des sinistres en précisant les modalités de déclenchement et les personnes responsables de ce plan.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

L'AC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente PC/DPC, des engagements de l'AC dans cette PC/DPC et des résultats de l'analyse de risque, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan de continuité est testé au minimum une fois par an.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise, l'ANCE décide, après enquête sur l'évènement, de demander à l'AC de niveau supérieur de révoquer le certificat de l'AC. Ensuite, une nouvelle bi-clé d'AC est générée et un nouveau certificat d'AC est émis. Les personnels de l'IGC et les Autorités subordonnées sont avisés dès que l'ancien certificat de l'AC est révoqué et ils sont aussitôt informés de la capacité retrouvée de l'AC de générer des certificats. Le plan de reprise d'activité apporte plus de détails concernant cette section.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite à la section § 5.7.1. Les scénarios de la procédure de continuité de service précisent les capacités de continuité d'activité des composantes de l'AC.

5.8 Fin de vie d'AC

La fin de vie de l'AC concerne soit un transfert partiel d'activité à une autre entité, soit une cessation totale de l'activité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'AC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec une nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité

Afin d'assurer un niveau de confiance constant pendant et après le transfert d'activité, l'AC s'engage à :

- aviser aussitôt les autorités subordonnées et les utilisateurs de certificats des changements envisagés ;
- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des autorités subordonnées et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LAR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC/DPC.

5.8.2 Cessation d'activité

La cessation d'activité peut être totale ou partielle, typiquement, la cessation d'activité pour une famille de certificats donnée seulement.

En cas de cessation partielle d'activité, l'AC s'engage à :

- en informer à l'avance, via le SP, les Autorités subordonnées et les utilisateurs de certificats (UC) ;
- continuer à assurer la révocation des certificats et la publication des LAR conformément aux engagements pris dans la présente PC/DPC, le temps que les autorités subordonnées soient équipés de nouveaux certificats, et au plus tard jusqu'à la fin de validité du dernier certificat émis.

En cas d'une cessation totale d'activité, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, s'engage à :

- prévenir les Autorités subordonnées et les utilisateurs de certificats via le SP ou tout autre moyen ;
- révoquer l'ensemble des certificats émis par l'AC ;
- mettre à disposition des porteurs des outils permettant la détection des certificats révoqués ;
- s'interdire de transmettre à quiconque les clés privées lui ayant permis d'émettre des certificats ou des LAR ;
- détruire les clés privées et toutes les copies de sauvegarde des clés privées lui ayant permis d'émettre des certificats ou des LAR.

Dans le cas où cette cessation totale d'activité s'opère suite à un retrait de l'autorisation du fournisseur de services de certification, et en conformité avec l'article 11 du décret 2001-1668 du 17 juillet 2001, l'AC subordonnée s'engage à :

- en informer, au moins un mois à l'avance, via le SP, les utilisateurs de certificats (UC) ;
- informer les UC de la possibilité de refuser le transfert envisagé ainsi que les délais et les modifications de refus ;
- détruire les clés privées, les certificats et les données personnelles restant chez le fournisseur, en présence de l'ANCE.

6 Mesures de sécurité techniques

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature de l'AC est effectuée dans un environnement sécurisé.

Les clés de signature d'AC sont générées lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle conforme aux exigences du niveau de sécurité considéré (FIPS 140-2 niveau 3).

Les dispositifs cryptographiques utilisés pour la génération de clés d'AC utilisent un générateur de nombres aléatoires (RNG) comme définie dans les spécifications techniques correspondantes.

Durant ces cérémonies, toutes les opérations sont effectuées dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance en suivant des scripts préalablement définis.

Les cérémonies de clés se déroulent dans les locaux de l'ANCE sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

Les manipulations des codes PIN et des codes d'authentification sont effectuées dans un environnement protégé contre les risques de fuites d'information par vidéo-surveillance.

6.1.1.2 Clés des autorités subordonnées générées par l'AC racine

Sans objet.

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 Clé privée de l'AC

La clé privée de l'AC est la propriété de l'ANCE. Elle est générée et protégée au niveau d'un module cryptographique situé dans les locaux sécurisés de l'ANCE.

6.1.2.2 Clé privées des Autorités subordonnées

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique d'une Autorité subordonnée est protégée en intégrité et son origine authentifiée lorsqu'elle est transmise de et vers l'AC Racine.

La clé publique d'une Autorité subordonnée est transmise sous forme pkcs#10.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat de l'AC Racine et l'empreinte de ce certificat sont publiés sur le site internet de l'ANCE : http://www.certification.tn.

6.1.5 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat de l'AC racine et l'empreinte de ce certificat sont publiés sur le site web de l'ANCE : http://www.certification.tn.

6.1.6 Taille des clés

6.1.6.1 Certificat AC

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats d'AC doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé. La taille des bi-clés de l'AC Racine est de 4096 bits.

6.1.6.2 Certificat d'Autorité Subordonnée

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats autorité subordonnée doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé pour les certificats des Autorités subordonnées. La taille des bi-clés est de 4096 bits.

6.1.7 Vérification de la génération des paramètres des bi-clés et de leur qualité

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles certifiées FIPS140-2 niveau 3.

6.1.8 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LAR.

L'utilisation de la clé privée d'Autorité Subordonnée et du certificat d'authentification associé est strictement limitée au service de signature de certificats et de LCR.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

L'AC dispose de modules cryptographiques FIPS 140-2 niveau 3 qui assurent la protection des clés avec un niveau de sécurité jugé acceptable au regard des menaces pesant sur l'intégrité, la disponibilité et la confidentialité des bi-clés.

Les ressources cryptographiques matérielles de l'AC utilisent des générateurs d'aléas qui sont conformes à l'état de l'art, et aux standards en vigueur. Les algorithmes utilisés pour générer l'aléa de départ sont conformes aux standards en vigueur.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC Racine est assuré par du personnel de confianceen suivant la méthode d'authentification M of N.

L'initialisation des modules cryptographiques est contrôlée via la mise en œuvre d'un processus de partage des secrets où les opérateurs de confiance intervenant doivent s'authentifier.

6.2.3 Séquestre de clé privée

Ni les clés privées d'AC, ni les clés privées des Autorités subordonnées ne sont séquestrées.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clé privée d'AC

Les copies de secours des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs acteurs du personnel de confiance à des fins de disponibilité. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

6.2.4.2 Clés privées des Autorités Subordonnées

Sans objet.

6.2.5 Archivage des clés privées

Les clés privées de l'AC ne sont en aucun cas archivées.

6.2.6 Transfert de la clé privée vers ou depuis le module cryptographique

Tout transfert d'une clé privée de l'AC vers / depuis le module cryptographique à des fins de restauration ou de sauvegarde se fait sous forme chiffrée moyennant le module cryptographique associé.

6.2.7 Stockage des clés privées de l'AC dans un module cryptographique

Les clés privées de l'AC sont stockées dans des ressources cryptographiques matérielles, répondant au minimum aux exigences du niveau de sécurité considéré. Les clés privées stockées sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation et fait intervenir initialement au moins trois porteurs de secrets dans des rôles de confiance.

6.2.8.2 Clés privées des autorités subordonnées

Sans objet.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès qu'il y arrêt ou déconnexion du module.

Les ressources cryptographiques sont stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

6.2.9.2 Clés privées des autorités subordonnées

Sans objet.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Une clé privée d'AC est détruite en fin de vie de cette clé privée, normale ou anticipée ; en particulier, quand le certificat auquel elle correspond est expiré ou révoqué.

L'autorisation de destruction d'une clé privée d'AC et la méthode correspondante sont décrites dans la « procédure de cessation d'activité ou de changement des composantes de l'AC ».

La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et ainsi que tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des autorités subordonnées

Une clé privée d'une autorité subordonnée est détruite en fin de vie de cette clé privée, normale ou anticipée ; en particulier, quand le certificat auquel elle correspond est expiré ou révoqué.

L'autorisation de destruction d'une clé privée d'AC et la méthode correspondante sont décrites dans la « procédure de cessation d'activité ou de changement des composantes de l'AC »

La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et ainsi que tout élément permettant de la reconstituer.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs

Se reporter au § 6.2.1.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des autorités subordonnées sont archivées dans le cadre de l'archivage des certificats correspondants.

Les moyens et les mesures mis en œuvre pour assurer la protection des archives sont précisés dans la procédure d'archivage de l'ANCE.

6.3.2 Durées de vie des bi-clés et des certificats

La durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

L'AC Racine ne peut pas émettre des certificats des Autorités Subordonnées dont la durée de vie est supérieure à celle de son certificat (se reporter à § 5.6).

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération des données d'activation permettant d'initialiser un module cryptographique se fait selon un schéma de type M parmi N lors de la phase d'initialisation et de personnalisation de ce module durant les cérémonies de clés (Voir § 5.2.1). Ces données d'activation sont choisies et saisies par les responsables de ces données eux-mêmes. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués et qui sont détaillés dans le document « Cérémonie des clés de l'autorité de certification racine dans la PKI de l'ANCE » .Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Génération et installation des données d'activation correspondant à une clé privée de l'autorité subordonnée

Sans objet.

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant aux clés privées de l'AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation et de secrets sont responsables de leur gestion et de leur protection. Un porteur de secret ne peut détenir plus d'une donnée d'activation d'une même clé d'AC à un même instant.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des autorités subordonnées

Sans objet.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

L'ANCE a effectué une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. La PSSI a été élaborée en fonction de cette analyse.

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur l'infrastructure informatique des composantes de l'IGC est défini dans la PSSI. Cette dernière répond aux objectifs de sécurité suivants :

- identification et authentification des utilisateurs pour l'accès au système ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression des droits d'accès ;
- protection du réseau contre les intrusions et pour l'assurance de la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières, découlant de l'analyse de risque.

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système sont mis en place.

6.5.2 Niveau de qualification des systèmes informatiques

Les mesures de sécurité relatives à l'IGC découlent d'une analyse de risques. Le module cryptographique mis en œuvre a fait l'objet d'une certification FIPS 140-2 niveau 3.

6.6 Mesures de sécurité liées au développement des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- les logiciels et les matériels sont acquis de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point est défini et documenté. Les logiciels auxquelles cette exigence ne s'applique pas sont acquises auprès de sources autorisées ;
- les matériels et logiciels dédiés à l'IGC ne sont pas utilisés pour d'autres activités autres que celles de l'AC ;
- les logiciels de l'AC font l'objet d'une recherche de codes malveillants avant leur première utilisation et périodiquement par la suite ;
- les mises à jour des matériels et logiciels sont installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.1 Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC. Toute modification non autorisée du logiciel ou de la configuration de l'AC est détectée par des mécanismes mis en œuvre.

Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'AC. Lors de son premier chargement, on s'assure que le logiciel de l'AC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

6.6.2 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, l'AC poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mesures de sécurité réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle. Les composantes accessibles de l'IGC sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système IGC est hébergé refuse tout service, hormis ceux qui sont

nécessaires au système IGC, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

Les équipements du réseau local utilisé par l'AC sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

6.8 Horodatage/Système de datation

Toutes les composantes de l'AC sont régulièrement synchronisées au moyen d'un serveur NTP (Network Time Protocol). Le temps fourni par ce serveur de temps est utilisé en particulier pour établir une datation sûre de :

- début de validité d'un certificat autorité subordonnée ;
- début de la révocation d'un certificat autorité subordonnée ;
- de l'inscription des évènements dans les journaux.

7 Profils des certificats et des LAR

Ce chapitre traite des exigences relatives aux profils des certificats X.509 v3 de l'AC racine ou émis par celle-ci, ainsi que des profils des LAR. Les certificats émis selon la présente PC/DPC sont conformes au RFC 5280.

7.1 Profil de Certificats

Les certificats émis par l'AC racine sont des certificats au format X.509 v3. Les champs des certificats de l'AC et des autorités subordonnées sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat d'AC

Les informations principales contenues dans le certificat de l'AC racine sont :

Champ de base	Valeur
Version	2 (= version 3)
Serial Number	128 bit
Issuer	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
Not Before	début de la période de validité du certificat
Not After	fin de la période de validité du certificat
Subject	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
Subject Public Key	Clé publique de l'AC racine
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Extensions

Champ de base	Criticité	Valeur
Key Usage	Critique	Certificate Sign et CRL Sign
		Certificat de l'AC émettrice : http://www.certification.tn/pub/TunRootCA2.crt
Basic Constraints	Critique	CA:TRUE, pathlen:1
Crl Distribution Points	non critique	Indique l'adresse HTTP où est publiée la LCR : http://crl.certification.tn/TunRootCA2.crl

7.1.1.2 Certificat de l'autorité subordonnée

Les informations principales contenues dans le certificat de l'autorité subordonnée sont :

Champ de base	Valeur
Version	2 (= version 3)
Serial Number	128 bit
Issuer	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
Not Before	début de la période de validité du certificat
Not After	fin de la période de validité du certificat
Subject	C=TN O=(Exigé) CN=(Exigé)
Subject Public Key	Clé publique de l'AC subordonnée
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Extensions

Champ de base	Criticité	Valeur
Key Usage	Critique	Certificate Sign et CRL Sign
Authority Information Access	non-critique	OCSP : http://ocsp.certification.tn
		Certificat de l'AC émettrice : http://www.certification.tn/pub/TunRootCA2.crt
Basic Constraints	Critique	CA:TRUE, pathlen:0
CRL Distribution Points	non critique	Indique l'adresse HTTP où est publiée la LCR

7.2 Profil des LAR

Les caractéristiques des LAR sont :

Champ de base	Valeur
version	1 (= version 2)
signature	sha256WithRSAEncryption OID:1.2.840.113549.1.1.11
issuer	C=TN

Champ de base	Valeur
	O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
This Update	Date et heure UTC de génération de la LAR
Next Update	Date et heure UTC de la mise à jour au plus tard de la LAR
Revoked Certificates	Liste des numéros de série des certificats révoqués ainsi que leur date de révocation.

Extensions

Champ de base	Criticité	Valeur
Crl Number	Extension non critique	nombre entier incrémenté

Autres caractéristiques :

Caractéristiques d'une LAR :	Durée de validité : 365j Périodicité de mise à jour : 300j

8 Audit de conformité et autres évaluations

Le présent chapitre concerne les audits et évaluations de la responsabilité de l'ANCE.

L'AC racine doit être intégrée au plan d'audit interne de l'ANCE.

Ces audits ont pour objet la validation du bon fonctionnement de son IGC, et la validation de la conformité de l'implémentation, de l'utilisation et de l'opération de l'AC telles que décrites au sein de la PC/DPC ; ainsi que vis-à-vis de la norme ETSI TS 102 042.

Un audit peut également avoir pour objet la vérification de l'absence de corruption ou d'atteinte aux services et données de l'AC, et l'absence de vulnérabilités sur ses services, qui peuvent être exploitées pour réaliser de telles corruptions.

8.1 Fréquences et / ou circonstances des évaluations

Dans le cadre de qualification ETSI, L'AC racine fait l'objet d'audit périodique de conformité au moins une fois par an.

Les audits de contrôle peuvent être effectués périodiquement ou lorsque l'ANCE reçoit des informations suspectes concernant la sécurité de l'AC racine.

En outre, suite à tout changement majeur dans son IGC, l'ANCE doit organiser un audit de conformité.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est effectué par une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée. L'équipe d'audit peut être interne ou externe à l'ANCE.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante contrôlée, quelle que soit cette composante. Elle est dûment autorisée à pratiquer les contrôles visés. Si l'AC entière est contrôlée, l'équipe d'audit ne doit pas faire partir des divisions opérationnelles de l'AC.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC/DPC, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.)

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis aux responsables de l'AC racine parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations au responsable d'exploitation qui peuvent être la cessation

(temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par le responsable d'exploitation et doit respecter ses politiques de sécurité internes.

- En cas de résultat "A confirmer", le responsable d'exploitation remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, le responsable d'exploitation confirme à la composante contrôlée la conformité aux exigences de la présente PC/ DPC.

8.6 Communication des résultats

A l'issue d'un audit de conformité, un rapport de contrôle de conformité, citant les versions des PC/DPC utilisées pour cette évaluation et, si besoin, incluant la mention des mesures correctives à appliquer par la composante, est remis à l'ANCE.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Les conditions tarifaires en vigueur pour l'acquisition ou le renouvellement de certificats sont publiées sur le site web http://www.certification.tn.

La mise à jour des tarifs passe par le conseil d'administration. Après avis favorable de ce dernier l'ANCE transmet la proposition au ministère pour validation.

Avant la mise en exécution des nouveaux tarifs l'ANCE s'engage à notifier ses clients et ses partenaires dans un délai d'un mois au minimum en leurs transmettant la date d'entrée en vigueur de ces tarifs.

9.1.2 Tarifs pour accéder aux certificats

L'accès aux certificats ne fait pas l'objet de facturation particulière de la part de l'ANCE.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Le service d'accès aux informations d'état et de révocation des certificats, qu'il s'agisse de la LAR ou du serveur OCSP, ne fait pas l'objet d'une facturation particulière de la part de l'ANCE.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

L'ANCE ne rembourse pas les frais de certificats électronique car l'acceptation de tout dossier n'est faite que si le dossier est complet. Un dossier incomplet est rejeté automatiquement.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

La présente PC/DPC ne formule pas d'exigences particulières concernant une souscription spécifique d'assurance.

9.2.2 Autres ressources

La présente PC/DPC ne formule aucune exigence sur ce point.

9.2.3 Couverture et garantie concernant les entités utilisatrices

La présente PC/DPC ne formule pas d'exigence sur ce point.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes (liste non exhaustive) sont considérées comme confidentielles :

- les clés privées des certificats d'AC ;
- les données d'activation associées aux bi-clés cryptographiques ;
- les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques ;
- les journaux d'événements des composantes d'AC ;
- les rapports d'audits ;
- les causes de révocation ;
- les informations techniques relatives à la sécurité des fonctionnements de certaines composantes d'IGC.

9.3.2 Informations hors du périmètre des informations confidentielles

Les informations publiées par le SP sont considérées comme non confidentielles.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC respecte la législation en vigueur sur le territoire tunisien.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'ANCE opère son IGC conformément à la législation tunisienne en vigueur sur le sujet.

9.4.2 Informations à caractère personnel

Sans objet.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

Sans objet.

9.4.5 Notification et consentement d'utilisation des données personnelles

Sans objet.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Sans objet.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits relatifs à la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'ANCE sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de non-respect.

- **loi n°2007 -50 du 23 juillet 2007** modifiant et complétant la loi n°2001 -36 du 17 avril 2001 relative a la protection des marques de fabrique, de commerce et de services

-**Loi n°2001-58 du 7 juin 2001** autorisant l'adhésion de la Tunisie au traité international de coopération en matière de Brevets.

-**Loi n°2000-84 du 24 août 2000** définit clairement la terminologie utilisée, traite du droit au brevet, de la procédure de la demande de brevet, de la délivrance du brevet, des recours, des droits et obligations découlant du brevet, de la renonciation de la nullité et de la déchéance, de la transmission, de la cession, et de la saisie des droits ; des licences contractuelles, des licences obligatoires, des licences d'office, de la contrefaçon et des sanctions associées et enfin des mesures à la frontière.

Décret, fixe le montant des redevances afférentes aux brevets d'invention.

-**Décret n°2001-275O du 26 novembre 2001**, fixe les critères et modalités de partage des produits d'exploitation des brevets d'invention ou de découverte revenant à l'établissement, à l'entreprise publiques et à l'agent public chercheur auteur d'une invention ou découverte

De même l'Institut National de la Normalisation et de la Propriété Industrielle (**INNORPI**) est considéré comme l'opérateur national de la protection de la propriété Industrielle.

9.6 Interprétations contractuelles et garanties

L'AC a pour obligation de :

- respecter et appliquer la présente PC/DPC;
- respecter les clauses qui la lient aux Responsables d'Autorité Subordonnée et aux utilisateurs de certificats ;
- se soumettre aux contrôles de conformité effectués par l'auditeur mandatée par l'AC et/ou l'organisme de qualification.

9.6.1 Autorités de Certification

L'AC Racine est responsable vis-à-vis de ses clients, bénéficiaires, mandataires de certification et tiers utilisateurs des opérations relatives aux services de certification réalisées par l'une des composantes de l'IGC. En particulier, l'AC Racine s'engage à :

- Pouvoir démontrer le lien entre une Autorité Subordonnée et son certificat, conformément aux exigences de la section § 0 ci-dessus ;
- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- Garantir et maintenir la cohérence des PC/DPC avec les services de l'IGC ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- Documenter les procédures internes de fonctionnement ;
- Vérifier régulièrement l'intégrité de ses services et données ;
- Apporter les mesures nécessaires à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs.

9.6.2 Service d'enregistrement

L'AE de l'AC Racine se conforme à toutes les obligations pertinentes de l'AC définies dans la section ci-dessus en se restreignant aux services qu'elle met en œuvre dans le cadre de la présente PC/DPC.

9.6.3 Responsable des Autorités Subordonnées

Les Responsables des Autorités Subordonnées doivent se conformer à toutes les exigences de la présente PC/DPC. Ils se conforment aux obligations suivantes :

- Respecter les termes du contrat le liant à l'AC ;
- Garantir que les informations fournies à l'ANCE concernant son identification ou celle de l'entité identifiée sont exactes, complètes et que les documents communiqués sont valides ;
- S'engager en cas de perte ou vol de la clé privée, à demander la révocation des certificats dans les plus brefs délais.

9.6.4 Utilisateurs de certificats

Les Utilisateurs de Certificat (UC) doivent se conformer à toutes les exigences de la présente PC/DPC. Ils s'engagent notamment à :

- Déclarer à l'AC les usages prévus des certificats émis selon la présente PC/DPC, via le formulaire de demande, et respecter ces usages par la suite, dans le respect de la législation en vigueur ;
- Respecter les termes des CGU ;
- Utiliser des logiciels qui sont à même de vérifier que le certificat :
  - n'est en dehors de sa période de validité au moment de son utilisation,
  - n'est pas révoqué,
  - est effectivement utilisé selon l'usage prescrit dans le certificat.

9.6.5 Autres participants

La PC/DPC ne précise pas d'autres participants

9.7 Limite de garantie

L'AC garantit au travers de ses différents services la gestion des certificats correspondants et des informations de validité des certificats selon la présente PC/DPC.

Aucune autre garantie ne peut être assurée par l'AC.

9.8 Limites de responsabilité

La responsabilité de l'ANCE est limitée à la fourniture de certificats conformes aux exigences de la présente PC/DPC.

L'usage des certificats fournis est strictement limité aux cas d'usage prévus dans la présente PC/DPC. En aucun cas l'ANCE ne peut être tenue responsable de tout manquement d'une autorité subordonnée ou d'un UC ayant été informé de ses obligations.

En outre, l'ANCE ne saurait être tenue responsable pour tout dommage causé lors de l'utilisation d'un certificat, dont :

- Perte de profits ;
- Perte de données ;
- Dommages indirects ou consécutifs suite à ou en connexion avec l'utilisation, la livraison, la licence, la performance ou non des certificats émis ou des signatures ;
- Tout autre dommage excepté ceux dus à une confiance dans les informations vérifiées contenues dans les certificats.

La responsabilité de l'Autorité Subordonnée est engagée en cas d'erreur dans les informations vérifiées des certificats résultant d'une fraude ou de manquement.

9.9 Indemnités

La présente PC/DPC de Certification ne présente pas d'exigence à ce sujet.

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

La présente PC/DPC doit rester en application au moins jusqu'à la fin de validité du dernier certificat émis selon cette PC/DPC.

9.10.2 Fin anticipée de validité

En fonction de la nature et de l'importance des modifications apportées à la présente PC/DPC, le délai de mise en conformité sera établi en fonction de la règlementation en vigueur.

Sauf cas exceptionnel lié aux modifications des exigences de sécurité, la mise à jour de la présente PC/DPC n'impose pas le renouvellement anticipé des certificats déjà émis.

9.10.3 Effets de la fin de validité et clauses restant applicables

La présente PC/DPC ne formule pas d'exigences à ce sujet.

9.11 Notifications individuelles et communication entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12 Amendements à la PC/DPC

9.12.1 Procédures d'amendements

L'AC s'engage à contrôler que tout projet d'amendement à la présente PC/DPC reste conforme à la réglementation tunisienne en vigueur ainsi qu'aux exigences du standard ETSI TS 102 042.

9.12.2 Mécanisme et période d'information sur les amendements

Il n'est pas prévu de révision systématique et périodique de la présente PC/DPC.

Dans le cas où une évolution se présente, l'AC est responsable de l'évaluation de la nécessité de l'application d'une mise à jour de la PC/DPC. Elle donne un préavis de deux mois au moins aux composantes de l'AC de son projet d'amendement avant de procéder aux changements et en fonction de l'objet de la modification.

9.12.3 Circonstances selon lesquelles un OID doit être changé

L'OID de la PC/DPC est modifié à chaque application de toute évolution ayant un impact majeur sur les certificats déjà émis.

9.13 Dispositions concernant la résolution de conflits

En cas de contestation ou de litige, toute partie doit notifier l'ANCE par lettre recommandée avec avis de réception. L'ANCE s'engage à traiter ces notifications et de fournir une réponse dans un délai de trente (30) jours.

Les requêtes sont adressées directement ou par l'entremise d'un avocat au directeur de l'ANCE, par lettre recommandé avec accusé de réception
La requête doit comporter les indications suivantes :

-La dénomination, la forme juridique, le siège social du demandeur et le cas échéant, le numéro d'immatriculation au registre de commerce,

-La dénomination et le siège social du défendeur ;

-Un exposé détaillé de l'objet du litige et les demandes.

-La requête doit être accompagnée de tous les documents, les correspondances et les moyens de preuve préliminaire.

-Le bureau d'ordre de l'agence est chargé de l'enregistrement de la requête selon son numéro et sa date, dans le registre des affaires.

- le litige peut être réglé a l'amiable.

- En cas d'échec de la tentative de conciliation, ce sont les tribunaux de l'Ariana qui sont compétents.

9.14 Juridictions compétentes

La législation et la réglementation en vigueur sur le territoire tunisien sont appliquées.

9.15 Conformité aux législations et réglementations

La présente PC/DPC est sujette aux textes législatifs et réglementaires applicables sur le territoire tunisien.

9.16 Dispositions diverses

9.16.1 Accord global

ANCE valide tous les éventuels accords passés avec les partenaires.

9.16.2 Transfert d'activités

Voir la section § 5.8.

9.16.3 Conséquences d'une clause non valide

Dans le cas d'une clause non valide de la présente PC/DPC, la validité des autres dispositions n'est en rien affectée. La PC/DPC continue à s'appliquer en l'absence de la clause inapplicable tout en respectant l'intention des parties concernées.

Les conséquences seront traitées en fonction de la législation en vigueur.

9.16.4 Application et renonciation

La présente PC/DPC ne formule pas d'exigence spécifique sur le sujet.

9.16.5 Force majeure

Sont considérés comme cas de force majeure la survenance des évènements irrésistibles, insurmontables et imprévisibles.

L'AC ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux FSCE.

9.17 Autres dispositions

Sans objet.

10 Références

Les documents référencés sont les suivants :

Réf.	Document
[X.509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. 6 th Edition. Version de novembre 2008. Disponible à l'adresse : http://www.x500standard.com/index.php?n=Ig.LatestAvail.
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003. Disponible à l'adresse : http://www.ietf.org/rfc/rfc3647.txt
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[ETSI]	European Telecommunications Standards Institute – ETSI TS 102 042 V2.1.1 (2009-05) – Electronic Signatures and Infrastructures (ESI): Policy requirements for certifications authorities issuing public key infrastructures
[BR-PTC]	CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates". v.1.2.3