Agence Nationale de Certification Electronique

Politique de certification et Déclaration des pratiques de certifications de l'autorité TN CEV

Rev	Date	Nature de la révision	Page
Rev 00	15/06/2017	Première Rédaction	Toutes les pages

	Elaboré par	Validé par	Approuvé par
Fonction :	ANCE	Comité du projet 2D-DOC	Directeur Général
Date :	03/03/2017	09/06/2017	15/06/2017
Visa :			

TABLE DES MATIÈRES

1 INTRODUCTION 10
1.1 Présentation générale 10
1.2 Identification du document 10
1.3 Définitions et acronymes 10
1.3.1 Acronymes 10
1.3.2 Définitions 12
1.4 Entités intervenant dans l'IGC 15
1.4.1 Autorité de Certification 15
1.4.2 Autorité d'Enregistrement 16
1.4.3 Responsables de certificats de cachets 17
1.4.4 Utilisateurs de certificats 17
1.5 Usage des certificats 18
1.5.1 Domaines d'utilisation applicables 18
1.5.2 Domaines d'utilisation interdits 18
1.6 Gestion de la PC/DPC 18
1.6.1 Entité gérant la PC/DPC 18
1.6.2 Point de contact 19
1.6.3 Procédures d'approbation de la conformité de la PC/DPC 19
2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES 19
2.1 Entités chargées de la mise à disposition des informations 19
2.2 Informations devant être publiées 19
2.3 Délais et fréquences de publication 19
2.4 Contrôle d'accès aux informations publiées 20
3 IDENTIFICATION ET AUTHENTIFICATION 20
3.1 Nommage 20
3.1.1 Types de noms 20
3.1.2 Nécessité d'utilisation de noms explicites 20
3.1.3 Anonymisation ou pseudonymisation de serveurs 21
3.1.4 Règles d'interprétation des différentes formes de noms 21

3.1.5 Unicité des noms 21
3.1.6 Identification, authentification et rôle des marques déposées 21
3.2 Validation initiale de l'identité 21
3.2.1 Méthode pour prouver la possession de la clé privée 21
3.2.2 Validation de l'identité d'un organisme 22
3.2.3 Informations non vérifiées du RCC et/ou du serveur informatique 23
3.3 Identification et validation d'une demande de renouvellement de clés 23
3.3.1 Identification et validation pour un renouvellement courant 23
3.3.2 Identification et validation pour un renouvellement après révocation 23
3.4 Identification et validation d'une demande de révocation 23
4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 24
4.1 Demande de certificat 24
4.1.1 Origine d'une demande de certificat 24
4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificats 24
4.2 Traitement d'une demande de certificat 25
4.2.1 Exécution des processus d'identification et de validation de la demande 25
4.2.2 Acceptation ou rejet de la demande 25
4.2.3 Durée d'établissement du certificat 25
4.3 Délivrance du certificat 25
4.3.1 Actions de l'AC concernant la délivrance du certificat 25
4.3.2 Notification par l'AC de la délivrance du certificat au RCC 26
4.4 Acceptation du certificat 26
4.4.1 Démarche d'acceptation du certificat 26
4.4.2 Publication du certificat 26
4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat 26
4.5 Usages de la bi-clé et du certificat 26
4.5.1 Utilisation de la clé privée et du certificat par le RCC 26
4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat 26
4.6 Renouvellement d'un certificat 26
4.7 Délivrance d'un nouveau certificat suite à un changement de la bi-clé 27
4.7.1 Causes possibles de changement de bi-clé 27
4.7.2 Origine d'une demande de nouveau certificat 27

4.7.3 Procédure de traitement d'une demande de nouveau certificat 27
4.7.4 Notification au RCC de l'établissement du nouveau certificat..... 27
4.7.5 Démarche d'acceptation du nouveau certificat..... 27
4.7.6 Publication du nouveau certificat..... 27
4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat..... 28
4.8 Modification du certificat..... 28
4.9 Révocation et Suspension des certificats..... 28
4.9.1 Causes possibles d'une révocation..... 28
4.9.2 Origine d'une demande de révocation..... 29
4.9.3 Procédure de traitement d'une demande de révocation 29
4.9.4 Délai accordé au RCC pour formuler la demande de révocation..... 30
4.9.5 Délai de traitement par l'AC d'une demande de révocation 30
4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats..... 30
4.9.7 Fréquence d'établissement des LCR..... 30
4.9.8 Délai maximum de publication d'une LCR..... 30
4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats31
4.9.10 Exigences sur la vérification en ligne de la révocation et l'état des certificats..... 31
4.9.11 Autres moyens disponibles d'information sur les révocations 31
4.9.12 Exigences spécifiques en cas de compromission de la clé privée 31
4.9.13 Causes possibles d'une suspension..... 31
4.9.14 Origine d'une demande de suspension..... 31
4.9.15 Procédure de traitement d'une demande de suspension..... 31
4.9.16 Limites de la période de suspension d'un certificat..... 31
4.10 Fonction d'information sur l'état des certificats..... 31
4.10.1 Caractéristiques opérationnelles..... 31
4.10.2 Disponibilité de la fonction..... 32
4.11 Fin de la relation entre le RCC et l'AC..... 32
4.12 Séquestre de clé et recouvrement 32
5 MESURES DE SECURITE NON TECHNIQUES..... 33
5.1 Mesures de sécurité physique..... 33
5.1.1 Situation géographique et construction des sites..... 33

5.1.2 Accès physique 33
5.1.3 Alimentation électrique et climatisation 33
5.1.4 Vulnérabilité aux dégâts des eaux 33
5.1.5 Prévention et protection incendie 33
5.1.6 Conservation des supports 34
5.1.7 Mise hors service des supports 34
5.1.8 Sauvegardes hors site 34
5.2 Mesures de sécurité procédurales 34
5.2.1 Rôles de confiance 34
5.2.2 Nombre de personnes requises par tâche 35
5.2.3 Identification et authentification pour chaque rôle 35
5.2.4 Rôles exigeant une séparation des attributions 35
5.3 Mesures de sécurité vis-à-vis du personnel 35
5.3.1 Qualifications, compétences et habilitations requises 35
5.3.2 Procédures de vérification des antécédents 35
5.3.3 Exigences en matière de formation initiale 36
5.3.4 Exigences et fréquence en matière de formation continue 36
5.3.5 Fréquence et séquence de rotation entre différentes attributions 36
5.3.6 Sanctions en cas d'actions non autorisées 36
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 36
5.3.8 Documentation fournie au personnel 36
5.4 Procédures de constitution des données d'audit 37
5.4.1 Type d'évènements à enregistrer 37
5.4.2 Fréquence de traitement des journaux d'évènements 38
5.4.3 Période de conservation des journaux d'évènements 38
5.4.4 Protection des journaux d'évènements 38
5.4.5 Procédure de sauvegarde des journaux d'évènements 39
5.4.6 Système de collecte des journaux d'évènements 39
5.4.7 Evaluation des vulnérabilités 39
5.5 Archivage des données 39
5.5.1 Types de données à archiver 39
5.5.2 Période de conservation des archives 39

5.5.3 Protection des archives 40
5.5.4 Exigences d'horodatage des données 40
5.5.5 Système de collecte des archives 40
5.5.6 Procédures de récupération et de vérification des archives 40
5.6 Changement de la clé d'AC 40
5.7 Reprise suite à compromission et sinistre 40
5.7.1 Procédures de remontée et de traitement des incidents et des compromissions 40
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 41
5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante . 41
5.7.4 Capacités de continuité d'activité suite à un sinistre 41
5.8 Fin de vie de l'IGC 41
5.8.1 Transfert d'activité 41
5.8.2 Cessation d'activité 42
6 MESURES DE SECURITE TECHNIQUES 43
6.1 Génération et installation des bi-clés 43
6.1.1 Génération des bi-clés 43
6.1.2 Transmission de la clé privée au serveur 43
6.1.3 Transmission de la clé publique à l'AC 43
6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats 44
6.1.5 Tailles des clés 44
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 44
6.1.7 Objectifs d'usages de la clé 44
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 44
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 44
6.2.2 Contrôle de la clé privée par plusieurs personnes 45
6.2.3 Séquestre de la clé privée 45
6.2.4 Copie de secours de la clé privée 45
6.2.5 Archivage de la clé privée 45
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique 45
6.2.7 Stockage des clés privées de l'AC dans un module cryptographique 45

6.2.8 Méthode d'activation de la clé privée 45
6.2.9 Méthode de désactivation de la clé privée 46
6.2.10 Méthode de destruction des clés privées 46
6.2.11 Niveau de qualification du module cryptographique et des dispositifs 46
6.3 Autres aspects de la gestion des bi clés 46
6.3.1 Archivage des clés publiques 46
6.3.2 Durée de vie des bi-clés et des certificats 46
6.4 Données d'activation 47
6.4.1 Génération et installation des données d'activation 47
6.4.2 Protection des données d'activation 47
6.4.3 Autres aspects liés aux données d'activation 47
6.5 Mesures de sécurité des systèmes informatiques 47
6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques 48
6.5.2 Niveau de qualification des systèmes informatiques 48
6.6 Mesures de sécurité liées au développement des systèmes 48
6.6.1 Mesures liées à la gestion de la sécurité 49
6.6.2 Niveau d'évaluation sécurité du cycle de vie des systèmes 49
6.7 Mesures de sécurité réseau 49
6.8 Horodatage/Système de datation 49
7 PROFILS DES CERTIFICATS,OCSP ET DES LCR 50
7.1 Profil de Certificats 50
7.1.1 Certificat d'AC 50
7.1.2 Certificats des cachets 51
7.2 Profil des listes de certificats révoqués 52
7.2.1 Champs de base des CRL 52
7.2.2 Extensions des CRL 52
7.3 Profil OCSP 53
7.3.1 Champs de base du certificat de signature des réponses OCSP 53
7.3.2 Extensions du certificat de signature des réponses OCSP 53
8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 54
8.1 Fréquences et / ou circonstances des évaluations 54

8.2 Des contrôles internes peuvent également être déclenchés sur décision de l'AC, sur des périmètres donnés. Identités / qualification des évaluateurs 54
8.3 Relations entre évaluateurs et entités évaluées 54
8.4 Sujets couverts par les évaluations 54
8.5 Actions prises suite aux conclusions des évaluations 54
8.6 Communication des résultats 55
9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES 56
9.1 Tarifs 56
9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats 56
9.1.2 Tarifs pour accéder aux certificats 56
9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats 56
9.1.4 Tarifs pour d'autres services 56
9.1.5 Politique de remboursement 56
9.2 Responsabilité financière 56
9.2.1 Couverture par les assurances 56
9.2.2 Autres ressources 56
9.2.3 Couverture et garantie concernant les entités utilisatrices 56
9.3 Confidentialité des données professionnelles 57
9.3.1 Périmètre des informations confidentielles 57
9.3.2 Informations hors du périmètre des informations confidentielles 57
9.3.3 Responsabilités en termes de protection des informations confidentielles 57
9.4 Protection des données personnelles 57
9.4.1 Politique de protection des données personnelles 57
9.4.2 Informations à caractère personnel 57
9.4.3 Informations à caractère non personnel 58
9.4.4 Responsabilité en termes de protection des données personnelles 58
9.4.5 Notification et consentement d'utilisation des données personnelles 58
9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 58
9.4.7 Autres circonstances de divulgation d'informations personnelles 58
9.5 Droits relatifs à la propriété intellectuelle et industrielle 58
9.6 Interprétations contractuelles et garanties 59

9.6.1 Autorités de Certification 59
9.6.2 Service d'enregistrement 60
9.6.3 RCC 60
9.6.4 Utilisateurs de certificats 61
9.6.5 Autres participants 61
9.7 Limite de garantie 61
9.8 Limites de responsabilité 61
9.9 Indemnités 61
9.10 Durée et fin anticipée de validité de la PC/DPC 62
9.10.1 Durée de validité 62
9.10.2 Fin anticipée de validité 62
9.10.3 Effets de la fin de validité et clauses restant applicables 62
9.11 Amendements à la PC/DPC 62
9.11.1 Procédures d'amendements 62
9.11.2 Mécanisme et période d'information sur les amendements 62
9.11.3 Circonstances selon lesquelles un OID doit être changé 62
9.12 Dispositions concernant la résolution de conflits 62
9.13 Juridictions compétentes 63
9.14 Conformité aux législations et réglementations 63
9.15 Dispositions diverses 63
9.15.1 Accord global 63
9.15.2 Transfert d'activités 63
9.15.3 Conséquences d'une clause non valide 63
9.15.4 Application et renonciation 63
9.15.5 Force majeure 63
9.16 Autres dispositions 63
10 RÉFÉRENCES 64

1 INTRODUCTION

1.1 Présentation générale

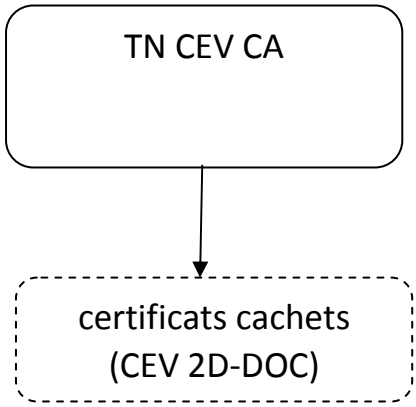
L'ANCE, l'Agence Nationale de Certification Electronique, est dépositaire en Tunisie de la confiance électronique. L'ANCE est notamment en charge de la création et de l'opération de l'Autorité Racine de Certification Nationale tunisienne.

L'ANCE propose un dispositif de sécurisation de documents par code à barre CEV 2D-DOC comme moyen de confiance permettant d'assurer l'authenticité de certains types de documents ainsi que l'intégrité et la conformité des copies faites par rapport à leur version d'origine.

Dans cette optique, l'ANCE offre des certificats cachets conformes aux exigences techniques du standard 2D-DOC v 3.0.0.

La présente PC/DPC définit les engagements de l'ANCE pour son offre de certificats de cachet de l'Autorité de Certification " TN CEV CA" (désignée par le terme AC dans le reste du document).

L'AC est une autorité de certification racine auto-signée qui délivre directement les certificats cachets.



1.2 Identification du document

Le présent document PC/DPC appelé Politique de certification et déclaration des pratiques de certification de l'autorité " TN CEV CA " est la propriété de l'ANCE.

Il est identifié de façon unique par l'identifiant OID suivant : 2.16.788.1.2.6.1.12.

1.3 Définitions et acronymes

1.3.1 Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AEC	Autorité d'Enregistrement Centrale
AED	Autorité d'Enregistrement Déléguée

AH	Autorité d'Horodatage
ANCE	Agence Nationale de Certification Electronique
CEV	Cachet électronique visible
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
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'Autorités Révoquées
LCR	Liste des Certificats Révoqués
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	*Online Certificate Status 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
RCC	Responsable Certificat de Cachet
RFC	Request For Comments
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SP	Service de Publication
SSL	Secure Socket Layer
SSCD	Signature Secure Creation Device
TLS	Transport Layer Security
UC	Utilisateur de Certificats
URL	Uniform Resource Locator

UTC	Universal Time Coordinated

1.3.2 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 ainsi que les standards dans le domaine, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.

Applicatif de vérification de cachet : Il s'agit de l'application mise en œuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices : Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du Porteur du certificat ou des besoins d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorité de certification (AC) : Entité responsable de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur 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 RCC. 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.

Autorité d'Enregistrement Centrale (AEC) :l'autorité d'enregistrement centrale est assurée par l'ANCE. Elle est chargée des services d'enregistrement et de la délivrance des certificats aux RCC.

Autorité d'Enregistrement Déléguée (AED) : l'autorité d'enregistrement déléguée est une entité tierce externe à l'IGC avec laquelle l'ANCE a conclu un contrat de délégation par lequel elle sous-traite une partie de l'activité de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des demandeurs de certificat cachet et la soumission des demandes de révocation ;.

Bi-clé : Une bi-clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Cachet électronique visible "2D-Doc": est un dispositif sécurisé et codé, non interprétable directement par un être humain, qui, lorsqu'il est apposé sur un document, permet de garantir l'authenticité, l'intégrité et la non-répudiation des données figurant également sur le même support physique et/ou numérique. Le CEV 2D-Doc se présente sous la forme d'un code bidimensionnel, contenant les données retenues du document, qui sont signées électroniquement par son émetteur avec sa clé privée. Cette signature authentifie l'émetteur et garanti l'intégrité des données signées lors de sa vérification.

Certificat : Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien

entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC/DPC, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCC et portant sur une bi-clé de cachet de données, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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.

CSR (*Certificate Signing Request*) : message au format PKCS#10 qui permet d'adresser à l'Autorité de Certification une requête signée de création de certificat et signature de ce certificat, contenant une clé publique préalablement générée.

Déclaration des pratiques de certification (DPC) : Une DPC identifie 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.

Dispositif de protection des clés privées : Il s'agit du dispositif matériel et/ou logiciel utilisé pour stocker et mettre en œuvre la clé privée. On parle aussi dans cette PC/DPC de « dispositif de création de cachet ».

Dossier d'enregistrement : ensemble des justificatifs nécessaires à la validation de la demande. Ils sont définis au paragraphe 4.1.2.

Entité : Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privée de type associations. Chaque certificat cachet se rapporte à une entité.

Fonction de génération des clés et des certificats : Cette fonction génère les clés dans les différents supports cryptographiques autorisés par l'IGC, et les certificats (création du format, signature électronique avec la clé privée de l'AC) à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur.

Fonction de gestion des révocations : Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction de publication : voir paragraphe 2.

Fonction d'information sur l'état des certificats : Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, valides, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

HSM (*Hardware Security Module*) : Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des Autorités de Certification.

Infrastructure de gestion de clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une

autorité d'enregistrement centralisée et/ou locale, d'une entité d'archivage, d'une entité de publication, etc.

Key Ceremony (KC) : Cérémonie de clés au cours de laquelle des opérations sensibles sont réalisées : initialisation de modules cryptographiques, génération de bi-clés, restauration de bi-clés sur des nouveaux modules cryptographiques etc. Une Key Ceremony a lieu dans un environnement sécurisé, en présence de témoins, et se déroule selon un Procès Verbal pré-établi.

Liste de Certificats Révoqués (LCR) : Liste contenant les identifiants des certificats révoqués ou invalides.

Mandataire : Personne, physique ou morale ayant directement, par la loi, par délégation ou par procuration du client, le pouvoir d'accomplir tout acte nécessaire à la demande d'émission et à la conclusion et à l'exécution du contrat ainsi que des obligations relatives à la gestion de tout certificat portant le nom du client, qui aura été émis à la demande et sous la responsabilité de ladite personne physique ou morale à défaut de désignation expresse, le mandataire est un représentant légal du client. Le mandataire est responsable des agissements des porteurs.

Motif de révocation : Circonstance pouvant être à l'origine de la révocation d'un certificat. Les motifs de révocation sont détaillés au paragraphe 4.9.1.

OID : Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Personne autorisée : Il s'agit d'une personne autre que le Porteur et le mandataire de certification et qui est autorisée par la Politique de Certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur ou d'un responsable des ressources humaines.

Politique de certification (PC) : Ensemble de règles, identifié par un nom (OID), définissant 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. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les RCC et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE) : Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Public Key Infrastructure (PKI) : **Infrastructure de Gestion de Clés (IGC)** : infrastructure technique permettant de mettre en œuvre toutes les fonctions de l'Autorité de Certification et de l'Autorité d'Enregistrement.

Renouvellement d'un certificat : Correspond à une nouvelle demande de certificat. Opération effectuée à la demande d'un RCC ou un mandataire en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat sur la base d'une nouvelle bi-clé.

Responsable du Certificat de Cachet (RCC) : Cf. paragraphe 1.4.3.

Révocation d'un certificat - Opération dont le résultat est la suppression de la garantie de l'AC sur un certificat donné, avant la fin de sa période de validité. Un certificat est révoqué quand l'association entre ce certificat, la clé publique et le porteur qu'il certifie n'est plus considérée comme valide.
Serveur : Il s'agit d'un service applicatif disposant d'un certificat fourni par l'AC, rattachés à l'entité (identifiée dans le certificat). Ce service est hébergé sur un ou plusieurs serveurs physiques rattachés à un même nom de domaine (FQDN).
Système d'information : Tout ensemble de moyen destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.
Utilisateur de certificat : voir paragraphe 1.4.4.
Validation de certificat : Opération de contrôle du statut (révoqué ou non) d'un certificat.
Validation de signature : Opération de contrôle d'une signature numérique

1.4 Entités intervenant dans l'IGC

1.4.1 Autorité de Certification

L'ANCE joue le rôle **d'Autorité de Certification** pour le **profil de certificats cachets** objet de la présente PC/DPC.
L'Autorité de Certification (AC) garantit le niveau de confiance dans les certificats émis.

Elle définit et assure la **mise en œuvre des fonctions** suivantes :

- **Génération des clés de l'AC, des certificats de l'AC, des certificats de cachet et des éléments secrets de l'IGC** : cette fonction est décrite au paragraphe 6.
- **Remise au Responsable de Certificat** : cette fonction consiste à remettre le certificat au Responsable de Certificat (voir 1.4.3). Cette fonction est décrite au paragraphe 4.3.
- **Autorité d'Enregistrement et gestion du cycle de vie des certificats** (enregistrement, révocation, renouvellement) : cette fonction est décrite aux paragraphes 3 et 4.
- **Publication des informations réglementaires de l'AC** : cette fonction est décrite au paragraphe 2.2.
- **Publication des informations sur le statut (ou l'état) des certificats** : cette fonction est décrite au paragraphe 4.10.
- **Gestion des demandes de révocation** : cette fonction est décrite au paragraphe 4.9.

L'Autorité de Certification remplit les exigences suivantes :

- Être en **relation par voie contractuelle / hiérarchique / réglementaire avec l'entité** pour laquelle elle a **en charge** la gestion **des certificats** de cette entité.
- **Rendre accessible l'ensemble des prestations déclarées dans sa PC/DPC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RCC, aux utilisateurs de certificats**, ceux qui mettent en œuvre ses certificats.
- **S'assurer que les exigences et les procédures de la PC/DPC sont appliquées par** chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.

- **Mettre en œuvre les différentes fonctions identifiées dans sa PC/DPC**, notamment en matière de génération des certificats, de remise au RCC, de gestion des révocations et d'information sur l'état des certificats.
- **Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles**, concernant ses installations, ses systèmes et ses biens informationnels.
- **Mener une analyse de risques 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. L'AC élabore sa PC/DPC en fonction de cette analyse.
- **Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC/DPC** notamment en termes de fiabilité, de qualité et de sécurité.
- **Générer,** et renouveler lorsque nécessaire**, ses bi-clés et les certificats correspondants** (signature de certificats, de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux RCC et utilisateurs de certificats.
- **Suivre les demandes en capacité** et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.4.2 Autorité d'Enregistrement

L'autorité d'enregistrement (AE) est constituée de :

- l'autorité d'enregistrement Centrale « AEC » ;
- des autorités d'enregistrement déléguées « AED » au niveau des guichets des partenaires.

L'Autorité d'Enregistrement assure **deux missions principales** :

- La **validation de l'identité et de la qualité des Responsables de Certificat de Cachet** (RCC) lors de l'enregistrement des certificats.
- La **gestion opérationnelle du cycle de vie des certificats** :
    - Etablissement de la demande de certificat et transmission à l'AC pour traitement (voir paragraphes 4.1 à 4.4).
    - Traitement des demandes de renouvellement (voir paragraphe 4.7).
    - Traitement des demandes de révocation (voir paragraphe 4.9).

De plus, l'Autorité d'Enregistrement assure les fonctions complémentaires suivantes :

- Archivage des pièces du dossier d'enregistrement.
- Conservation et protection des données des personnes concernées par les fonctions de l'IGC (notamment RCC).

1.4.2.1 Autorité d'enregistrement centrale (AEC)

L'ANCE assure le rôle d'AEC qui est chargée de :

- l'enregistrement pour les demandes de certificats ;
- la révocation des certificats ;
- la délivrance des certificats CEV aux RCC se déplaçant au guichet de l'ANCE.

1.4.2.2 Autorité d'enregistrement déléguée (AED)

Les guichets des partenaires ayant signé une convention avec l'ANCE assurent le rôle d'AED.

Les AED sont chargées de :

- Le recueil des demandes de certificats et leur transmission en format électronique à l'AEC ;
- La délivrance des certificats aux RCC ayant effectué leur demande via l'AED.
- Le traitement des demandes de révocation.

1.4.3 Responsables de certificats de cachets

Chaque certificat de cachet est confié à un Responsable de Certificat de Cachet (RCC).

- Le RCC a un lien hiérarchique ou contractuel avec l'entité organisationnelle identifiée dans le certificat.
- La qualité du RCC est validée par l'Autorité d'Enregistrement lors de la demande initiale (voir paragraphe 3.2.3.1).
- Le RCC garantit le lien entre le certificat et l'organisme qui émet des cachets CEV 2D-Doc.
- Le RCC est responsable du renouvellement du certificat (voir paragraphe 4.7).
- Il fait partie des personnes autorisées à demander une révocation du certificat (voir paragraphe 4.9.2).

La présente PC/DPC autorise le **changement de RCC**, notamment pour gérer le cas du départ d'un RCC : voir le paragraphe 3.2.3.2.

1.4.4 Utilisateurs de certificats

Les utilisateurs de certificats sont décrits dans le standard 2D-DOC V3.0.0. Ils sont de deux types :

- Les **émetteurs du CEV 2D-DOC** : ils utilisent la clé privée associée au certificat cachet pour signer les données contenues dans le CEV 2D-DOC.
- Les **utilisateurs du CEV 2D-DOC** : ils utilisent le certificat cachet lors de la validation de l'authenticité d'un document protégé par un CEV 2D-DOC. Le certificat sert à valider la signature incluse dans le CEV 2D-DOC.

Les émetteurs du CEV 2D-DOC qui se conforment au standard 2D-DOC V3.0.0 doivent être référencés par l'ANCE. D'après ce standard, un émetteur référencé correspond à un **participant** (personne morale signant les CEV 2D-DOC) référencé qui s'appuie sur la solution d'un éditeur (fournisseur de la solution technique) référencé.

Un RCC est lié hiérarchiquement ou contractuellement à l'organisation d'un participant référencé par l'ANCE. Ce lien est validé par l'AE lors de l'enregistrement, en plus de la vérification du référencement du participant (voir paragraphe 3.2.3.1).

Les utilisateurs du CEV 2D-DOC ne sont pas contrôlés: la validation d'un CEV 2D-DOC est libre.

Remarque : un **client** de l'ANCE pour la solution CEV 2D-DOC peut être soit un émetteur soit un utilisateur du CEV 2D-DOC. **Dans le cas où il s'agit d'un émetteur du CEV 2D-DOC, il devra désigner au moins un RCC afin d'obtenir un certificat de cachet, et de gérer le cycle de vie du certificat.**

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.1.1.1. Bi-clés et certificats des porteurs

La clé privée associée au CEV 2D-Doc sert exclusivement à **signer les données contenues dans les CEV 2D-DOC,** conformément au standard 2D-DOC v3.0.0.

1.1.1.2. Bi-clés et certificats d'AC et de composantes

La clé privée de l'Autorité de Certification "TN01" est utilisée exclusivement dans les cas suivants :

- Signature des certificats cachet.
- Signature des Listes de Certificats Révoqués (LCR ou CRL).
- Signature du certificat OCSP

D'autres certificats sont utilisés dans le cadre de l'IGC :

- Authentification mutuelle entre les différents composants logiciels de l'IGC.
- Authentification des administrateurs ANCE lors de l'accès aux serveurs de l'IGC.
- Authentification du personnel de l'Autorité d'Enregistrement lors de l'accès aux fonctions de l'Autorité d'Enregistrement.

Ces certificats sont émis par une **IGC distincte, propre à l'ANCE**. Le niveau de sécurité de cette IGC est cohérent avec le niveau de sécurité requis pour l'AC TN01.

1.5.2 Domaines d'utilisation interdits

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.

1.6 Gestion de la PC/DPC

1.6.1 Entité gérant la PC/DPC

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

1.6.2 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

1.6.3 Procédures d'approbation de la conformité de la 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.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

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/pub/PC-DPC-CEV-CA.pdf);
- Le certificat de l'AC (http://www.certification.tn/pub/TN01.crt);
- La Liste de Autorités Révoquées (LAR) valide et à jour (http://crl.certification.tn/cevca.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 TN01 de l'ANCE sont disponibles en permanence selon un taux de disponibilité 24h/24 7j/7 et mises à jour selon les besoins.

La fonction de **publication des certificats d'AC** est disponible **24 heures / 24 et 7 jours / 7**. Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats d'entité finale et/ou de LCR correspondantes.

Une nouvelle LCR est publiée toutes les 24 heures 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 le paragraphe 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

Dans chaque certificat X.509, l'AC (*Issuer*) et le porteur de certificat (*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.

Les certificats de l'AC et des cachets sont identifiés par un DN de type X.500.

3.1.1 Types de noms

Les noms utilisés sont conformes à la norme X.500.
Les certificats de l'AC et des cachets sont identifiés par un DN de type X.500.
Le DN du certificat de l'AC comporte les informations suivantes :

- Country = TN
- Organization = National Digital Certification Agency
- Organization Unit = TN CEV CA
- Common Name = TN01

Le DN du certificat des cachets est construit selon le modèle suivant :

- Country =TN
- Organization = [nom de l'organisation du client]
- Organization Unit = 0002 [matricule fiscal l'organisation du client]
- Common Name = [nom du certificat tel que décrit au paragraphe 3.1.2]

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services de création de cachet respectent la **nomenclature définie par l'ANCE dans le standard 2D-DOC V3.0.0.**

Le standard 2D-DOC V3.0.0 impose que les noms soient codés sur 4 caractères alphanumériques majuscules. De plus :
Le nom de l'AC est choisi par l'ANCE. Il s'agit de « TN01 » dans le cas de la présente PC/DPC.

Le nom des certificats cachets émis par l'AC TN01 est attribué par l'AE selon la règle suivante :

- Sur les trois premiers caractères : désignation du client.
- Sur le quatrième caractère : numéro du certificat de cachet (dans l'ordre de création des certificats cachets, pour le client). Le numéro va de 0 à 9, puis de A à Z.

3.1.3 Anonymisation ou pseudonymisation de serveurs

Les pseudonymes et les certificats anonymes ne sont pas autorisés par la présente PC/DPC.

3.1.4 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire sur le nom des certificats.

3.1.5 Unicité des noms

L'ANCE est garante de **l'unicité des noms des AC** qu'elle référence conformément au standard 2D-DOC V3.0.0.
L'AC TN01 se porte garante de **l'unicité des noms des CEV 2D-DOC**.
Cette unicité repose sur le **DN du certificat**, et plus précisément sur le **champ CN** à l'intérieur du DN.
Le CN est un identifiant unique du certificat au sein de l'AC.
La détection des éventuels cas d'homonymie est réalisée par l'Autorité d'Enregistrement lors de l'enregistrement initial des demandes de certificats.

3.1.6 Identification, authentification et rôle des marques déposées

L'AC décide du nom inscrit dans les certificats sur la base des règles présentées au paragraphe 3.1.2 lors de l'enregistrement de la demande.
Toute demande de changement de nom de certificat se gère via une révocation de certificat suivie d'une nouvelle demande.

3.2 Validation initiale de l'identité

L'enregistrement d'une demande de certificat de cachet requiert l'enregistrement du RCC qui lui est associé.
L'AC TN01 impose la réalisation d'un certain nombre de contrôles sur l'identité et la qualité du RCC.
Ces contrôles ont lieu :

- Soit lors de l'enregistrement de la demande de certificat.
- Soit lors de l'arrivée d'un nouveau RCC en cours de validité d'un certificat.

Ces deux cas de figure sont précisés respectivement aux paragraphes 3.2.3.1 et 3.2.3.2.

3.2.1 Méthode pour prouver la possession de la clé privée

Si la bi-clé est générée par le RCC qui aura la charge du certificat, l'AC exige que la bi-clé soit générée dans un dispositif de sécurité matériel homologué par l'ANCE et certifié au minimum au FIPS 140-2 Level 3 ou plus ou bien CC EAL 4 ou plus.
Le RCC doit fournir une demande de certificat au format PKCS#10 à l'AC.

L'AC TN01 vérifie la validité de la demande de certificat en provenance du RCC en vérifiant au moins les points suivants:

- La requête de certificat est issu d'un module cryptographique certifié
- Les champs inclus au niveau de la requête sont conformes aux champs définies dans la demande.

3.2.2 Validation de l'identité d'un organisme

3.2.2.1 Enregistrement d'un RCC pour un certificat cachet à émettre

La phase d'enregistrement de la demande de certificat, décrite au paragraphe 4.1, comporte une **phase de validation de l'identité et de la qualité du RCC, réalisée par l'AE.**
Dans le cadre de la **demande initiale,** un **face-à-face** doit être réalisé entre l'AE et le RCC. Cette identification est décrite au niveau du paragraphe 6.1.1.3.
Les vérifications effectuées par l'AE sont les suivantes :

- **Vérification de la qualité du RCC** sur la base d'un formulaire de nomination signé par le représentant légal de l'organisation qu'il représente, signé par le RCC, et daté de moins de 3 mois.
- **Vérification de l'identité du RCC** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE de l'ANCE vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du RCC.
- **Vérification de l'acceptation des CGU par le RCC.** Le nouveau RCC doit lire et accepter les CGU pour le certificat dont il devient RCC. L'AE enregistre une trace de cette acceptation.
- **Vérification de l'organisation d'appartenance du RCC** et de son représentant légal :
  - Un extrait du registre de commerce ne dépassant pas trois mois.
  - **l'organisation est référencée par l'ANCE au titre de « participant » ou** figure sur une **liste d'émetteurs de confiance produite par l'ANCE**.
- **Vérification de la qualité du représentant légal** à l'aide de l'extrait du registre de commerce fourni.
- **Vérification de l'identité du représentant légal** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE de l'ANCE vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du représentant légal.

La totalité du processus d'enregistrement et le contenu du dossier d'enregistrement sont présentés aux paragraphes 4.1 à 4.4.

3.2.2.2 Enregistrement d'un nouveau RCC pour un certificat cachet déjà émis

Un certificat cachet doit toujours être placé sous la responsabilité d'un RCC disposant d'un lien hiérarchique ou contractuel valide avec l'organisation mentionnée dans le DN du certificat.
Le RCC a l'obligation de signaler la fin de ses fonctions de RCC à l'AE. Si aucun nouveau RCC n'est désigné pour ce certificat, l'AE se réserve le **droit de révoquer** ce certificat (voir paragraphe 4.9.1).
Sinon, l'AE procède à la **validation de l'identité et de la qualité du nouveau RCC** qui doit être **nommé par le représentant légal** de son organisation d'appartenance. Les **pièces justificatives suivantes** sont demandées pour effectuer les vérifications suivantes :

- **Vérification de la qualité du RCC** sur la base d'un formulaire de nomination signé par le représentant légal de l'organisation qu'il représente, signé par le RCC, et daté de moins de 3 mois.
- **Vérification de l'identité du RCC** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE de l'ANCE vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du RCC.
- **Vérification de l'acceptation des CGU par le RCC.** Le nouveau RCC doit lire et accepter les CGU pour le certificat dont il devient RCC. L'AE enregistre une trace de cette acceptation.
- **Vérification de la qualité du représentant légal** à l'aide d'une attestation du représentant légal (nécessaire si le représentant légal n'est pas celui indiqué dans les statuts publics de l'organisation).
- **Vérification de l'identité du représentant légal** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE de ANCE vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du représentant légal.

3.2.3 Informations non vérifiées du RCC et/ou du serveur informatique

Sans objet.

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

Le renouvellement de la bi-clé d'un porteur entraîne la génération et la fourniture d'un nouveau certificat. La procédure est identique à la procédure de génération de certificat. Dans tous les cas, les informations d'enregistrement sont de nouveau vérifiées. En cas de détection de modification, les justificatifs nécessaires sont à fournir. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante Voir paragraphes 4.6 et 4.7.

3.3.1 Identification et validation pour un renouvellement courant

L'AE procède à la vérification de l'identité et de la qualité du RCC comme indiqué au paragraphe 3.2.3.1 (**enregistrement initial**).

3.3.2 Identification et validation pour un renouvellement après révocation

Une **révocation** de certificat peut être suivie d'une **nouvelle demande** de certificat.
Dans ce cas, l'AE procède à la vérification de l'identité et de la qualité du RCC comme indiqué au paragraphe 3.2.3.1 (**enregistrement initial**).

3.4 Identification et validation d'une demande de révocation

La demande de révocation peut être effectuée :

- A travers la présence physique du RCC ou du représentant légal au niveau du guichet de l'AE moyennant un formulaire de demande de révocation dûment signé. L'identité du RCC ou du représentant légal doit être vérifiée par l'AE.

  Le formulaire contient une information communiquée sous pli intitulée le challenge. Celui-ci doit être communiqué dans la demande de révocation.

- A travers une demande de révocation interne par l'une des composantes de l'IGC conformément aux dispositions décrites dans le paragraphe 4.9.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Un certificat peut être demandé par le **représentant légal de l'organisation**.

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

Le demandeur aura à satisfaire les **pré-requis** suivants **:**

- **Générer une bi-clé dans le dispositif de création de cachet** (voir paragraphe 6.1.1.3) et **conformément aux types et tailles de clés attendus pour la présente PC/DPC** (voir paragraphe 6.1.5).
- **Préparer les justificatifs** nécessaires pour la constitution du dossier d'enregistrement.

La **demande de certificat** doit au moins mentionner :

- Les nom, prénom, adresse email du RCC.
- Le nom de la personne morale (organisation) qui sera identifiée dans le DN du certificat et dans les signatures réalisées avec le certificat.
- Le matricule fiscal de cette personne morale.
- Les nom, prénom, adresse email du représentant légal.

Remarque : c'est l'AE qui détermine le champ Common Name du certificat sur la base des informations d'organisation fournies.

Le demandeur doit **lire les CGU et les accepter**.
Le demandeur doit ensuite fournir les justificatifs propres à la demande (et qui constituent, avec les CGU, le dossier d'enregistrement) :

- **Justificatif d'identité du RCC** (carte d'identité, passeport ou titre de séjour)
- **Formulaire de nomination du RCC** signé par le RCC et son représentant légal, daté de moins de 3 mois. Un modèle de formulaire de nomination peut être téléchargé au niveau du site de publication (voir paragraphe 2).
- **Justificatif d'existence de l'organisation du client** (extrait du registre de commerce).
- **Justificatif d'identité du représentant légal** (carte d'identité, passeport ou titre de séjour)
- **Attestation de représentant légal**, si le représentant légal n'est pas connu à travers les statuts publics de l'organisation (extrait du registre de commerce).

Le demandeur doit présenter une **demande de certificat au format PKCS#10 (*Certificate Signing Request*, CSR) signée à l'aide de la clé privée générée par le RCC dans le dispositif de création de cachet** (voir paragraphe 6.1.1.3).
Le dossier de demande est établi et signé par le représentant légal de l'organisation.

4.2 Traitement d'une demande de certificat

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

L'AE procède au **traitement de la demande d'enregistrement** de certificat :

- L'AE vérifie la **cohérence des justificatifs** présentés dans le dossier d'enregistrement avec les informations d'identité et d'organisation renseignées par le demandeur.
- L'AE **valide l'identité et l'autorité du demandeur** conformément au paragraphe 3.2.3.1.
- L'AE **valide l'existence de l'organisation du client et son appartenance au dispositif CEV 2D-DOC.**
- L'AE **valide la nomination du RCC**.
- L'AE vérifie les éventuels **cas d'homonymie**, et statue sur le nom du certificat porté d'une part dans le champ Common Name dans le DN du certificat, et d'autre part dans le champ Subject Alt Name conformément aux règles de l'AC (voir paragraphe 3.1).
- Si la demande de certificat est acceptée, l'opérateur d'enregistrement valide la demande. Cela déclenche l'envoi de la CSR auprès des composantes de l'AC chargée de la production des certificats.

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 du 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 du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Afin de traiter la demande de certificat, l'AC effectue les actions suivantes :

- Vérification de la **conformité du type et de la taille de clés** par rapport au profil du certificat demandé.

- **Génération d'un certificat et signature** par l'AC.
- **Ajout du certificat dans l'annuaire de certificats** publié par l'AC.

4.3.2 Notification par l'AC de la délivrance du certificat au RCC

La remise du certificat au RCC s'effectue par l'AE par courrier électronique ou bien au niveau du guichet de l'AEC ou l'une des AED.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Dès que le certificat est reçu par le RCC, l'AC "TN01" considère le certificat comme accepté. L'acceptation est tacite. En cas de contestation dans un délai de sept (07) jours ouvrables, le RCC alerte l'AE et demande la révocation de son certificat.

4.4.2 Publication du certificat

Le certificat de l'AC TN01 et les certificats cachets délivrés par l'AC TN01 sont publiés par le SP.

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

Le demandeur est informé de la délivrance d'un certificat cachet pour les codes CEV 2D-DOC dont il est responsable. Le service de l'AEC est également informé de la délivrance du certificat.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le RCC

Les RCC sont responsables de l'usage du certificat cachet qui leur est remis par l'AC, conformément aux exigences du paragraphe 1.5.
L'extension Key Usage du certificat permet de vérifier les usages autorisés du certificat.
Dans le cadre de la présente PC/DPC, les certificats de cachet contiennent dans l'extension Key Usage marquée comme critique les valeurs « Digital signature » et « Non-repudiation ».

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificat doivent respecter les usages autorisés, décrits au paragraphe 1.5.

4.6 Renouvellement d'un certificat

La notion de renouvellement telle que définie dans la RFC 3647 n'est pas autorisée dans le cadre de cette PC/DPC.
Remarque : l'IGC de ANCE vérifie qu'un nouveau certificat ne peut pas être établi pour une même bi-clé.

Le service de renouvellement est complété par une notification automatique des clients de l'expiration prochaine de leur certificat deux (2) fois par mail, les deux dernières semaines avant la fin d'utilisation (1 an) des bi-clé.

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

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 du certificat expiré.

Tout besoin d'un nouveau certificat pour un même service applicatif de création de cachet est traité par la création d'un nouveau certificat, identifié par un nouveau Common Name, selon la règle de nommage indiquée au paragraphe 3.1.

Le processus de demande d'un nouveau certificat est donc celui décrit dans les paragraphes 4.1 à 4.4.

Le service de renouvellement est complété par une notification automatique des clients de l'expiration prochaine de leur certificat deux (2) fois par mail, les deux dernières semaines avant la fin d'utilisation (1 an) des bi-clé.

4.7.1 Causes possibles de changement de bi-clé

Les causes possibles d'un changement de bi-clé sont les suivantes :

- Expiration du certificat.
- Fin de la période d'utilisation de la clé privée.
- Révocation du certificat.

Les bi-clés des certificats de cachet ont une durée de validité de 3 ans.
La présente PC/DPC définit une période d'utilisation des clés privées de 1 an.
Au-delà de la période d'utilisation des clés privées, une nouvelle bi-clé doit être créée et un nouveau certificat doit être demandé. Une fois le nouveau certificat émis, la précédente clé privée doit être supprimée. Le certificat reste valide jusqu'à sa date d'expiration (il n'est pas révoqué).

4.7.2 Origine d'une demande de nouveau certificat

Identique aux dispositions décrites au niveau du paragraphe 4.1.1.

4.7.3 Procédure de traitement d'une demande de nouveau certificat

Identique aux dispositions décrites au niveau du paragraphe 4.2.

4.7.4 Notification au RCC de l'établissement du nouveau certificat

Identique aux dispositions décrites au niveau du paragraphe 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Identique aux dispositions décrites au niveau du paragraphe 4.4.1.

4.7.6 Publication du nouveau certificat

Identique aux dispositions décrites au niveau du paragraphe 4.4.2.

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

Identique aux dispositions décrites au niveau du paragraphe 4.4.3.

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 de cachet

Les **causes possibles d'une révocation de certificat de cachet** sont les suivantes :

- **Les informations du service applicatif** figurant dans son certificat **ne sont plus en conformité** avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat.
- **Le RCC n'a pas respecté** les **modalités** applicables **d'utilisation** du certificat.
- **Le RCC et/ou** le cas échéant **l'entité** n'ont **pas respecté** leurs **obligations** découlant de la PC/DPC de l'AC.

Remarque : cela concerne le cas où il n'existe plus de RCC explicitement identifié pour le certificat de cachet (voir paragraphe 4.11).

- Une **erreur** (intentionnelle ou non) a été détectée **dans le dossier d'enregistrement**.
- **La clé privée du service applicatif est suspectée de compromission**, est **compromise**, est **perdue** ou est **volée**, (éventuellement les données d'activation associées).
- Le RCC n'a pas respecté ses obligations découlant de cette PC/DPC;
- **Le RCC ou une entité autorisée** (voir paragraphe 4.9.2.1) **demande la révocation du certificat** (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support).
- Le changement de l'information contenue dans le DN du certificat;
- **L'arrêt définitif du service applicatif** ou la **cessation d'activité** de l'organisation identifiée dans le DN du certificat de cachet associé (voir paragraphe 4.11).

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance de l'AC afin qu'elle révoque le certificat dans les meilleurs délais.

4.9.1.2 Certificats d'une composante de l'IGC

Les causes possibles d'une révocation de certificat d'AC ou d'une composante de l'IGC (voir paragraphe 1.5.1.2) sont les suivantes :

- **Suspicion de compromission, compromission, perte ou vol de la clé privée** de la composante.
- 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 la DPC/DPC (par exemple, suite à un audit de qualification ou de conformité négatif).
- Cessation d'activité de l'entité opérant la composante.

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance de l'AC qui révoque immédiatement le certificat.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de cachet

Les **personnes autorisées** à demander la **révocation d'un certificat de cachet** sont les suivantes :

- Le Responsable de l'AC.
- Tout opérateur d'enregistrement.
- Le RCC en charge du certificat.
- Le représentant légal de l'organisation identifiée dans le certificat.

4.9.2.2 Certificats d'une des composantes de l'IGC

Les **personnes autorisées** à demander la **révocation d'un certificat d'AC** sont les suivantes :

- Le Responsable de l'AC.
- Une Autorité judiciaire via une décision de justice.

La révocation des certificats de **composantes de l'IGC** est décidée par le **Responsable de l'AC**.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de cachet

La révocation d'un certificat de cachet se déroule par les canaux suivants :

- Guichet de l'ANCE : un formulaire papier est mis à disposition des clients au guichet de l'ANCE pour la révocation des certificats. Il est également possible de télécharger et d'imprimer le même formulaire disponible sur le site web pour l'envoyer par courrier ou par fax à l'ANCE. Le formulaire de demande de révocation doit être dûment rempli et signé par le demandeur.
- Guichets des partenaires : le même formulaire papier est mis à disposition des clients aux guichets des partenaires pour la révocation des certificats. Le formulaire de demande de révocation doit être dûment rempli et signé par le demandeur.
- Site web : le RCC ou le représentant légal peut effectuer la révocation à partir de son espace personnel sur le site web de l'ANCE.

Toutes les personnes autorisées mentionnées au paragraphe 4.9.2 peuvent faire leur demande via le formulaire de révocation.
Le demandeur de la révocation est authentifié par l'AE selon les règles définies au paragraphe 3.4.
Quel que soit le canal, la demande de révocation doit comporter au minima les informations suivantes :

- Le nom du certificat (contenu du champ Common Name) à révoquer.
- le numéro du dossier permettant de retrouver rapidement le certificat à révoquer ;
- Le challenge communiqué au préalable dans l'enveloppe sous pli. Cette information n'est pas obligatoire dans le cas de présence physique du demandeur aux guichets de l'AE.

Les AED transmettent les demandes à l'AEC. Celle-ci authentifie l'AED et effectue les contrôles adéquats.
L'AEC transmet la demande à l'AC chargée de la production des certificats et des LCR.
L'AC effectue ensuite la révocation et génération de la LCR.
Le SP se charge ensuite de la publication de la LCR contenant l'information de révocation et met à jour le serveur OCSP.
Les causes de révocation ne sont pas publiées ni dans les LCR ni sur le serveur OCSP.
Le demandeur de la révocation est informé de la prise en compte de sa demande et de la révocation effective du certificat.

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

En cas de révocation d'un certificat d'AC, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

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 au RCC pour formuler la demande de révocation

Le RCC formule sa demande de révocation sans délai, dès connaissance d'une cause possible de révocation.

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

4.9.5.1 Révocation d'un certificat de cachet

Le service de révocation est disponible 24 heures sur 24 7 jours sur 7.

Toute demande de révocation d'un certificat porteur 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 d'un certificat de signature de l'AC TN01 (signature de certificats, de LCR et/ou de réponses OCSP) est effectuée immédiatement, en particulier dans le cas de la compromission de la clé.

4.9.6 Exigences de vérification de la 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 méthode utilisée (LCR, OCSP) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

La validité d'une LCR est contrôlée par vérification de sa signature et vérification de la validité du certificat de l'AC TN01.

4.9.7 Fréquence d'établissement des LCR

La fréquence de génération des LCR est de 24 heures.

4.9.8 Délai maximum de publication d'une LCR

La publication d'une LCR suite à sa génération doit être effectuée au maximum dans un délai de 30 minutes.

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

L'ANCE maintient en ligne 24x7 un serveur OCSP permettant la vérification de l'état d'un certificat.

- Le certificat de l'OCSP est issu de l'autorité "TN01",
- Les informations de révocation des certificats sont disponibles sur le serveur OSCP à l'adresse http://va.certification.tn.
- L'autorité "TN01" publie et génère une CRL chaque 24 heures et dans un délai de demi heure suite à la révocation d'un certificat porteur. La durée de validité d'une CRL est de 6 jours.

le certificat de signature du serveur OCSP contient une extension de type id-pkix-ocsp-nocheck tel défini par le RFC 2560.

4.9.10 Exigences sur la vérification en ligne de la révocation et l'état des certificats

Cf. paragraphe 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.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission avérée ou soupçonnée d'une clé privée, la révocation du certificat associé doit être demandée dans les plus brefs délais.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC met les CRL à disposition de tous les utilisateurs via son site de publication.

Les LCR sont publiées sur le site web de l'ANCE accessible à l'adresse http://crl.certification.tn/cevca.crl et sur l'annuaire ldap.certification.tn accessible à travers le protocole LDAP V3.

L'AC publie également sur son site de publication son certificat d'AC et son empreinte, ce qui permet aux utilisateurs de vérifier la validité de la signature des certificats de cachet.

4.10.2 Disponibilité de la fonction

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

4.11 Fin de la relation entre le RCC et l'AC

Dans le cas où la relation contractuelle entre l'AC et la personne morale identifiée dans le DN du certificat de cachet se termine, alors le certificat de cachet doit être révoqué. La clé privée correspondante sera supprimée.

Remarque : afin de faciliter la validation du CEV 2D-DOC, le certificat pourra ne pas être révoqué en cas de fin de relation contractuelle entre l'AC et la personne morale identifiée dans le DN du certificat de cachet. Par contre, la clé privée sera supprimée.
Dans le cas où il n'existe plus de RCC explicitement identifié pour un certificat de cachet, le certificat doit être révoqué.

4.12 Séquestre de clé et recouvrement

Les bi-clés et les certificats cachets émis conformément à la présente PC/DPC ne font pas l'objet de séquestre ni de recouvrement.

5 MESURES DE SECURITE 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 les 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.

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 séquence 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 le paragraphe 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 journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'GC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation d'une demande de certificat ;
- Evènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...) ;
- Génération des certificats ;
- Transmission des certificats;
- Publication et mise à jour des informations liées à l'AC ;

- Génération d'information de statut d'un certificat cachet.

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 semaine. 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 documentation fonctionnelle de l'AC :les différentes versions de la PC/DPC, les CGU;
- les dossiers complets des demandes de création et de révocation de certificats ;
- les certificats et LCR 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

Par défaut, les archives sont conservées pendant 20 ans.

- C'est le cas notamment des dossiers d'enregistrement.
- Les journaux d'événements sont archivés pendant 07 ans à compter de leur génération.

Les certificats et CRL sont archivés pendant 20 ans après leur arrivée à expiration.

Pour l'archivage des journaux autres que les journaux d'évènements traités au paragraphe 5.4.1 , aucune exigence n'est stipulée.

La procédure d'archivage définit le processus de gestion des demandes d'accès aux archives.

5.5.3 Protection des archives

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

5.5.4 Exigences d'horodatage des données

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

5.5.5 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 paragraphe 5.5.3).

5.5.6 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 la clé d'AC

La durée de vie du certificat de l'AC TN CEV "TN01" est de 10 ans.

La durée de vie des certificats de cachet émis par l'AC est de 3 ans.

Afin de permettre aux utilisateurs de vérifier l'origine des certificats de cachet, à tout moment de la vie du certificat, l'AC choisit de ne plus émettre de certificats 3 ans avant sa date de fin de validité.

Une nouvelle AC sera créée afin de maintenir la continuité du service. La nouvelle clé privée de cette AC (et seulement cette nouvelle clé) sera utilisée pour signer les nouveaux certificats de cachet.

L'ancien certificat d'AC servira à valider les certificats émis par la première AC. La publication des CRL correspondant à l'ancienne AC sera maintenue jusqu'à expiration du dernier certificat émis par l'ancienne AC.

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.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC devient insuffisant pour son utilisation prévue restante, alors l'AC TN01 réalise les actions suivantes :

- Informer tous les responsables d'AC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Révoquer tout certificat concerné.

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

Le cas de compromission de la clé privée d'une composante de l'IGC fait partie des sinistres traités par le PRA.

Le cas de compromission d'une clé d'AC amène sa révocation (voir paragraphe 4.9.1.2).
De plus, l'AC informe de la compromission tous les RCC et les entités avec lesquelles elle a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information est mise à disposition des autres tiers utilisateurs.

L'AC indique que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

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 au paragraphe 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 de l'IGC

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 RCC 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 et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), 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 RCC et les utilisateurs de certificats (UC) ;
- continuer à assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC/DPC, le temps que les porteurs 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 porteurs 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 LCR ;
- détruire les clés privées et toutes les copies de sauvegarde des clés privées lui ayant permis d'émettre des certificats ou des LCR.

Plus de détails sont fournies au niveau de la procédure de cessation d'activité ou de changement des composantes de l'AC.

6 MESURES DE SECURITE 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 et CC EAL 4+).

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 (voir paragraphe 5.2.1) en suivant les instructions d'un procès verbal préalablement défini.

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.

6.1.1.2 Clés serveurs générées par l'AC

sans objet.

6.1.1.3 Clés porteurs

le RCC en charge du certificat cachet s'engage, via la signature des conditions générales d'utilisation, à générer la clé privée dans un **dispositif de création de cachet certifié au moins au niveau 3 selon la norme FIPS 140-2 ou bien EAL 4+**.

Le RCC génère une clé cryptographique dont la clé publique est contenue dans une demande de certificat au format PKCS#10 fournie à l'AC "TN01".

D'autre part, le RCC doit créer une bi-clé différente pour chaque type de document à signer.

6.1.2 Transmission de la clé privée au serveur

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La transmission de la clé publique vers l'AC doit permettre :

- La protection de l'intégrité de la clé.
- La vérification de l'origine de la transmission.

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

Le certificat de l'AC "TN01" et l'empreinte de ce certificat sont publiés sur le site web de l'ANCE : http://www.certification.tn/pub/TN01.crt.
Les Conditions Générales d'Utilisation disponibles sont publiées sur le site web de l'ANCE : http://www.certification.tn/pub/CGU-CEV.pdf.

6.1.5 Tailles des clés

Les tailles de clés autorisées dans le cadre de cette PC/DPC sont les suivantes :

- Clés des cachets : La taille des clés pour un certificat cachet est de type P-256 (NIST) en ECDSA/ Algorithme de hachage SHA-256 (256 bits) .
- Clés de l'AC : La taille des clés de l'AC est P-384 (NIST) en ECDSA / Algorithme de hachage SHA-384 (384 bits) .

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

Les équipements de génération des bi-clés utilisent des paramètres respectant les normes de sécurité propres aux algorithmes correspondant aux bi-clés.
Les algorithmes utilisés pour la génération des certificats sont SHA-384 avec ECDSA pour l'AC et SHA-256 avec ECDSA pour les certificats cachets.
Voir le paragraphe 7 pour les profils de certificats.

6.1.7 Objectifs d'usages de la clé

L'utilisation d'une clé privée d'AC est limitée à la signature de certificats et de CRL.
L'utilisation d'une clé privée de cachet est limitée au service CEV 2D-DOC.

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

6.2.1.1 Module cryptographique de l'AC

L'AC dispose de modules cryptographiques certifiés FIPS 140-2 niveau 3 et EAL 4+ 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.

6.2.1.2 Dispositifs de protection des clés privées des serveurs

le dispositif de création de cachet, être un dispositif de sécurité matériel certifié au minimum au niveau 3 selon la norme FIPS 140-2 et EAL 4+.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de signature de l'AC est assuré par des porteurs de parts de secret, comme décrit au paragraphe 6.1.1.1.
Le quorum des parts de secrets nécessaire à la restauration de la clé privée d'AC sur un module cryptographique est fixé par l'AC à 3 sur 8.

Les porteurs de secrets font partie des personnes ayant un rôle de confiance (voir paragraphe 5.2.1).

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

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.

Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC.

6.2.5 Archivage de la clé privée

Les clés privées ne sont pas archivées.

6.2.6 Transfert de la clé privée vers / 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 de la clé privée d'AC dans le module cryptographique est contrôlée par des données d'activation (voir paragraphe 6.4.1.1), et fait intervenir deux porteurs de secret.

6.2.8.2 Clés privées des porteurs

L'activation de la clé privée du porteur est faite dès la génération du certificat de cachet. Elle est contrôlée via les données d'activation.

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 cachets

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, 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 porteurs

En fin de vie d'une clé privée de cachet, le RCC s'engage à détruire la clé privée.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs

Se reporter au paragraphe 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 porteurs 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 Durée de vie des bi-clés et des certificats

Voir le paragraphe 5.6 pour les durées de vie des certificats et pour les modalités de renouvellement du certificat de l'AC.

Pour le service applicatif CEV 2D-DOC, le certificat a une **durée de validité de 3 ans**, mais la **durée d'utilisation de la clé privée est de 1 an**. Une nouvelle bi-clé et un nouveau certificat sont générés 1

an après la première génération des bi-clé et du certificat. Cela permet aux CEV 2D-DOC émis d'être vérifiables simplement pendant une durée d'au moins 2 ans.

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 paragraphe 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 PV de la cérémonie des clés correspondant à la création de la clé privée et du certificat de l'AC TN01 .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 la clé privée du serveur

La clé privée du porteur est générée dans un module cryptographique dont la création et la répartition des données d'activation ont été faites lors de la phase d'initialisation et de personnalisation de celui-ci.

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 correspondant à la clé privée de l'AC 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 porteurs

Les données d'activation des dispositifs de création de cachet des services applicatifs sont conservées de manière à en assurer la disponibilité, l'intégrité, et la confidentialité.

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).

Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre les 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 porteur ;
- début de la révocation d'un certificat porteur ;
- de l'enregistrement des évènements dans les journaux.

7 PROFILS DES CERTIFICATS,OCSP ET DES LCR

Ce chapitre traite des exigences relatives aux profils des certificats X.509 v3 de l'AC "TN01" ou émis par celle-ci, ainsi que des profils des LCR. Les certificats émis selon la présente PC/DPC sont conformes au RFC 5280.

7.1 Profil de Certificats

Les certificats de l'AC "TN01" et des certificats cachet sont des certificats au format X.509 v3. Les champs des certificats de l'AC et des porteurs sont définis par le RFC 5280.

7.1.1 Certificat d'AC

7.1.1.1 Les champs de base

Les informations principales contenues dans le certificat de l'AC "TN01" sont :

Champ de base	Valeur
Version	2 (pour V3)
Numéro de série	= 6a b8 26 4e 06 82 56 97
DN Émetteur	C=TN OU = TN CEV CA O=National Digital Certification Agency CN=TN01
Valide à partir du	YYMMDDHHMMSS = jeudi **27 avril 2017 13:52:57**
Valide jusqu'au	YYMMDDHHMMSS +10 = mardi **27 avril 2027 13:52:57**
DN Objet	C=TN OU = TN CEV CA O=National Digital Certification Agency CN=TN01
Signature du certificat	SHA256ECDSA
Algorithme de clé pulique	ECDSA_P384
Clé publique	< valeur de la clé publique l'AC TN01> =04 e4 f6 ba 90 e0 9d 07 90 2d 94 a8 67 72 b3 fe 59 42 0d 87 2c 83 80 f6 91 c8 d5 93 fc c0 b8 2f 3c a1 00 05 8c 68 83 6d 9d 8b 01 f4 ba c8 ed b6 9e b5 cb 22 fe 6d d5 b6 5e c4 bb 43 15 36 fd b7 d0 28 ad 76 03 21 8b a0 57 c7 27 7a a5 1a 76 0e c9 7e 37 3b 22 15 73 dd 88 11 13 40 95 56 cf 5b 0e

7.1.1.2 Extensions

Champ de base	Critique(O/N)	Valeur
Identificateur de la clé du sujet	N	<Valeur de Hachage> =ce 87 48 48 a9 2f a8 f5 b6 cb f7 97 b5 f7 02 91 d2 8a 9c 58
Identificateur de la clé de l'émetteur	N	<Valeur de Hachage> =ce 87 48 48 a9 2f a8 f5 b6 cb f7 97 b5 f7 02 91 d2 8a 9c 58
Contraintes de base	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)
Utilisation de la clé	O	Signature numérique, Signature du certificat, Signature de la Liste de Révocation des Certificats, Signature de la Liste de Révocation des Certificats hors connexion.

7.1.2 Certificats des cachets

7.1.2.1 Champs de base

Champ de base	Valeur
Version	2 (pour V3)
Numéro de série	<défini lors de la génération du cachet>
DN Émetteur	C=TN OU = TN CEV CA O=National Digital Certification Agency CN=TN01
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS +3
DN Objet	CN=< nom du certificat de cachet > OU= < numéro du matricule fiscal de l'organisation émettant les CEV 2D-DOC > O= < nom de l'organisation émettant les CEV 2D-DOC > C=TN
Signature du certificat	SHA256withECDSA
Clé publique	<ECDSA P-256 (NIST)>

7.1.2.2 Extensions

Champ de base	Critique(O/N)	Valeur
Identificateur de la clé du sujet	N	<Valeur de Hachage>

Champ de base	Critique(O/N)	Valeur
		=
Identificateur de la clé de l'émetteur	N	<Valeur de Hachage> = ce 87 48 48 a9 2f a8 f5 b6 cb f7 97 b5 f7 02 91 d2 8a 9c 58
Stratégies de certificat	N	Identificateur de politique =2.16.788.1.2.6.1.12
Contraintes de base	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucune
Utilisation de la clé	O	Signature numérique, Non-répudiation
Accès aux informations de l'autorité	N	CertPath=http://www.certification.tn/pub/TN01.crt OCSP= http://va.certification.tn
Point de distribution de la CRL	N	Indique l'adresse HTTP où est publiée la LCR : URL=http://crl.certification.tn/cevca.crl

7.2 Profil des listes de certificats révoqués

Ce paragraphe décrit le profil des CRL.

7.2.1 Champs de base des CRL

Champ de base	Valeur
Version	1 (pour V2)
Algorithme de clé publique	sha384WithECDSA
DN Émetteur	C=TN OU = TN CEV CA O=National Digital Certification Agency CN=TN01
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 6 jours
Certificats révoqués	< liste des certificats révoqués identifiés par leur numéro de série, et comportant la date de révocation >

7.2.2 Extensions des CRL

Champ de base	Critique(O/N)	Valeur
Identificateur de la clé de l'autorité	N	<Valeur de Hachage> = ce 87 48 48 a9 2f a8 f5 b6 cb f7 97 b5 f7 02 91 d2 8a 9c 58
Numéro de CRL	N	< numéro incrémental pour les CRL >

7.3 Profil OCSP

Les réponses OCSP délivrées par le répondeur OCSP associé à l'AC sont conformes à la RFC 2560. Ces réponses sont signées par un certificat délivré par cette même AC.

7.3.1 Champs de base du certificat de signature des réponses OCSP

Champ de base	Valeur
Version	2 (pour V3)
Numéro de série	<défini lors de la génération du certificat>
DN Émetteur	C=TN OU = TN CEV CA O=National Digital Certification Agency CN=TN01
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS +3
DN Objet	CN=CEV OCSP O=National Digital Certification Agency C=TN
Signature du certificat	sha384ECDSA
Clé publique	<ECDSA P-384 (NIST)>

7.3.2 Extensions du certificat de signature des réponses OCSP

Champ de base	Critique(O/N)	Valeur
Identificateur de la clé du sujet	N	<Valeur de Hachage> =
Identificateur de la clé de l'émetteur	N	<Valeur de Hachage> = ce 87 48 48 a9 2f a8 f5 b6 cb f7 97 b5 f7 02 91 d2 8a 9c 58
Contraintes de base	O	Type d'objet=Entité finale
Utilisation avancée de la clé	N	Signature OCSP (1.3.6.1.5.5.7.3.9)
Utilisation de la clé	O	Signature numérique, Non-répudiation
Point de distribution de la CRL	N	Indique l'adresse HTTP où est publiée la LCR : URL= http://crl.certification.tn/cevca.crl

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

L'AC "TN01" est 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 ;

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

Avant la première mise en service de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fait procéder à un contrôle de conformité de cette composante.
L'AC procède à un contrôle régulier de conformité de l'ensemble de son IGC une fois par an.

8.2 Des contrôles internes peuvent également être déclenchés sur décision de l'AC, sur des périmètres donnés. Identités / qualification 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 partie 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 les 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 "TN01" 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 LCR 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 aucune exigence sur ce point.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les clés privées de l'AC, des composantes et des serveurs.
- Les données d'activation associées aux clés privées d'AC et des porteurs
- Tous les secrets de l'IGC
- Les journaux d'événements des composantes de l'IGC.
- Les dossiers d'enregistrement des serveurs et des RCC.
- Les causes de révocations.
- Les rapports d'audit
- 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.

En particulier, d'après la loi organique n° 2004-63 du 27 juillet 2004, article 27, le RCC doit consentir au traitement de ses données personnelles avant toute utilisation.

En outre, et selon l'article 12, les données collectées ne peuvent être utilisées par l'ANCE ou un tiers à des fins autres que la vérification initiale d'identité et la génération du certificat, sauf accord explicite du RCC, selon la même loi, chapitre IV.

L'AC doit informer le RCC des procédures qu'il applique en termes de protection des données personnelles (article 31).

Enfin, le RCC se d'un droit d'accès et de modification à ses données personnelles selon l'article 32.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats cachet
- Les données d'enregistrement contenant notamment les données d'identification des RCC.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

Toutes les composantes traitent et protègent toutes les données à caractère personnel de manière à ce que seuls des personnels dans des rôles de confiance y aient accès, selon la présente PC/DPC.

Les RCC disposent d'un droit d'accès et de rectification de leurs données personnelles collectées par l'ANCE pour la création, le renouvellement, le recouvrement et la révocation du certificat.

9.4.5 Notification et consentement d'utilisation des données personnelles

Le consentement exprès et préalable du porteur de certificat concernant l'utilisation de ses données personnelles est requis lors de l'enregistrement de celui-ci. Aucune donnée personnelle ne peut être collectée sans son accord, en vertu de la loi organique n° 2004-63 du 27 juillet 2004, articles 27 et 12.

Le RCC est informé avant tout traitement de ses données personnelles des procédures que l'AC "TN01" applique en matière de protection des données personnelles.

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

L'AC agit conformément à la réglementation tunisienne. L'ANCE dispose de procédures pour permettre l'accès des autorités judiciaires aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Lors d'un transfert d'activité (cf paragraphe 9.15.2), le RCC est sollicité pour donner son accord quant au transfert de ses données personnelles.

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.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC/DPC de l'AC et les documents qui en découlent,
- respecter et appliquer la présente PC/DPC
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. paragraphe 8) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RCC ,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC "TN01" est responsable vis-à-vis de ses clients, bénéficiaires 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 "TN01" s'engage à, durant la durée de validité certificat porteur émis, de manière non exhaustive, les garanties suivantes :

- Existence légale: l'AC "TN01", vérifie et confirme que le sujet figurant dans le certificat, avant sa date de génération, existe légalement;

- Autorisation du certificat : l'AC "TN01" vérifie et confirme que le demandeur a les droits nécessaires de représenter l'organisme demandeur du certificat ;

- Exactitude des informations: l'AC "TN01" a pris toutes les mesures raisonnablement nécessaires pour vérifier que toutes les informations incluses dans le certificat sont exactes avant sa date de génération;

- Aucune information trompeuse : l'AC "TN01" a pris toutes les mesures raisonnablement nécessaires pour réduire la probabilité que les informations contenues dans le certificat soient erronées ceci avec la mise en place des procédures de saisie et de validation des demandes de certificats électroniques;

- Identité du demandeur : L'AC "TN01" a pris toutes les mesures raisonnablement nécessaires pour vérifier l'identité du demandeur du certificat avant sa génération ;

- Accord du demandeur en signant les conditions générales d'utilisations du certificat cachet;

- Statut: l'AC "TN01" garantit de maintenir un répondeur en ligne sur l'état des certificats qu'elle a émis accessible 24/24 7/7 ;

- Révocation: l'AC "TN01" suit les lignes directrices pour la révocation d'un certificat tel décrit dans le paragraphe 4.9.

En plus, l'AC "TN01" a l'obligation de :

- Pouvoir démontrer le lien entre un RCC et son certificat, conformément aux exigences du paragraphe **Erreur ! Source du renvoi introuvable.** ci-dessus ;
- Protéger les clés privées de l'AC 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 Serveurs se conforme à toutes les obligations pertinentes de l'AC définies dans le paragraphe 9.6.1 en se restreignant aux services qu'elle met en œuvre dans le cadre de la présente PC/DPC pour:

- Vérifier la validité des pièces justificatives et l'exactitude des mentions du dossier d'enregistrement qui établissent l'identité et l'organisation d'appartenance du RCC,
- Vérifier l'origine et l'exactitude de toute demande de révocation et mettre en œuvre les moyens permettant de les traiter,
- Respecter les politiques de contrôle d'accès aux composantes techniques de l'Autorité d'enregistrement.

9.6.3 RCC

Le RCC a le devoir de :

- Générer la Bi-Clé du CEV 2D-DOC sur le support physique,
- Communiquer les informations exactes et à jour lors de la demande ou du renouvellement du certificat,
- Protéger la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement,
- Protéger les données d'activation de cette clé privée,
- Protéger l'accès à la base de certificats du serveur,
- Respecter les conditions d'utilisations de la clé privée et du certificat correspondant,
- Informer l'AC de toute modification concernant les informations contenues dans le certificat de cachet,
- Faire, sans délai, une demande de révocation du certificat de cachet dont il est responsable auprès de l'AE, ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante.

La relation entre le RCC et l'AC ou ses composantes est formalisée par un engagement du RCC visant à certifier l'exactitude des renseignements et des documents fournis.

9.6.4 Utilisateurs de certificats

Les utilisateurs utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis,
- Vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat,
- Vérifier et respecter les obligations des utilisateurs de certificats exprimés dans la présente PC/DPC.

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 :

- l'identification et l'authentification des RCC avec les certificats générés par l'AC ;
- 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'un RCC 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 du RCC est engagée en cas d'erreur dans les informations vérifiées des certificats résultant d'une fraude ou de manquement du RCC.

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 Amendements à la PC/DPC

9.11.1Procédures d'amendements

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC. En cas de changement important, l'AC pourra faire appel à une expertise technique pour en contrôler l'impact.

9.11.2 Mécanisme et période d'information sur les amendements

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.11.3 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.

9.12 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 à l'amiable.

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

9.13 Juridictions compétentes

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

9.14 Conformité aux législations et réglementations

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

9.15 Dispositions diverses

9.15.1 Accord global

L'ANCE valide tous les éventuels accords passés avec les partenaires.

9.15.2 Transfert d'activités

Voir le paragraphe 5.8.

9.15.3 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.

9.15.4 Application et renonciation

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

9.15.5 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 porteurs.

9.16 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
[RFC2560]	IETF - X.509 Internet Public Key Infrastructure- Online Certificate Status Protocol - OCSP - Juin 1999 Disponible à l'adresse : https://www.ietf.org/rfc/rfc2560.txt
[RFC5280]	IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - Mai 2008 Disponible à l'adresse : https://www.ietf.org/rfc/rfc5280.txt
[FIPS 140-2]	Federal Information Processing Standards Publication 140-2: Security requirements for cryptographic modules National Institute of Standard and Technology (NIST)
[2D-DOC]	Spécifications techniques des Codes à Barres 2D-Doc (ANTS) Disponible à l'adresse : https://ants.gouv.fr/content/download/516/5665/version/.../ANTS_2D-Doc-v3.0.0.pdf