INTERNATIONAL TELECOM ASSISTANCE

LA DECLARATION DES PRATIQUES DE CERTIFICATION

Version 1.1

Avril 2017

LA DECLARATION DESPRATIQUES DE CERTIFICATION (DPC)

Version 1.1

Avril 2017

Historique du document				
Date	**Version**	**Rédacteur**	**Commentaires**	**Approbateur**
Janvier 2017	1.0	Ghislain AGUIE & Freddy ECHUI	Création du document	Laurent COFFIE
Avril 2017	1.1	Freddy ECHUI	Mise à jour	Laurent COFFIE

SOMMAIRE

Sigles

AC	Autorité de Certification
AE	Autorité d'Enregistrement
DN	Distinguish Name
DPC	Déclaration de la Pratique de Certification
ITA	International Telecom Assistance
LRC	Liste de Révocation de Certificats
MC	Mandataire de Certification
PC	Politique de certification
PKI	Public Key Infrastructure
RDN	Relative Distinguish Name
SCP	Service de Certification Publique
UGC	Unité de Gestion des Certificats

Définitions

Algorithme : Exécutiond'un ensemble d'opérations ou d'instructions permettant d'obtenir un résultat donné répondant à un problème donné.

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

Autorité d'enregistrement : Organisme ou agent autorisé par ITA à émettre le Certificat ITA.

Autorité de certification: Tierce partie qui signe et délivre des certificats.

Certificat : Clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC: Certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats AC (certificat auto signé).

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

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

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

Déclaration des Pratiques de Certification (DPC) :une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

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

Fonction de hachage : Fonctionparticulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale.

Gestionnaire de certificat:système logiciel qui gère les clés cryptographiques pour des utilisateurs.

Liste de Certificats Révoqués : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

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

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

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une requête de signature de certificat (CertificateSigningRequest, CSRen anglais).

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

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

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

Utilisateur / Client : toute personne enregistrée par ITA, et à qui ITA à délivré un certificat ITA.

1 INTRODUCTION

1.1 Présentationgénérale

International Telecom Assistance S.A (ci-après dénommée «ITA CertificateAuthority») en tant qu'Autorité de Certification (AC) agit comme un tiers de confiance pour confirmer qu'une clé publique appartient à une entité nommée. Cette confirmation est expressément représentée par un Certificat ITA X.509 Version 3 (ci-après dénommé Certificat) - Un certificat délivré est une déclaration de l'AC indiquant que le certificat est associé à une personne ou un équipement nommé de façon unique au sein de ce certificat.

Pour jouer son rôle d'AC, ITA a créé un Service de Certification Publique (ITA SCP) pour émettre, gérer, révoquer et renouveler des certificats conformément aux pratiques énoncées dans la présente Déclaration des Pratiques de Certification («DPC»). L'ITA SCP est conçu pour fournir des services électroniques sécurisés et d'autres services de sécurité générale.

La DPC de ITA est un exposé détaillé des pratiques et procédures opérationnelles de ITA. Il prend en charge plusieurs Politiques de Certificat (PC) qui sont implémentées par ITA. Une PC est un ensemble de règles qui indiquent l'applicabilité d'un certificat à une communauté et / ou une classe particulière d'applications ayant des exigences de sécurité communes. Tout utilisateur devrait pouvoir consulter la PC applicable, afin de décider s'il doit ou non faire usage de tels certificats pour ses besoins.

Chaque PC correspondant à un certificat, est représentée dans ledit certificat par un Identifiant d'Objet Unique et enregistré (ci-après dénommé OID). ITA peut mettre en œuvre diverses PC à tout moment. Chaque PC peut être trouvée sur le site Web de ITA à l'adresse http://www.ita-ci.com ou à toute autre adressedésignée par ITA.

La DPC de ITA est :

(i) destinée à être applicable et à être un document juridiquement contraignant entre ITA,l'Autorité d'Enregistrement (AE), le partenaire,leutilisateur, le tiers de confiance et chacun de leur personnel ;

(ii) destinée à servir d'avis à toutes les parties dans le contexte de la SPC de ITA et les parties au sein de ITA SPC sont tenues de comprendre et consulter cette DPC à tout moment pendant la durée de vie du certificat du client.

1.2 Identification

La présente DPC appelée est la propriété de ITA. Cette DPC contient des OID unique par type de certificats:

- AC <Certificat Personne Physique>
    - Offre ITA Personnes Physiques : usage Signature et Authentification;
        - OID: 1.3.6.1.4.1.49449.1.1.101.14
- AC Certificat Personne Morale
    - offre ITA Personnes Morale
        - OID: 1.3.6.1.4.1.49449.1.1.101.12
- AC Certificat Serveur
        - OID: 1.3.6.1.4.1.49449.1.1.101.15
- AC Certificat Employé Personne MoraleOID: 1.3.6.1.4.1.49449.1.1.101.13

1.3 Acteurs du service de gestion des clés

1.3.1 Autorité de certification (AC)

ITA est l'AC qui va créer et signer le certificat. Le certificat associe la clé publique de chaque utilisateur à chaque certificat généré. ITA publiera l'état du certificat à l'aide de Listes de Révocation de Certificats (LRC) et appliquera la PC pour chaque certificat délivré.

ITA peut effectuer une certification croisée avec d'autres AC au sein et / ou en dehors de ITA SCP. La certification croisée est un processus exécuté par ITA où ITA passe en revue touts les documents, les pratiques et les procédures applicables des autres AC. Le tiers de confiance doit également examiner la documentation, les pratiques et les procédures applicables de l'autre AC, si la partie qui détient choisit de se fonder sur les certificats délivrés par cette autorité de certification. Le processus de certification croisée ne correspond en aucun cas à l'approbation de l'autre AC par ITA.

1.3.2 Autorité d'enregistrement (AE)

L'AE de ITA autorisée procède à l'enregistrement des données des utilisateurs. Ces procédures d'enregistrement sont requises, conçues et approuvées par ITA Conformément à la PC applicable, à la présente DPC et à l'accord AE applicable. Une AE doit fournir à ITA le nom, l'identification et les coordonnées (y compris les coordonnées postales, adresses et numéros de téléphone, etc) de chaque utilisateur à certifier. L'AE doit utiliser lesinformations fournies par l'utilisateur pour créer le certificat. Une AE peut employer des Agent(s) chargé(s) d'effectuer les fonctions d'enregistrement et auquel cas, l'AE est directement responsable des activités de l'agent(s) et des fonctions que l'agent effectue pour le compte de l'AE. Les actions, inactions et / ou omissions de chaque agent sont réputées être les actions, inactions et / ou omissions de l'AE.

Une AE peut être un sous traitant, si elle remplit les exigences et définitions du sous-traitant comme indiqué ci-dessous. Dans un tel cas, l'AE sera appelée «AE sous-traitant».

Une AE exerçant les fonctions de AE sans aucune obligation de paiement, comme l'exige un sous-traitant, est appelée «AE non sous-traitant».

Le terme AE désigne collectivement l'AE sous-traitant et l'AE non sous-traitant.

1.3.3 Client

Le termeclientdésigne les personnes physiques, les personnes morales, les serveurs d'applications ou toute autre entité titulaire de tout certificat délivré par ITA.

1.3.4 Mandataire de certification (MC)

Un Mandataire de Certification est une personne physique, en relation avec l'entité légale du Client, mandatée par un Client afin d'authentifier des porteurs du Client, de procéder aux enregistrements et demande de certificat auprès de l'AE, et de remettre les supports de bi-clés aux porteurs. En aucun cas, le MC n'a accès aux moyens qui lui permettrait d'activer et d'utiliser la clé privée, associée à la clé publique contenue dans le certificat, délivré au porteur. Le porteur reste seul capable de mettre en œuvre la clé privée qui lui est remise par l'AE ou le MC.

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité qui souhaite délivrer des certificats à ses porteurs. Une même entité peut s'appuyer sur un ou plusieurs MC. Dans le cas où elle y a recours, le MC est formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE.

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC.Dans tous les cas, le MC agit conformément à la PC et à la DPC associée qui sont établies par l'AGPC et au contrat qui la lie à l'AE via les CGU qu'il signe.

En fonction des services qu'il met en œuvre, le MC respecte les exigences qui incombent à l'AE pour les services supportées. La PC ne précise donc pas les procédures avec ou sans MC. La DPC apporte ces précisions.

Ce mandat stipule notamment que le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC ;
- Respecter les engagements décrits dans les CG ;
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

Un mandat de MC est valable tant que la personne est toujours habilitée par le Client à être MC et que le Client n'a pas communiqué la fin du mandat de MC pour une personne désignée à l'AE.

L'entité signale à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigne un successeur

1.3.5 Domaines d'application

Les certificats ITA sont destinés à être utilisés pour prendre en charge les besoins de sécurité de base suivants:

- Authentification - assure l'identité de l'abonné;
- Intégrité des messages - assure que le contenu d'un message est intact et n'a pas été modifié entre le moment de l'envoi et sa réception;
- Signature numérique - aider toute partie de confiance à empêcher un abonné de nier qu'un tel abonné ait autorisé une transaction particulière si cet abonné a signé la transaction numériquement.

ITApropose des classes de certificats distinctes dans le ITA SCP. L'étendue et la portée de l'utilisation de chaque catégorie de certificat et les restrictions relatives à chaque catégorie de certificat sont déterminées et établies spécifiquement à chaque PC. Chaque classe de certificats est décrite et est présentée dans la PCcorrespondante. Toutes les AE, les sous-traitants, les utilisateurs et les tiers de confiance doivent connaître les termes, conditions, exigences, recommandations et dispositions de la PCapplicable.

Les certificats ITA peuvent être utilisés pour diverses applications comme indiqué dans les exemples sur le site ITA à www.ita-ci.com.Les utilisateurs et les tiers de confiance doivent évaluer et déterminer de façon indépendante le caractère approprié de chaque catégorie de certificat pour un usage particulier.

ITA ne sera pas tenu responsable de toute utilisation d'un Certificat, à moins que ITA ne se soit expressément engagé à assumer les responsabilités contenues dans cette DPC.

1.4 Gestion de la PC

1.5 Entité gérant la DPC

Cette DPC est publiée et gérée par International Telecom Assistance S.A, Abidjan.

1.5.1 Point de contact

Coordonnées de la personne ou de la Direction responsable de l'élaboration de la DPC :

- ITA S.A ;
- Nom de la personne : Laurent COFFIE

- Contact : (+225) 07 89 69 12
- Email : laurent@ita-ci.com
- Adresse : ABIDJAN Plateau, Avenue Chardy, Immeuble Chardy 8e étage Suite 8 A 01 BP 12333 Abidjan 01 COTE D'IVOIRE
- Email : www.ita-ci.com
- Téléphone : (+225) 20 33 20 57/ 20 33 20 39
- Fax : (+225) 20 33 20 55

1.5.2 Responsable conformité DPC - PC

La gestion de la conformité de la DPC avec toute PC est sous la supervision du Directeur Technique de ITA.

2 Dispositions générales

2.1 Obligations

2.1.1 Obligations de l'AC

Nonobstant toute autre disposition contraire contenue dans la présente DPC, ITA a pour obligation de s'assurer que:

- l'algorithme de clé publique utilisé et déployé par ITA n'est pas compromis;
- la clé de signature privée de l'AC ITA sera raisonnablement sécurisée et protégée dans le SCP de ITA conformément aux pratiques courantes de l'industrie.

Les dispositions énoncées ci-dessus seront les obligations uniques et absolues de ITA en ce qui concerne sa capacité en tant qu'AC et aucune disposition contenue dans le présent document ne sera réputée ou interprétée de sorte que ITA sera obligée d'exécuter toute autre fonction ou être tenue de faire en sorte que d'autres fins soient exercées par ITA, ses employés ou ses agents.

Pour des raisons de clarté, cette DPC définit les procédures appliquées par ITA et la technologie selon laquelle ITA déploie ces services.Toutefois, ces procédures ne sont pas considérées comme des obligations de ITA d'exécuter, d'adhérer ou de se conformer ; mais elles ne représentent que des procédures par lesquelles ITA opère son SCP.La seule obligation par laquelle ITA est tenue d'exécuter, d'adhérer ou de se conformer est exposée ci-dessus.

ITA ne sera pas responsable des pertes, dommages ou pénalités résultant de retards ou d'échecs d'exécution résultant d'actes de Dieu ou d'autres causes indépendantes de sa volonté.Pour des raisons de clarté, ces événements comprennent, mais sans s'y limiter, les grèves ou autres conflits de travail, les émeutes, les troubles civils, les actions ou les actions des fournisseurs, les actes de force majeure, la guerre, l'incendie, l'explosion, le tremblement de terreou autres catastrophes.

Dans l'un ou l'autre des cas figures énumérés ci-dessus, ITA sera, pour la durée de cet événement, dégagé de toute obligation, responsabilité et devoirs en vertu de la présente Clause 2.1.1, de cette DPC et du PCcorrespondant affecté par l'évènement.

2.1.2 Obligations de l'AE

L'AE est tenue de se conformer à toutes les procédures et garanties d'enregistrement qui peuvent être déterminées par ITA et qui sont énoncées dans la présente DPC ou dans la convention AE applicable et qui peuvent être ultérieurement modifiées par ITA.

L'AE doit respecter et se conformer notamment aux dispositions de la présente DPC, incluant mais sans s'y limiter, les dispositions énoncées à la clause 3 (Identification et authentification) ci-dessous.

L'AE est seulement autorisée à émettre des certificats aux utilisateurs, mais n'est pas autorisée à suspendre ou révoquer des certificats en aucune circonstance.

2.1.3 Obligations des utilisateurs

Tous les utilisateurs sont tenus de se conformer strictement aux procédures en ce qui concerne l'application du certificat. Ils sont responsables de la protection de leurs clés privées et les procédures d'applications de certificat suivantes :

- Toutes les déclarations ou renseignements fournis par l'utilisateur dans les formulaires de demande de certificat doivent être à tous égards complets, exacts, véridiques et pourraient être vérifiés par ITA ou l'AE ;

- Que toutes les mesures de sécurité physique décrites dans la présente DPC ou qui peuvent être applicables ou recommandées par ITA sont respectées et pour assurer une protection adéquate et sécurisée des clés privées de l'utilisateur ;

- Que l'Abonné soit au courant des dispositions de la présente DPC et de la PC relative à son certificat et qu'il connaisse les restrictions applicables à l'utilisation du certificat d'utilisateur et s'y conforme; et

- Que l'Abonné notifie sans délai à ITA, ou l'AE applicable, immédiatement après la survenance d'un événement qui a compromis, y compris, mais sans s'y limiter la perte, le déplacement ou l'exposition des clés privées de l'utilisateur.

2.1.4 Disponibilité du répertoire

ITA publie les certificats des utilisateurs et les LRC dans le répertoire ITA. Ce répertoire est disponible sur Internet et fournit des opérations quotidiennes de 24 heuresavec un tauxde disponibilité de 99,7% en un an.

ITA veillera à ce que le temps d'arrêt du répertoire ne dépasse pas 30 minutes à un moment donné.

2.2 Responsabilité

2.2.1 Responsabilité de l'AC

Les garanties fournies par l'AC et leurs limites sont les suivantes :

ITA ne fournit aucune autre garantie express ou implicite et n'y aucune autre obligation aux termes de cette DPC et sauf celles expressément prévues dans ce qui précède, ITA rejette toutes les garanties et obligations de tout type, y compris, par exemple et non limitatif; (i) toute garantie de commercialisation; (ii) toute garantie d'adaptation à un usage particulier; (iii) que l'utilisation du certificat ou de tout logiciel fourni et / ou fourni par cette section et / ou en vertu de cette DPC ne contre pas tout brevet, droit

d'auteur ou marque ou autre droit de propriété d'autres; (iv) et toute garantie de l'exactitude des informations fournies, et décline en outre toute responsabilité pour négligence et laxisme.

ITA ne garantit pas l'exactitude, l'authenticité, la fiabilité, l'intégrité, l'actualité, la qualité marchande ou l'adéquation de l'objet par rapport à toute information contenue dans le Certificat ou compilée, publiée ou diffusée par ITA ou pour ITA et renonce à toute responsabilité pour les représentations d'informations.

Les types de dommages considérés :

- ITA ne sera pas responsable des pertes ou dommages, quels qu'ils soient, causés directement ou indirectement en relation avec l'utilisation ou le recours à un Certificat par des parties ;

- Nonobstant toute autre disposition contraire, ITA a expressément exclu la responsabilité pour tous dommages indirects, spéciaux, accessoires et consécutifs, quels qu'en soient les causes, y compris, sans limitation, négligence, défaut ou tout acte de ITA, de ses employés, de ses agents , Les entrepreneurs, les représentants, y compris, mais sans s'y limiter, les pertes ou dommages à d'autres équipements ou biens ou pour perte de profit, d'affaires, de revenus, d'écart d'acquisition ou d'épargne anticipée en vertu de l'utilisation ou de la confiance de tout Certificat ou de toute autre transaction, Par cette DPC même si ITA a été informé de la possibilité de tels dommages. Aucune action découlant de l'utilisation ou de la dépendance d'un certificat, quelle que soit sa forme, ne peut être intentée par une partie plus d'un (1) an après l'apparition de la cause d'action.

La limitation des pertes est telle que :

- Sous réserve des dispositions de la présente clause, dans le cas où (i) toute limitation ou disposition contenue dans le présent Contrat est jugée invalide pour quelque raison que ce soit;et (ii) ITA enfreint l'une de ses obligations en vertu de la clause 2.1 ci-dessus, et ITA devient responsable des pertes ou dommages qui auraient autrement été exclus en vertu des présentes ou susceptibles d'être exclus en droit, (a) la responsabilité totale de ITA sera limitée au montant global de sa responsabilité en vertu des polices d'assurance qu'elle souscrit pour chaque certificat au niveau indiqué ci-dessous ou tout autre plafond de responsabilité applicable pour ce Certificat qui peut être ultérieurement modifié par ITA; et (b) ITA ne sera responsable de ces pertes ou dommages que si la perte ou le préjudice est survenu ou est encouru pendant le paiement de la période d'abonnement.

- Cette limitation des dommages s'applique aux pertes et dommages de tous types, y compris, sans s'y limiter, les dommages directs, compensatoires, indirects, spéciaux, consécutifs, exemplaires ou accessoires encourus par toute personne, y compris, sans limitation, un utilisateur, un demandeur, un bénéficiaire qui sont causées par la dépendance ou l'utilisation à un Certificat que ITA émet, gère, utilise ou révoque ou un tel Certificat qui expire.Cette limitation des dommages s'applique aussi bien à la responsabilité contractuelle, délictuelle et à toute autre forme de réclamation. Le plafond de responsabilité de chaque certificat sera le même quel que soit le nombre de signatures numériques, de transactions ou de réclamations liées à ce certificat.Pour chaque catégorie de Certificat, le plafond de responsabilité est stipulé dans son PC respectif. Dans le cas où le plafond de responsabilité est dépassé, le plafond de responsabilité disponible est réparti d'abord sur les revendications les plus anciennes pour obtenir le règlement définitif du litige, sauf ordonnance contraire d'un tribunal compétent. En aucun cas, ITA ne sera obligée de payer plus que le plafond de responsabilité globale pour chaque Certificat, quelle que soit la méthode de répartition entre les demandeurs du montant du plafond de responsabilité

Autres exclusions

- Les SCP de ITA ne sont pas conçus ou autorisés pour l'utilisation ou la revente en tant qu'équipement de commande dans des circonstances dangereuses ou pour des utilisations exigeant des performances sûres telles que l'exploitation d'installations nucléaires, de systèmes de navigation ou de communication d'aéronefs, où l'échec pourrait mener directement à la mort, aux blessures corporelles ou aux dommages environnementaux sévères.

2.2.2 Responsabilité de l'AE

Les engagements de l'AE sont abordées dans l'accord approprié et applicable conclu entre l'AE et ITA.

2.3 Tarifs

ITAfacture les clients et toutes les autres parties pour leur utilisation du SCP de ITA et de tous les clients et toutes ces autres parties sont tenues de payer à ITA ces Tarifs conformément à son tarif et aux moments prescrits par ITA.

Tous les Tarifs sont sujets à changement sept (7) jours après leur affichage sur le site Web de ITA www.ita-ci.com ou peut être notifié par ITA de toute autre manière. Les Tarifs facturés par ITA comprennent:

- Tarif de souscription ou de renouvellement du certificat - se référer à ITA pour le barème des Tarifs ;

- Taris de révocation de certificat - se référer à ITA pour le barème des Tarifs ;

- Tarif de révocation de certificat - se référer à ITA pour le barème des Tarifs ;

- Tarif pour d'autres services tels que les renseignements sur les polices - Liste de Tarifs à déterminer.

- Politique de remboursement - ITA a une politique où aucune somme ne sera remboursée en aucune circonstance.

2.4 Répertoires et publication

2.4.1 Entité en charge de la publication des informations

ITA publie les informations relatives à ITA sur son site Web.

2.5 Fréquence de publication

Les informations, une fois publiées sur le site ITA, resteront accessibles sur le site Web jusqu'à ce qu'une nouvelle version soit disponible.Il est de la seule responsabilitéde ITA de mettre à disposition des anciennes versions de publications sur le site Web.

ITA peut, le cas échéant, mettre en œuvre un contrôle d'accès à certaines publications liées à ITA, tel que déterminé par ITA, de sorte que seuls les abonnés à la SCP de ITA aient le privilège de lire ces publications.

ITA met également en œuvre des mesures de contrôle d'accès et / ou de sécurité telles que seul le personnel autorisé de ITA peut écrire ou modifier la version en ligne de ses publications.

2.5.1 Répertoires

Sous réserve des dispositions de la clause 2.1.1 ci-dessus, ITA doit:

- Publier une copie du certificat d'utilisateur lors de l'acceptation par l'utilisateur du certificat et des données de révocation de la manière et aux moments qu'il juge appropriés, mais suffisamment pour que la partie qui fait confiance puisse accéder à ces informations dans le répertoire ITA;

- Faire des efforts raisonnables pour publier les amendements et modifications apportées à toute information publiée dans le Répertoire ITA et s'efforcer de maintenir à jour toutes les informations publiées dans ce Répertoire.

2.6 Audit de conformité

2.6.1 Fréquence de l'audit de conformité

ITA effectuera une vérification de la conformité de toutes ses procédures et pratiques telles qu'énoncées ici dans cette DPC et la PC appropriée, à la fréquence qui peut être déterminée par ITA ou qui peut être exigée en vertu de la Loi applicable.

ITA soumettra le rapport d'audit de conformité au contrôleur de l'autorité de certification à Abidjan dans les délais requis suivant la fin de la vérification.

2.6.2 Identité / qualifications des évaluateurs

L'évaluateur qui effectuera l'audit de conformité de ITA aura les qualifications et l'expérience qui sont conformes à la loi applicable et aux pratiques de ce secteur d'activité, y compris les qualifications suivantes:

- Être un comptable agréé ou un cabinet d'évaluation agréé, conformément à la loi applicable et aux pratiques du secteur d'activité ;

- Avoir une compétence reconnue des systèmes informatiques, des environnements de réseaux de télécommunications, de la technologie PKI, des normes et des pratiques ;

- Avoir une connaissance des techniques d'audit professionnelles pour tester les systèmes.

2.6.3 Relation entre évaluateurs et entités évaluées

L'auditeur nommé par ITA ou lerégulateur doit être une entité indépendante de tout contrôle de ITA.

2.6.4 Sujets couverts par les évaluations

L'évaluation de la conformité de ITA établira que:

- Toutes les exigences de la PC appuyées par ITA sont suffisamment abordées dans cette DPC, y compris les politiques et pratiques techniques, procédurales et de personnel de ITA.

- ITA met en œuvre ces politiques et pratiques techniques, procédurales et de personnel.

2.6.5 Mesures prises en raison de la carence

Si des irrégularités sont constatées, ITA préparera un rapport sur toute mesure qu'il prendra en réponse au rapport d'audit. Sur la base de la gravité des irrégularités, ITA effectuera les corrections des problèmes de la manière la plus expéditive et conformément à la pratique internationale généralement acceptée et à la loi applicable.

2.6.6 Communication des résultats

Les résultats de l'évaluation de conformité de ITA ne seront rendus publics que si la loi l'exige. Le cas échéant, la méthode et le détail de la notification des résultats de l'audit aux partenaires de ITA (c'est-à-dire le commanditaire, l'AE) seront définis dans les ententes respectives entre ITA et l'autre partie.

2.7 Confidentialité

2.7.1 Types d'informations à caractères confidentiels

Les types d'informationsque ITA gardera confidentiels comprennent les accords, la correspondance et les accords commerciaux avec son sous-traitant, son AE et l'utilisateur. Ces informations sont considérées comme sensibles et ne peuvent être divulguées sans le consentement préalable de l'autre partie, sauf si la loi l'exige.

Toute divulgation de données de l'utilisateur spécifiques par ITA ou l'AE doit être autorisée par l'utilisateur tel que défini au point 1.3.4.

Les clés privées de l'utilisateur doivent être gardées secrètes par l'utilisateur. La divulgation de ces clés par l'utilisateur est à ses risques et périls.

Les résultats de l'évaluation et les informations sont considérés comme sensibles et ne seront divulgués à personne autre que le personnel autorisé et approuvé par ITA. Ces informations ne seront utilisées qu'à des fins d'audit ou lorsque la loi l'exige.

2.7.2 Types d'informations à caractères non confidentiel

Nonobstant toute autre disposition contraire, toutes les informations révélées à ITA et à l'AE dans les formulaires de demande sont considérées et sont réputées ne pas être de nature confidentielle et ITA et son AE sont autorisées à utiliser toutes ces informations de la sorte comme l'exigerait ITA et / ou l'AE dans la conduite des affaires de ITA ou de l'AE, y compris, sans s'y limiter, le droit de diffuser les informations susmentionnées à tout tiers.

Les types d'information qui ne sont pas considérés comme confidentiels comprennent les renseignements relatifs au certificat d'abonné. Les renseignements personnels ou corpAEtifs qui apparaissent dans les annuaires publics ou les sites Web ne sont pas non plus considérés comme confidentiels.

2.7.3 Divulgation des informations sur la révocation / la suspension des certificats

ITA publie les informations de révocation de certificat dans le répertoire ITA.

2.7.4 Adresse aux responsables de l'application de la loi

Dans le cas où ITA est tenu, en vertu de toute disposition de toute règle, règlement ou disposition législative ou par une ordonnance de la cour de divulguer tout renseignement qui est réputé être ou de nature confidentielle en vertu de la présente DPC, ITA est libre de divulguer toutes les informations qui doivent être divulguées en vertu de toute disposition de ces règles, règlements ou dispositions législatives ou par une ordonnance judiciaire sans aucune obligation et toute libération ne doit pas être interprétée comme une violation d'obligations ou Exigences de confidentialité.

2.7.5 Responsabilité civile

Dans le cas où ITA est tenue, en vertu de toute poursuite ou procédure judiciaire engagée par elle-même ou autrement, en vertu de toute disposition d'un règlement, d'une disposition législative ou d'une ordonnance judiciaire de divulguer toute information réputée ou interprétée comme De confidentialité en vertu de la présente DPC, ITA est libre de communiquer toutes les informations requises, disposition de ces règles, règlements ou dispositions légales ou par une ordonnance judiciaire sans aucune

responsabilité et toute libération ne doit pas être interprétée comme un manquement à des obligations ou des exigences de confidentialité.

2.7.6 Divulgation à la demande du propriétaire

Dans le cas où le propriétaire de toute information confidentielle demanderait à ITA de révéler ou de divulguer des informations confidentielles détenues par ledit propriétaire pour quelque raison que ce soit, ITA ne le fera que si elle estime que la divulgation de ces informations n'entraînera pas La survenance de toute responsabilité envers une autre partie et ITA ne sera pas responsable des dommages ou pertes découlant de la révélation ou la divulgation de ces informations confidentielles et le propriétaire des informations confidentielles doit indemniser ITA pour toute responsabilité, dommages, Pertes ou toute autre responsabilité découlant de la révélation ou de la divulgation de ces renseignements confidentiels.

2.7.7 Autres circonstances de divulgation de l'information

Tous ces autres renseignements peuvent être divulgués par ITA aux dates et dans les cas où ITA peut à sa seule discrétion déterminer.

2.8 Droits de propriété intellectuelle

ITA conserve la propriété unique et exclusive de tous les droits, titres et / ou intérêts sur le Certificat et tous les logiciels fournis par ITA. ITA a le droit de continuer à utiliser le Certificat et tous les logiciels fournis sous la forme, de la manière ou du modèle qu'elle choisit.

Toutes les parties doivent reconnaître que tous les droits d'auteur, marques et autres droits de propriété intellectuelle utilisés ou incorporés dans ou en relation avec tout Certificat émis et tous les logiciels fournis par ITA conformément à la présente DPC, y compris tous les documents et manuels s'y rapportant , est et restera la propriété de ITA et les parties ne pourront, pendant ou à tout moment après la révocation, l'expiration ou la suspension d'aucun de leurs Certificats, remettre en question ou contester la propriété ou tout autre droit de ITA.

Les parties reconnaissent également que ces marques de commerce, droits d'auteur et autres droits du certificat appartiennent à ITA et / ou que ITA à le pouvoir d'utiliser toutes les marques de commerce, droits d'auteur et autres droits et ne doit être utilisé par les parties que consentement écrit de ITA. À la résiliation, à la révocation ou à l'expiration d'un certificat, les parties mettront immédiatement un terme à cette utilisation sans recevoir de compensation pour cette interruption et les parties remettront à ITA toutes les copies du certificat et des logiciels fournis par ITA en sa possession ou, à la demande de ITA, détruira toutes copies du Certificat et des logiciels fournis par ITA qu'il a en sa possession et rendra à ITA une attestation que les parties l'ont dûment fait.

Les parties ne peuvent utiliser ou adopter, sans l'autorisation écrite préalable de ITA, pendant ou après l'expiration, la révocation ou la résiliation de tout certificat, un nom, un nom commercial, un style de négociation ou une désignation commerciale qui comprend ou est similaire ou peut être confondu avec la totalité ou une partie de la marque, du nom commercial, du style commercial ou de la désignation commerciale utilisé par ITA.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

Chaque utilisateur sera représenté par un Distinguished Name (DN) clairement distinctif et unique dans le certificat X.509 et conformément à PKIX Partie 1.

Chaque Entité peut utiliser un nom alternatif via leSubjectAlternate Name field (Nom Alternatif du Sujet), qui sera conforme à PKIX Partie 1.

Le DN est encodé en printableString(chaîne imprimable) suivant la norme X.509 ou sous une autre forme, mais ne sera pas vierge.

3.1.2 Importance des noms

Le contenu de chaque champ Nom du certificat et Nom de l'émetteur peut avoir une association avec le nom authentifié de l'abonné.

Dans le cas des individus, le nom distinctif relatif (RDN) doit être une combinaison de prénom, de nom de famille et éventuellement le numéro de la pièce d'identité requise.

3.1.3 Nécessité d'utilisation de noms explicites

Le contenu de chaque champ du certificat et le nom de l'émetteur peuvent avoir une association avec le nom authentifié du client.

Le RDN peut inclure si nécessaire, une fonction ou un rôle organisationnel. Toutefois, le RDN doit refléter le nom légal authentifié du client.

Si un certificat fait référence à un rôle ou à un poste, le certificat peut également contenir l'identité de la personne qui détient ce rôle ou ce poste.

3.1.4 Règles d'interprétation des divers formulaires de nom (Sans objet)

3.1.5 Unicité des noms

Le DN doit être unique pour tous les clients du SCP de ITA. ITA adopte l'identificateur unique de telle sorte que les abonnés avec des noms identiques peuvent être pris en charge par leSCP de ITA.

3.1.6 Procédure de règlement des différends relatifs à la revendication de nom

En cas de litige concernant des réclamations, ITA se réserve le droit de prendre toutes les décisions et sera l'arbitre final de toutes les réclamations relatives aux noms d'utilisateur dans tous les certificats attribués. Une partie qui demande un certificat doit démontrer son droit d'utiliser un nom particulier. ITA aura le droit de refuser tout nom à sa seule et entière discrétion.

3.1.7 Identification, authentification et rôle des marques déposées

L'utilisation de marques de commerce sera réservée aux détenteurs de marques déposées et la preuve documentaire appropriée de cette propriété doit être produite auprès de ITA.

3.1.8 Méthode pour prouver la possession de la clé privée de l'abonné

Le SCP de ITA fournit un ensemble d'informations de configuration pour le client au stade initial de l'enregistrement. Cette information de configuration est ensuite utilisée par le client pour confirmer avec le SCP de ITA qu'il est le propriétaire légitime de la ou des clés privées. Les informations de configuration,sonttransmises au propriétaire via un mode sécurisé.

3.1.9 Authentification de l'identité de l'organisation

Une demande pour qu'un représentant d'organisation, organisation ou serveur d'application soit un client doit être fait par une personne autorisée à agir pour le compte du futur client. ITA ou l'AE effectuera l'authentification face-à-face du client.

L'identification et l'authentification de l'éventuel utilisateur doivent se faire par l'un des suivants:

- ITA ou l'AE doit examiner des copies de la documentation, dûment certifiée par les personnes reconnues par ITA, en apportant la preuve de l'existence de l'organisation;

- Si ITA ou l'AE a déjà établi l'identité d'un particulier, ITA ou l'AE aura le droit de s'appuyer sur une telle vérification initiale et d'utiliser ces informations privées partagées.

ITA ou l'AE vérifiera également l'identité et l'autorité, y compris toutes les lettres d'autorisation, de la personne agissant pour le compte du futur client et son autorité pour recevoir les clés au nom de cette organisation.

ITA ou l'AE tiendra un registre des informations du client tel que décrit dans le formulaire de demande de l'abonné.

3.1.10 Authentification de l'identité individuelle

Le processus d'identification d'un utilisateur diffère selon le type de certificat demandé et peut se faire via: a) la validité du courrier électronique; (B) base de données d'informations fiables (c) authentification face à face (d) nom de domaine et validation de propriété. La PC applicable énonce le processus d'identification pour chaque catégorie de certificat. La demande de certificat doit être faite (i) personnellement par un particulier, (ii) par le représentant dûment autorisé du client.

Pour la validation par e-mail, l'identification et l'authentification de la personne seront effectuées en vérifiant et en vérifiant que l'adresse e-mail de l'abonné existe effectivement.

Pour une base de données d'informations fiables, l'identification et l'authentification de la personne sera effectuée en vérifiant et en vérifiant une base de données existante dans laquelle les détails nécessaires de la personne ont été stockés. Une telle base de données peut être une base de données tiercede celle de ITA existante.

Pour l'identification face-à-face, l'identification et l'authentification de la personne doivent être effectuées par l'un des moyens suivants:

- ITA ou l'AE comparera l'identité de l'individu avec deux pièces d'identité (photocopies et originaux). Le document d'identification doit être une pièce d'identité délivrée par le gouvernement contenant une photographie; ou

- Si ITA ou l'AE a préalablement établi l'identité d'une personne, ITA ou l'AE aura le droit de s'appuyer sur cette vérification initiale et utiliser cette information partagée en privé.

La vérification de la validation du nom de domaine et de la propriété implique de vérifier que le demandeur / l'entité est un détenteur inscrit ou a le contrôle exclusif du nom de domaine à inclure dans le nom du certificat dans lequel les éléments suivants seront vérifiés :

- l'existence et l'identité légales du demandeur ;

- l'existence physique du demandeur (présence d'entreprise à une adresse physique) ;

- l'existence opérationnelle ou l'inscription de l'entreprise du demandeur (activité commerciale).

ITA ou l'AE enregistrera les informations de l'utilisateur telles qu'elles sont détaillées dans le formulaire de demande.

3.2 Procédure de renouvellement

Un mois avant l'expiration de chaque certificat, ITA enverra un avis de renouvellement d'abonnement, ainsi que toute information applicable au client. Les avis de renouvellement peuvent être envoyés par ITA par courrier ou par courrier électronique conformément aux dispositions prévues par la DPC.

Le client peut choisir de renouveler la période de souscription par le paiement des frais de souscription ou de renouvellement nécessaires à ITA.

Seuls (i) l'utilisateur, (ii) le mandataire ; ou (iii) toute autre partie dûment autorisée par le client payeur ou le mandataire, peut renouveler le contrat.

3.3 Renouvellement après révocation

En cas de soupçon de compromis clé, le certificat délivré doit être révoqué. Il est de la responsabilité de ce client de le notifier immédiatement à ITA ou l'AE qui a délivré le Certificat. Le processus de renouvellement effectué par ITAou l'AE après cette révocation se fera de la même manière que l'enregistrement initial. Tout changement apporté aux informations contenues dans un certificat devra être ré-certifié par ITAou l'AE pertinente avant qu'aucun autre certificat ne soit délivré.

3.4 Demande de révocation

ITA ou l'AE vérifiera toute demande de révocation d'un certificat. Les modalités de traitement de toute demande de révocation et les moyens par lesquels sa validité est établie seront stipulés à la clause 4.4.2.

Toutes les demandes de révocation seront enregistrées par ITA ou son AE selon le cas.

4 Exigences opérationnelles

4.1 Demande de certificat

4.1.1 Origine de la demande

Le SCP deITA prend en charge les demandes de certificat en face-à-face. Le processus de demande diffère selon les types de certificats ITA et respecte les procédures établies par chaque PC respectif.

4.1.2 Demande face-à-face

Pour la demande face-à-face, ITA exige du demandeur de:

- Soumettre en personne un formulaire dûment rempli et signé. Le formulaire doit inclure les conditions d'utilisations.

- Fournir des documents d'identification tels que:

Type d'utilisateur	Document d'identification
Personnes physiques: • Ivoirien	• CNI / Attestation d'identité plus le récépissé d'identification ONI

• Non-ivoirien	• Carte de séjour / Passeport
Personnes morales	Procuration signée par le mandataire et le représentant légal, et document d'identification du demandeur et du mandataire mentionné ci-dessus, y compris les autres types de document que ITA peut exiger de temps à autre. NB : ITA vérifiera la preuve de l'existence de la société
Organisation	• Procuration de l'entreprisepour la délivrancede certificat mentionnant les références du futur titulaire ; • Les documents d'identification de l'utilisateur (Document tel qu'indiqué ci-dessus) ; • tout autre type de documents que ITA peut exiger de temps à autre. NB : ITA vérifiera la preuve de l'existence de la société
Serveur d'application	• Procuration de l'entreprise pour la délivrance de certificat mentionnant les références du futur titulaire ; • Les documents d'identification de l'utilisateur (Document tel qu'indiqué ci-dessus) ; • Justification de propriété du nom de domaine du serveur.
SSL	Idem que ci-dessus et propriété du nom de domaine sauf qu'une vérification face à face n'est pas nécessaire après toutes vérifications et validations achevées

Les formulaires de demande remplis et les photocopies des pièces justificatives pertinentes sont déposés et archivés pour une période de sept ans ou jusqu'à ce que l'abonnement de ITA au demandeur soit invalidé, selon la plus longue des deux.

ITA ou l'AE sont responsables de s'assurer que la vérification de l'identité du demandeur est dûment effectuée. Le nom, la désignation, la signature et la date de vérification du vérificateur sont enregistrés à des fins de reddition de comptes et de vérification.

4.2 Délivrance du certificat

4.2.1 Actions de l'AC concernant la délivrance du certificat

Au cours du processus de délivrance du certificat, l'unité de gestion des certificats (UGC) recevra un ensemble de codes secrets et l'UGC aura le contrôle du processus de génération du certificat.

4.2.2 Conditions de délivrance des codes

ITA ou l'AE délivre l'ensemble de codes uniquesà l'utilisateur seulement si toutes les conditions suivantes sont remplies:

- Les procédures de demande de certificat énoncées ci-dessus sont respectées;
- Le paiement est effectué par le client;
- ITA ou l'AE approuve la demande.

4.2.3 Notification par l'AC de la délivrance du certificat

La méthode d'émission de l'ensemble des codes uniques diffère selon les différents types de certificats ITAet elle respecte les procédures décrites ci-dessous:

- Pour tous les Certificats ITA, les codes sont délivrés au demandeur de façon sécurisée, par exemple imprimé sous plis fermé, livré en mains propres à l'utilisateur ou envoyé par courrier électronique chiffré.

- Pour les certificats d'essai, aucun code ne sera émis. Les certificats d'essai sont délivrés directement au client.

4.2.4 La génération du certificat

À la réception de l'ensemble des codes uniques, l'UGC peut procéder à la génération du certificat. Le processus de génération de certificats utilise le logiciel autorisé ITA et implique les étapes suivantes:

- L'application utilisée par ITA génère la paire de clés de signature de l'utilisateur et envoie une clé de vérification publique au serveur pour la certification. Celui-ci est communiqué en toute sécurité via Internet en utilisant le secret partagé, c'est-à-dire les codes uniques établis précédemment délivrés à l'UGC. Alternativement, le SCP de ITA prend également en charge les demandes de certificats aux normes PKCS # 10 ;

- ITA valide l'authenticité de la demande de certification et lors de la validation, crée le certificat de vérification de l'abonné ;

- Le cas échéant, ITA crée la paire de clés de cryptage de l'utilisateur et le certificat.

4.3 L'acceptation du certificat

Le SCP de ITA prend en charge différents processus d'acceptation de certificats pour chaque type de certificats de ITAet respecte les procédures établies par chaque PC respective.

ITA exige que toutes les acceptations de certificats soient formellement reconnues et acceptés par le client après que l'AC ou l'AE a émis le certificat.

4.4 Révocation de certificat

4.4.1 Circonstances de la révocation

Un certificat doit être révoqué dans les circonstances suivantes (y compris, mais sans s'y limiter):

- Les paires de clés sont remplacées par un nouvel ensemble. ;

- La clé privée correspondant à la clé publique a été compromise ;

- Un changement des informations contenues dans le certificat;

- Cessation d'exploitation c'est-à-dire lorsque ce certificat n'est plus nécessaire pour son objectif initial ;

- Cessation des activités du client ;

- Le non paiement du renouvellement du certificat;

- Le client enfreint ou manqueaux obligations qui lui incombe en vertu de la présente DPC ou de tout autre accord, règlement ou loi qui pourrait être en vigueur ;

- L'utilisateur n'appartient pas à la communauté dont il est membre et qui est assujetti à la politique de certificat. (Par exemple en cas de décès ou de cessation d'emploi) ;

- Une demande de révocation est faite par le client ;

- ITA s'aperçoit que le certificat n'a pas été délivré conformément à la DPC ;

- La clé de certification de ITA a été compromise ou la cessation des opérations de ITA en tant qu'autorité de certification ;

- Toute autre circonstance pouvant être déterminée par ITA de temps à autre ou conformément aux exigences, règles ou règlements de la loi applicable.

ITA n'a aucune obligation de divulguer la raison de la révocation.

4.4.2 Personnes pouvant demander une révocation de certificat

La demande de révocation ne peut être faite que par:

- Le client à qui le certificat a été délivré;

- Le représentant dûment autorisé du client.

- Le personnel autorisé de l'AEde ITA ou lorsquel'utilisateur a enfreint l'accord, le règlement ou la loi qui peut être en vigueur.

4.4.3 Procédure de demande de révocation

Une demande de révocation est formulée par le client dès qu'un évènement susceptible de compromettre son certificat est effectif.

Le SCP de ITA prend en charge différentes procédures de demande de révocation conformément aux procédures décrites dans les dispositions «Perte et remplacement» de chaque PC respective. Celles-ci inclus:

- Une demande de révocation faite personnellement ;

- Une demande de révocation faite par télécopieur ou par téléphone, où des contrôles stricts sont incorporés pour s'assurer que le demandeur est effectivement le personnel autorisé comme indiqué en 4.4.2

ITA ou l'AE qui exécute les demandes de révocation doit s'assurer que la vérification de l'identité et de l'autorité du demandeur est dûment effectuée. La date,le nom, la fonction, la signature de l'agent qui a effectué la vérification et la révocation sont consignés pour des raisons de contrôle.

ITA s'assurera que le demandeur de révocation remplisse ultérieurement le cas échéant un «Formulaire de demande de gestion de certificat ITA» en plus des documents justificatifs définis à l'article 4.1.2 afin que ITA ou son l'AE vérifient et exécutent la demande de révocation.

4.4.4 Délai de traitement d'une demande de révocation

Le SCP ITAprévoit un délai de traitement des demandes de révocation conformément aux procédures ci-après. Ceux-ci inclus:

- Pour tous les certificats ITA, l'action de révocation doit être initiée immédiatement dans les 6 heures après la réception de la demande de révocation et mise à jour de la LRC est immédiate ;

- Toute demande de révocation, authentifiée et établie par ITA est traitée en urgence par les services appropriés de ITA dans un délai de 6 heures sauf les week-ends et jour fériés.

Sous réserve des dispositions de la clause dans le point 2.4.2 ci-dessus, ITA informera l'abonné de l'action de révocation par télécopieur, courriel ou téléphone dans les quarante-huit heures (48H) de cette révocation dans un avis incluant la date, l'heure et le motif de la révocation.

4.4.5 Circonstances de suspension

Un certificat peut être suspendu pour les raisons suivantes:

- Le certificat ne contient pas d'informations valides ;
- Le certificat pendant l'émission a été fourni avec des informations trompeuses et fausses ;
- La clé privée correspondant à la clé publique dans ce certificat est suspectée d'être compromise ;
- Le paiement du renouvellement du certificat n'est pas reçu dans les trente (30) jours suivant l'expiration du certificat.

4.4.6 Qui peut demander la suspension

La demande de suspension ne peut être faite que par:

- L'utilisateur à qui le certificat a été délivré ;
- Le représentant du clientdûment autorisé ;
- Le personnel autorisé de l'AE de ITA lorsque le client a violé l'entente, la réglementation ou la loi en vigueur.

4.4.7 Procédure de demande de suspension

Le SCP de ITA gère les différentes procédures de demande de suspension conformément aux procédures décrites dans les dispositions «Perte et remplacement» dans chaque PC respective.Celles-ci inclus:

- La demande de suspension est présentée en personne ;
- La demande de suspension est faite par télécopieur ou par téléphone lorsque des vérifications rigoureuses sont effectuées pour s'assurer que l'utilisateur est effectivement le personnel autorisé tel qu'indiqué dans le point 4.4.6.

ITA ou l'AE qui exécute les demandes de suspension doit veiller à ce que la vérification de l'identité et de l'autorité de l'utilisateur soit dûment effectuée. Le nom, la désignation, la signature et la date du vérificateur pour lesquels la vérification et la suspension sont effectuées sont consignés à des fins de reddition de comptes et de vérification.

ITA exige que le demandeur de suspension soumette un «Formulaire de demande de gestion de certificat ITA» en plus des documents justificatifs définis au 4.1.2 pour que ITA ou l'AE vérifient et exécutent la demande de suspension.

4.4.8 Limites de la période de suspension

La période de suspension sera d'un mois à compter de la réception de la demande de suspension. Toute extension supplémentaire de cette limite sera soumise à la discrétion de ITA.

4.4.9 Fréquence d'émission des LRC

ITA met à jour et publie la Liste de révocation de certificats (LRC) toutes les quarante-huit heures (48h)

4.4.10 Exigences de vérification des LRC

Il est vivement conseillé à la Partie qui fait confiance (i) de vérifier l'état du Certificat par rapport à la LCR mise à jour publiée par ITA avant leur utilisation; (Ii) vérifier l'authenticité et l'intégrité de la LCR pour s'assurer qu'elle est délivrée et signée numériquement par ITA.

ITA met à jour et publie la liste de révocation de certificats (LRC) toutes les quarante-huit heures après toute demande de révocation. Il est de la seule responsabilité de la partie tierce de s'assurer que le certificat en cours d'utilisation est validé par rapport à la LRC mise à jour publiée par ITA.

4.4.11 Disponibilité en ligne de la révocation / vérification d'état (non applicable)

4.4.12 Exigences en matière de vérification de révocation en ligne (sans objet)

4.4.13 Autres formes de révocation Publicités disponibles (Sans objet)

4.4.14 Vérification des exigences relatives aux autres formes de publicité de révocation (Sans objet)

4.4.15 Exigences particulières aux clés compromises

Toutes les demandes de révocation sont traitées conformément aux exigences opérationnelles énoncées aux clauses 4.4.1 à 4.4.4. Aucune exigence particulière n'est requise lorsque le certificat est révoqué en raison d'un compromis clé.

4.5 Evaluation des procédures de sécurité

4.5.1 Types d'événements enregistrés

ITA gère les journaux d'audit pour toutes les questions liées au système. Les journaux, manuels ou électroniques, contiendront la date et l'heure de l'événement et l'identité de l'entité qui a causé l'événement.

ITA gère également les journaux d'audit pour les questions non liées au système, par exempleles journaux d'accès physique, les changements de personnel.

4.5.2 Fréquence de traitement des journaux d'événements

ITA examine les journaux de traitement au moins une fois par semaine et les mesures prises à partir de ces examens sont documentées à des fins de responsabilisation et d'audit.

4.5.3 Période de conservation des journaux d'événements

ITA conserve ses journaux d'évènement sur place pendant au moins deux mois et les archive ensuite hors site pendant au moins sept ans.

4.5.4 Protection du journal d'évènement

ITA met en œuvre des contrôles d'accès stricts pour s'assurer que seul le personnel autorisé ITA peut accéder à ces journaux d'audit. Ces journaux sont protégés contre l'affichage, la modification et la suppression non autorisés

4.5.5 Procédures de sauvegarde du journal d'évènement

ITA s'assure que tous les rapports d'audit et les résumés d'audit sont sauvegardés conformément aux normes et procédures de sauvegarde ITA. Il s'agit de sauvegardes quotidiennes, hebdomadaires, mensuelles et annuelles, ainsi que des installations de sauvegarde sur site et hors site.

4.5.6 Système de collecte des journaux évènements (interne / externe)

Le système de collecte des journaux évènements du SCP de ITA comprend:

- Le système de gestion des certificats ;
- Le système d'annuaire des certificats ;
- Le système d'accès à distance ;
- Les pare-feu ;
- Le système de détection d'intrusion ;
- Les outils de surveillance de réseau ;

ITA passe en revue constamment d'autres outils de gestions et d'évaluation du système le cas échéant ces systèmes seront mis en œuvre pour appuyer les exigences d'évaluation.

4.5.7 Notification au sujet de la cause de l'événement

La décision de notifier le sujet causant l'événement est à la seule appréciationde ITA. ITA n'est pas obligé de notifier à la personne ou le système ou l'application si elles ont causé un événement qui a été enregistré par les systèmes de vérification du SCP de ITA.

4.5.8 Evaluation de la vulnérabilité

ITA effectuera une vérification du système pour surveiller la vulnérabilité des systèmes à des périodes déterminées par ITA. Le cas échéant, des évaluations de la vulnérabilité seront réalisées et examinées en fonction des résultats ou des recommandations de l'audit.

ITA effectuera également des tests de pénétration du réseau tous les six mois (6 mois).

4.6 Archivage des données

4.6.1 Types de données à conserver

ITA archivera les données des certificats et LRC qu'il émet et la clé privée de cryptage de l'utilisateur aux périodes déterminées par ITA. Il archive également les journaux d'évènement et les informations utilisées pour l'identification et l'authentification.

4.6.2 Période de conservation des archives

La période de conservation des archives du SCP ITA est de sept ans (7ans), sauf indication contraire.

4.6.3 Protection des archives

Les archives sont protégées à un niveau de sécurité physique où seules les personnes autorisées peuvent y accéder. Ils sont également protégés des menaces environnementales telles que la température, l'humidité etmagnétisme.

4.6.4 Procédures de sauvegarde des archives

Tous les documents archivés sont entreposés à des emplacements situés hors du site avec une protection similaire énoncée à la clause 4.6.3.

4.6.5 Exigence d'horodatage des enregistrements

Tous les documents archivés mentionnés à l'article 4.6.1 doivent être horodatés, sauf indication contraire.

4.6.6 Système de collecte des archives (interne ou externe)

Le système de collecte d'archives du SCP de ITA est exécuté manuellement.

4.6.7 Procédures d'obtention et de vérification des archives

ITA vérifiera l'intégrité des informations archivées sur une base annuelle. Des procédures détaillées sont documentées dans les Normes et Procédures de ITA.

4.7 Changement de clé

Le changement de clé automatique est autorisé dans le SCP de ITA. Un utilisateur peut demander l'ouverture de ce processus.

4.8 Restauration des clés / renouvellement des clés

La récupération des clés ou la récupération du certificat est requise si le mot de passe du certificat a été verrouillé ou a expiré. L'utilisateur ou l'AE est tenu de fournir les documents suivants et ITA exigera une vérification face à face.

Type de certificat	Document requis
Certificat de personnes : ▪ Physique ▪ Morales	▪ CNI / Passeport / Carte de séjour ▪ Demande formulaire
▪ Certificat employé personne morale ▪ Certificat serveur	▪ Procuration de la société ▪ CNI de l'agent / Passeport / Carte de séjour ▪ Demande de formulaire
SSL	Justificatif des propriétés du serveur et du nom de domaine

4.9 Compromis et reprise après sinistre

4.9.1 Ressources informatiques, logiciels et / ou corruption de données

Cette disposition sera énoncée dans le plan de reprise d'activité après sinistre.

4.9.2 Révocation de la clé publique

Dans le cas où le certificat d'AC de ITA est révoqué, ITA prendra les mesures nécessaires pour informer tout les clients de cette révocation conformément aux dispositions contenues au point 2.4.2 de la présente DPC.

4.9.3 Compromission de la clé entité

Dans le cas où la clé privée ITA est révoquée, ITA doit effectuer des procédures de reprise après sinistre comme indiqué dans le plan de reprise d'activité.

4.9.4 Sécurité après un type de catastrophe naturelle ou autre

Cette disposition sera décrite dans le plan de reprise d'activité.

4.10 Cessation d'activité

Dans l'éventualité où ITA entend mettre fin à ses activités, ITA remettra à l'AE, et au client un préavis écrit d'au moins trois mois avant de mettre fin à ses activités et suivra les procédures en conformité avec toutes les lois applicables.

ITA prendra des dispositions pour que ses dossiers et certificats soient archivés de façon prescrite par les lois applicables en Côte d'Ivoire.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

Le SCP de ITA hébergé dans un centre de données sécurisé doté de quatre couches de protection pour contrôler l'accès physique au Centre des opérations de ITA. Celles-ci inclus:

a- Une remise d'un badge visiteur ouprestatairecontre un document d'identification à la réception du data center ;

b- Un accès limitéau data center ;

c- Un accès par une porte sécurisée pour entrer dans le data center où est situé le Centre des Opérations (NOC). Le NOC est une pièce distincte du data center et les agents du NOC qui sont en service 24 heures sur 24 et 7 jours assurent que seuls les employés de ITA peuvent accéder à la salle ;

d- Un système de contrôle d'accès biométrique est installé pour contrôler l'accès au NOC.

Un registre manuel renseigné pour suivre l'accès au NOC. Sur la base de la restriction ci-dessus, la personne est tenue de le signer à l'entrée comme à la sortie du NOC. Les personnes sont tenues d'indiquer la date, l'heure et le but de la visite. En outre, les mouvements d'autres personnels autorisés de ITA doivent être accompagnés par le personnel du NOC dans la zone réservée. Une liste du personnel autorisé par ITA est fournie au NOC pour s'assurer que seuls les employés autorisés de ITA peuvent accéder au NOC. Les autres visiteurs, prestataires et / ou fournisseurs de ITA qui souhaitent accéder au NOC doivent être escortés par un personnel autorisé de ITA.

Tous les sites AE deITA doivent également être protégés, afin de s'assurer que seul le personnel autorisé a accès au système de l'AE. Les administrateursde ITAsont responsables de la protection du profil d'administrateur de ITA. Toutes ces exigences et directives sont énoncées dans l'accord AEen vigueur.

L'utilisateur d'un certificatITA doit prendre toutes les dispositions pour s'assurer que ses postes de travail et son mot de passe sont épargnésd'un accès non autorisé et / ou d'une divulgation.

5.1.2 Alimentation électrique et climatisation

Les installations deITA sont adéquatement protégés par des onduleurs (UPS) contre les fluctuations ou la perte totale d'énergie.

ITAdispose également d'un système de climatisation et de refroidissement adéquat pour protégés ses installations.

5.1.3 Vulnérabilité aux dégâts des eaux

Les installations de ITA sont adéquatement protégées contre l'exposition à l'eau et écoulements de liquides.

5.1.4 Prévention et protection incendie

Les installations de ITA sont adéquatement protégées contre les incendies. ITA s'appuie sur les opérations et procédures d'iSTT pour répondre à cette protection. Les exigences en matière de protection contre les incendies de ITA sont précisées dans la convention de gestion de l'installation iSTT et l'accord est révisé annuellement, sauf indication contraire.

5.1.5 Supports de sauvegardes

Le système de stockage utilisé dans les installations de ITA sont protégées contre les menaces environnementales telles que la température, l'humidité et le magnétisme. Les exigences spécifiques sont spécifiées dans la norme de ITA.

5.1.6 Traitement des déchets

ITA effectuera la destruction des données une fois que celles-ci ne sont plus nécessaires et / ou la période d'archivage a expiré. ITA veillera à ce que les médias respectifs qui stockent ces informations soient correctement désinfectés ou détruits avant d'être mis à la décharge.

Toutes les destructions seront enregistrées à des fins d'audit et seront soumis aux critères indépendants qui peuvent être exigés en vertu des lois applicables en Côte d'Ivoire.

5.1.7 Sauvegardes hors site

ITA réalise une sauvegarde hors site pour une reprise de ses services qui sont spécifiés dans le Plan de reprise d'activité de ITA.

Les exigences de sécurité pour la sauvegarde hors site sont similaires à celles qui sont pratiquées parITA, et elles sont en conformité avec les normes de sauvegarde et les procéduresde ITA.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

ITA établit des rôles de confiance pour effectuer la fonction AC. Ceux-ci comprennent :

- Agent (s) de sécurité de l'AC (minimum de 3)
    - Mettre en œuvre les politiques de CA;
    - Incorporer de nouveaux agents de sécurité;
    - Gérer les administrateurs CA;
    - Vérifier les journaux d'audit, PC et conformité à la DPC; et
    - Est le gestionnaire du système.

- Administration
  - gérer le processus d'inscription des utilisateurs; et
  - créer, supprimer, renouveler et / ou révoquer le certificat d'utilisateur.

- Administration (Ingénieur)
  - configurer et maintenir le matériel et les logiciels de l'AC;
  - administrer le début et la cessation des services d'AC; et
  - gérer les prestataires de l'AC.
  - effectuer la surveillance quotidienne des systèmes de l'AC.
  - mener des activités telles que la collecte de journaux et de sauvegarde

- Auditeur
  - vérifier les journaux

La clarification de ces rôles de confiance est faite pour assurer la séparation des tâches de sorte qu'aucune personne ne peut malicieusement utiliser le système de l'AC sans détection. Chacun des rôles de confiance est limité aux actions qu'ils sont tenus d'accomplir dans l'accomplissement de leurs responsabilités.

ITA fournira des recommandations et des directives à l'AE pour s'acquitter de ses responsabilités en tant qu'administrateurs à distance de l'AC. Le cas échéant, l'AE assurera la séparation des tâches manière à ce que toutes les fonctions administratives ne sont pas exécutées par un seul individu.

5.2.2 Nombre de personnes requises par tâches

ITA doit s'assurer qu'aucune personne ne peut accéder aux clés privées de l'utilisateur stockées par l'AC.

Au minimum deux individus, de préférence, utilisentle partage des connaissances comme des mots de passe associés pour effectuer n'importe quelle opération de récupération de clé.

Au minimum deux individus, de préférence en utilisant une technique de partage des connaissances comme des mots de passe jumeaux pour effectuer n'importe quelle opération de récupération de clé.

Toutes les autres fonctions associées aux rôles de l'AC de ITA peuvent être exercées par une seule personne.

5.2.3 Identification et authentification pour chaque rôles

L'identité et les autorisations de tout membre du personnel de l'AC ITA, sont vérifiées et authentifiées avant qu'il ne reçoit un compte ou un certificat pour exercer sa fonction.

Le personnel reconnu de ITA veille à ce que :

- Le compte ou certificat est directement délivré, attribué à un particulier ou à une organisation ;
- Le compte ou le certificat émis n'est pas partagé ;
- Il utilise la restriction d'actions autorisées et/ou un certificat qui lui est délivré pour accomplir le rôle qui lui est dévolu.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Les qualifications et l'expérience du personnel de ITAsont conformes à la responsabilité professionnelle qui leur est attribuée. ITA fournit une formation complète en ce qui concerne les fonctions qu'ils doivent remplir. (ITA peut délivrer des attestations qui peuvent être déterminées par ITA à ce personnel au terme de la formation).

ITA mettra en place des vérifications d'antécédents appropriées pour son personnel clé de l'AC. Les AE sont recommandés pour effectuer ces contrôles pour leurs administrateurs.

ITA établit des contrôles de sorte que le personnel de confiance de l'AC est tenupar la loi ou le contrat de ne pas divulguer des informations sensibles du SCP de ITA.

5.3.2 Procédures de vérification des antécédents

Les employés de ITA sont tenus de déclarer qu'ils n'ont pas d'antécédents judiciaires, ni impliqués dans un arrangement avec des créanciers ou condamnés pour une infraction en Côte d'Ivoire. Le défaut de se conformer entraînera des mesures disciplinaires prises par ITA.

Les employés de ITA sont également tenus de notifier à ITA dans le cas où ils sont impliqués ou peuvent être impliqués dans toute poursuite. Le défaut de se conformer entraînera des mesures disciplinaires prises par ITA.

5.3.3 Exigences en matière de formation initiale

ITA s'assure que son personnel de confiance a été formé en ce qui concerne:

- Les principes et mécanismes de sécurité de ITA ;
- L'utilisation du logiciel d'AC de ITA en cours d'utilisation ;
- Les systèmes d'exploitation et la mise en œuvre de l'infrastructure de l'AC ;
- Les fonctions opérationnelles ;
- Les politiques, normes et procédures de ITA ;
- Les règlements et règles applicables, le cas échéant ;
- La capacité des agents de ITA à délivrer des certificats après la fin de la formation.

5.3.4 Fréquence et séquence de rotation entre différentes attributions

La fréquence renouvellement de la formation est soumise à la fréquence des changements du système d'AC de ITA.

Les exigences de formation sont conformes à celles spécifiées à la clause 5.3.3.

5.3.5 Fréquence et séquence de rotation des travaux (Sans objet).

5.3.6 Sanctions en cas d'actions non autorisées

ITA suspendra l'accès au personnel de confiance, en cas de suspicion, ou au cas om il aura effectué des actions non autorisées telles que l'utilisation non autorisée de l'autorité et l'utilisation non autorisée des systèmes ITA CA ou des opérations.

La suspension sera immédiate au moment de la détection et la période de suspension fera l'objet de rapport d'enquête.

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

ITA n'emploie pas de personnel contractuel pour effectuer les rôles de confiance dans le SCP de ITA.

Dans le cas où les fournisseurs autorisés ITA et / ou les prestataires doivent accéder au système ITA, le personnel ITA autorisé doit les accompagner en tout temps. Toutes les actions effectuées par ces sous-traitants seront enregistrées et consignées à des fins de reddition de comptes et d'audit.

5.3.8 Documentation fournie au personnel

En ce qui concerne la formation énumérée à la clause 5.3.3, les documents respectifs seront mis à la disposition du personnel de ITA si nécessaire.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

L'AC ITA possède un ensemble de paires de clés de signature. La paire de clés est générée à l'aide du logiciel de génération de clé utilisé par ITA.

La génération de paires de clés pour le client est conforme à la PC de ITA.

6.1.2 Bi-clés de Porteurs

La clé privéede ITA est générée lors de l'initialisation du système. Il n'y a pas d'obligations de fournir cette clé, car celle-ci reste dans le système de ITA.

Le SCP de ITA prend en charge les conditions dans lesquelles la clé privée est livrée au client dans une opération sécurisée.

6.1.3 Transmission de la clé publique à l'AC

Le Certificat de ITA est auto-signé et ceci est exécuté à l'étape d'initialisation du système.

La clé publique est transmise à l'AC lors de la génération de la bi-clé, sous un format PKCS#10, et lors d'une connexion sécurisée de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et l'AE.

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

ITA PCS prend en charge les conditions dans lesquelles la clé publique CA est livrée dans une transaction sécurisée en ligne ou téléchargée depuis le site ITA

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le support qui est remis au client lors de la délivrance de son certificat.

6.1.5 Taille des clés

Les paires de clés asymétriques de ITA seront d'au moins 2048 bits pour l'algorithme RSA avec la fonction de hachage SHA-256.

6.1.6 Génération de paramètres de clé publique

Les paramètres de clé publique seront générés via le logiciel de ITA.

6.1.7 Vérification de la qualité des paramètres (non applicable)

6.1.8 Génération de clés matérielles / logicielles

Les paires de clés et de signature de ITA doivent être générées dans un module cryptographique.

Des paires de clés pour tous les clients peuvent être générées dans un module cryptographique logiciel ou matériel.

6.1.9 Principaux buts d'utilisation (selon le champ d'utilisation des clés X.509 v3)

L'utilisation de la clé de ITA est différenciée par les types de certificat.

ITA garantit que la clé de signature est la seule clé autorisée pour la signature de certificats et de LCR.

La clé de signature peut être utilisée pour fournir des services tels que l'authentification, la non-répudiation et l'intégrité des messages.

La paire de clés de cryptage peut être utilisée pour établir une session chiffrée pour l'échange de message.

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

Se référer au point 6.8

6.2.2 Contrôle de la clé privée par plusieurs personnes

L'activation de la clé privée d'AC nécessite la présence d'au moins 2 personnes pour terminer la génération avec succès. Aucun personnel de confiance ITA n'est autorisé à générer la clé privée de l'autorité de certification.

Les individus concernés génèrent les clés privées à l'aide du logiciel de ITA.

6.2.3 Détenteur de clés privées (Ne s'applique pas)

6.2.4 Sauvegarde de clé privée

ITA ne sauvegarde pas les clés de signature privée des clients. Les utilisateurs doivent sauvegarder leurs clés de signature privée et s'assurer que celles-ci sont protégées de manière sécurisée.

ITA peut sauvegarder les clés de chiffrement privées de l'abonné et s'assurer que les clés sont protégées de manière sécurisée.

ITA peut sauvegarder la clé privée d'AC et doit s'assurer que la sauvegarde et le stockage sont aussi sécurisés.

6.2.5 Archivage de la clé privée

Les clés privées d'AC ne font jamais l'objet d'archives

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

Selon le SCP de ITA, seul le responsable de certificats de ITA peut transmettre la clé de signature cryptée au module cryptographique.

6.2.7 Méthode d'activation de la clé privée

L'activation de la clé privée dans le SCP de ITA se fait via l'authentification par mot de passe.

6.2.8 Méthode de désactivation de la clé privée

La désactivation de la clé privée selon le SCP de ITA est la fin du processus. Une fois terminée, les clés doivent être effacées de la mémoire avant que la mémoire ne soit allouée de nouveau.

Le module cryptographique de ITA prend également en charge la désactivation automatique de la clé privée après une période d'inactivité prédéfinie.

6.2.9 Méthode de destruction des clés privées

La procédure de destruction des clés privées selon le SCP de ITA se fait dans les cas suivant :

- Le support de stockage pour le privé est endommagé ou perdu.
- Après la remise des clés parITA ou l'AE.
- Les clés sont remplacées par un nouveau jeu de clés.
- ITA exécute les procédures d'élimination des déchets comme indiqué à la clause 5.1.6.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

ITA effectue l'archivage des clés publiques conformément aux procédures d'archivage.

6.3.2 Durée de vie des clés publiques et privées

La période d'utilisation des clés publiques et privées deITAest conforme à la PC deITA applicable. Les clés de ITA ont une durée de vie allant de six mois, un an, trois ans à vingt-cinq ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Le SCP de ITA prend en charge des données d'activation uniques, de sorte que l'ensemble des codes de référence et d'autorisation et le mot de passe de clé privée sont imprévisibles.

6.4.2 Protection des données d'activation

ITA fournit des recommandations pour s'assurer que les données d'activation sont protégées contre toute utilisation non autorisée, y compris un contrôle d'accès physique et un mécanisme cryptographique où le verrouillage est activé après un nombre prédéterminé de tentatives non autorisées.

6.4.3 Autres aspects de données d'activation (Non applicable)

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

ITA assure que les fonctions de sécurité du SCP de ITA concernent via:

- Identification et authentification forte des utilisateurs pour l'accès au système ;
- Séparation des rôles de confiance ;
- Communication cryptée durant l'utilisation du système d'AC de ITA ;
- Vérification de tous les événements liés à la sécurité.

6.5.2 Évaluation de la sécurité informatique

ITA travaille avec les fournisseurs et organismes standards pour atteindre les normes de sécurité internationales pour le SCP.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Le processus de conception et de développement des applications de ITA s'effectuera comme suit par:

- Vérification / examen par un tiers ;
- Évaluation des risques en cours pour influencer les mesures de sécurité.

6.6.2 Contrôles de gestion de la sécurité

La configuration du SCP de ITA ainsi que les modifications et mises à niveau sera documentée et contrôlée.

ITA mettra en place un système de gestion des changements pour contrôler et surveiller les configurations des systèmes et empêcher toute modification non autorisée.

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

ITA travaille avec différents fournisseurs et organismes de certification pour atteindre les normes de sécurité internationales durant le cycle de vie du SCP de ITA.

6.7 Mesures de sécurité réseau

Un pare-feu doit être utilisé pour protéger l'environnement des opérations d'AC de ITA contre les attaques provenant d'Internet.

L'accès au gestionnaire de certificats ITA, à l'annuaire de certificats ITA, et à tout autre appareil du centre d'opération de ITA ne sera accordé au personnel autorisé ITA que par le biais d'un mécanisme de contrôle d'accès, tel que l'authentification ID et mot de passe.

7 Profils des certificats et des LCR

7.1 Profil des certificats

7.1.1 Numéro (s) de la version

Le Certificat de ITA est de la forme x.509 version 3 conformément à la Recommandation UIT. X.509 et la norme commune ISO / CEI 9594-8.

7.1.2 Identifiant d'algorithmes

Le SCP de ITA prend en charge, sans s'y limiter, les algorithmes suivants :

- RSA 2048/4096/ 6144 signature électronique;
- EllipticCurve -192 signature électronique ;
- RSA 2048/4096/6144 key transfer ;
- SHA-1, SHA-256, SHA-384 et SHA-512;
- Triple-DES et AES ;
- Message Authentication Code (MAC) ;
- MD5 Message-Digest Algorithm.

7.1.3 Formes de noms

ITA respecte des formulaires uniques pour les catégories d'utilisateurs suivants:

- Individuel ;
- Représentant d'entreprise / d'entreprise ;
- Serveur d'applications ;
- La particularité de ces formulaires consiste en des attributs nom commun et / ou numéro de série.

7.1.4 Contraintes de noms (Sans objet)

7.1.5 Identificateur des politiques de certificats (OID)

Type	OID
Personne Morale	1.3.6.1.4.1.49449.1.1.101.12
Employé Personne Morale	1.3.6.1.4.1.49449.1.1.101.13
Personne Physique	1.3.6.1.4.1.49449.1.1.101.14
Serveur	1.3.6.1.4.1.49449.1.1.101.15

7.1.6 Limitation des contraintes de stratégie (Non applicable)

7.1.7 Syntaxe et sémantique (non applicable)

7.1.8 Sémantique de traitement pour l'extension de la politique de certificat critique (Non applicable)

7.2 Profil LCR

7.2.1 Version

La liste LRC de ITA est x.509 version 3 conformément à la Recommandation UIT X.509 et la norme commune ISO / CEI 9594-8.

8 Gestion des cas spécifiques

8.1 Procédure de modification

Avant de faire des changements de PC de ITA et dans cette DPC, ITA documentera la liste des modifications proposées. La liste sera distribuée aux AE, AC auprès desquellesITA a obtenu une certification croisée directe, et l'autorité de régulation en Côte d'Ivoire pour amendement. La période de d'amendement sera de trente jours, sauf indication contraire.

Tous les commentaires seront consolidés et revus par la Direction de ITA. La décision de mettre en œuvre les changements proposés est laissée à la discrétion exclusive de ITA ou, le cas échéant, soumise à l'approbation de l'autorité de régulation. Une décision de changement final sera annoncée après deux semaines.

ITA adhérera à ses procédures de contrôle de la gestion des changements de sorte que toutes les modifications apportées à la PC et à la DPC sont suivis et les contrôles de version soient mis en place.

8.2 Politique de publication et de notification

Tous les articles de PC de ITA et de cette DPC sont soumis à l'obligation de publication et de notification.

Toute publication et notification sera effectuée via le site Web de ITA à l'adresse http://www.ita-ci.com, à moins que la notification ait un gros impact pour ITA, l'AE, le client et la tierce partie.

ITA peut signer numériquement chaque publication et chaque notification avant d'être affichée sur le site Web ITA.

ITA proposera, de temps à autre, et mettra à la disposition des utilisateurs, ou en avisera, ce qui peut être constitué comme des mesures adéquates de protection des clés privées.

ITA mettra à la disposition des utilisateurs, ou les avisera des risques liés à l'utilisation d'un Certificat, émis par ITA, en fonction de toute technologie utilisée par ITA qui a été abandonnée ou remplacée.

8.3 Procédures d'approbation de la DPC

Une fois qu'uneDPC révisée est prête à être publiée, la Direction de ITA l'approuvera avec le conseil juridique des avocats de la Société.