DKBS
DOCUMENT KNOWLEDGE BUSINESS SOLUTIONS
DEPUIS 1994

## Politique de Certification

# AC DKB SOLUTIONS MACHINES 1

# Certificats SSL

# AC DKB SOLUTIONS

| | | | |
|---|---|---|---|
| **Version du document :** | 1.0 | **Nombre total de pages :** | 60 |
| **Statut du document :** | ☐ Projet | ☒ Version finale | |
| **Rédacteur du document :** | DKB SOLUTIONS | DKB SOLUTIONS | |

| | | |
|---|---|---|
| **Liste de diffusion :** | ☒ Externe | ☒ Interne DKB SOLUTIONS |
| | Public | Tous personnels |

| **Historique du document :** | | | | |
|---|---|---|---|---|
| Date | Version | Rédacteur | Commentaires | Vérifié par |
| 01/04/2019 | 0.1 | AYEWA RAISSA | Création du document | DJAHA BERTIN |
| 12/07/2019 | 0.2 | N'GUESSAN SYLVIA | Modification du document | KASSI JAMMES |
| 26/07/2019 | 1.0 | N'GUESSAN SYLVIA | Mise à jour du document et première publication de la PC | KASSI JAMMES |

# SOMMAIRE

# 1 INTRODUCTION

## 1.1 Présentation générale

La dématérialisation, ou conversion au format électronique des transactions quotidiennes traditionnelles (contrats, courrier, factures, formulaires administratifs, etc.), permet avant tout d'accélérer les processus métier et documentaires. En raison de l'aspect innovant et technique de ces processus, les entreprises doivent faire appel à des prestataires de services spécialisés à même d'assurer le rôle de tierce partie de confiance et de fait, de fournir une preuve de la transaction. Les certificats électroniques et les opérations de certification signature électronique se trouvent au cœur de ces technologies.

Dans cette perspective, DKB SOLUTIONS a mis en place pour la délivrance de certificats électroniques les Autorité de Certification dénommées :

- AC DKB SOLUTIONS MACHINES 1;

Qui s'appuient sur une Infrastructure de Gestion de Clés (IGC).

L'AC est certifiée par l'Autorité de Certification Racine (noté ACR) AC RACINE DKB Solutions 1.

Les certificats délivrés par l'AC sont remis à des Contacts Techniques (CT), agissant pour le compte d'entreprises ou d'administrations.

La présente PC a pour objet de décrire la gestion du cycle de vie des :

- Des certificats SSL/TLS délivrés par l'AC,
- Des bi-clés associées,
- L'AC et sa bi-clé.

La présente PC est élaborée conformément :

Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;

Au document : « Electronic Signatures and Infrastructures (ESI), Policy requirements for Trust Service Providers issuing certificates Part 1: General requirements », ETSI EN 319 411-1 v 1.1.1 ;

Au document : « Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons », EN 319 412-2 V2.1.1 (2016-02).

Aux exigences [Mozilla]:https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist qui contient l'ensemble des règles que les AC doivent respecter lorsqu'elles sont signées par une AC Racine (ACR). Dans le cas de la présente PC, l'ACR utilisée est l'ACR «AC RACINE DKB Solutions 1 » pour signer toutes les AC qui émettent des certificats ;

Aux exigences [CAB Forum]: https://cabforum.org/ qui contient l'ensemble des règles de sécurité qui sont référencées par l'ETSI EN 319 401 pour la gestion des certificats dit "OV".

## 1.2 Identification du document

La présente PC appelée : « DKB SOLUTIONS Certificats SSL » est la propriété de DKB SOLUTIONS. Cette PC contient les OID suivants (un seul OID par type de certificats) :

AC DKB Solutions MACHINES 1

- Offre DKB SOLUTIONS SSL Organization Validated (OV)
  - OID: 1.3.6.1.4.1.46111.1.3.101.11

- OCSP pour l'AC DKB SOLUTIONS MACHINES 1
  - OID: 1.3.6.1.4.1.46111.1.3.101.12 ;

La présente PC contient les exigences communes et particulières liées aux services et aux types de certificats gérés par l'AC. La PC précise également les évolutions nécessaires pour le renouvellement de certificat SSL.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

## 1.3 Entités intervenant dans l'IGC

Pour délivrer les certificats, l'AC s'appuie sur les services suivants :

Service d'enregistrement : ce service collecte et vérifie les informations d'identification du CT qui demande un certificat, avant de transmettre la demande de certificat au service de demande de certificat ;

Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par le service d'enregistrement dans le but de créer et de transmettre une demande de certificat au service de génération de certificat ;

Service de génération de certificat : ce service génère les certificats électroniques pour les CT à partir des informations transmises par le service de demande de certificat ;

Service de remise de Certificat : ce service remet au CT son certificat ;

Service de révocation de certificats : ce service traite les demandes de révocation des certificats SSL et détermine les actions à mener, dont la génération des Listes de Certificats Révoqués (LCR) ;

Service de Publication : ce service met à disposition des utilisateurs de certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC, ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations ;

Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci -dessus dans la délivrance des certificats par l'AC aux CT. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

### 1.3.1 Autorité de Gestion des Politiques de Certifications (AGPC)

L'AGPC est DKB SOLUTIONS. L'AGPC est responsable de l'AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité de l'AC est composé de la présente PC, de la DPC associée, des conditions générales d'utilisation et des procédures mises en œuvre par les composantes de l'IGC. L'AGPC valide le référentiel de sécurité composé de la PC et de la DPC. Elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et/ou contrôle de conformités effectuées sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application. Elle valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre.

### 1.3.2 Autorité de Certification Racine (ACR)

L'ACR génère des certificats et révoque (ARL) des certificats d'AC à partir des demandes que lui envoie l'AGPC.

DKB SOLUTIONS s'appuie sur ses propres capacités afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

L'ACR agit conformément aux règles de sécurités qui sont établies par l'AGPC.

DKB SOLUTIONS est ACR au sens de la responsabilité de gestion du cycle de vie des certificats.

### 1.3.3 Autorité de Certification (AC)

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de génération de certificats, de révocation de certificats et de journalisation et d'audit.

DKB SOLUTIONS s'appuie sur ses propres capacités afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

L'AC agit conformément à la présente PC et à la DPC associée qui sont établies par l'AGPC. Dans la présente PC, l'AC est identifiée par son « CN ».

DKB SOLUTIONS est AC.

### 1.3.4 Autorité d'Enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, de remise de Certificat SSL au CT, de révocation de certificats et journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les CT. L'AE est mise en œuvre par DKB SOLUTIONS.

De même, DKB SOLUTIONS en tant qu'AC peut déléguer l'ensemble de l'AE à une entité tierce. En ce cas, un contrat est établi entre l'entité tierce qui sera AE et DKB SOLUTIONS. Dans ce cas, ceux sont l'ensemble des fonctions d'AE qui sont déléguées suivant les procédures définies par DKB SOLUTIONS. Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée qui sont établies par l'AGPC.

### 1.3.5 Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (Se reporter au § 2).

Le SP agit conformément à la PC et à la DPC associée.

### 1.3.6 Autres participants

#### 1.3.6.1 Propriétaire du Nom de Domaine (SSL Serveur)

Le propriétaire du nom de domaine (FQDN, IP ou Wildcard) est l'entité légale qui détient le nom de domaine concerné par la délivrance d'un certificat. Le nom de domaine est géré par un administrateur de nom de domaine désigné par le propriétaire du nom de domaine et tel qu'enregistrer par un Registrar. Le propriétaire de nom de domaine fait appel à un contact technique pour gérer les certificats SSL associé aux noms de domaines dont il est propriétaire.

L'entité légale d'un propriétaire de nom de domaine est représentée par un Représentant Habilité ou une personne autorisée par le Représentant habilité.

C'est le propriétaire du nom de domaine qui autorise le CT à gérer la bi-clé et les demandes de certificat et de révocation de certificat.

#### 1.3.6.2 Contact Technique (CT)

Un Contact Technique est une personne nommée et autorisé par le propriétaire du nom de domaine et qui est autorisée à :

Agir en tant que demandeur SSL pour la génération de la CSR;

Générer les bi-clés dont les clés publiques seront associées à un certificat

SSL; Remplir les formulaires de demande de certificat SSL ;

Récupérer les certificats SSL ;

Procéder le cas échéant aux demandes de révocation des Certificats;

Mettre en œuvre une clé privée, pour des sessions SSL/TLS en tant que serveur;

## 1.4 Usage des certificats

### 1.4.1 Domaines d'utilisation applicables

#### 1.4.1.1 Certificat de l'AC

Le certificat de l'AC sert à authentifier les certificats SSL/TLS. La clé privée associé au certificat d'AC sert pour :

La signature de certificat SSL ;

La signature de certificat de répondeur OCSP ;

La signature de LCR.

#### 1.4.1.2 Certificat SSL

Un certificat SSL délivré par l'AC est utilisé par les UC pour vérifier l'identité d'un nom de domaine sur un serveur donné.

Les certificats SSL ont les usages suivants :

Certificat OV SSL (1.3.6.1.4.1.46111.1.3.101.11) : désigne un certificat électronique « Organization Validated (OV) » ayant pour objet de permettre la mise en place d'une connexion SSL "Secure Socket Layer" sécurisée entre un serveur de site web disposant du Certificat SSL et l'UC se connectant au site web. Un Certificat OV SSL contient l'information sur l'entité légale qui est propriétaire de l'IP, du Wildcard ou du FQDN contenu dans le Certificat OV SSL.

Les certificats délivrés aux CT sont exclusivement utilisés par les CT identifiés au § 1.3.6 ci-dessus pour mettre en œuvre des sessions SSL/TLS pour les noms de domaine pour lesquels ils sont autorisés par les propriétaires de nom de domaine.

Il est rappelé que l'utilisation de la clé privée, par les CT, et du certificat associé doit rester strictement limitée au service de sécurisation de serveur SSL/TLS. Dans le cas contraire, leur responsabilité pourrait être engagée.

### 1.4.2 Domaines d'utilisation interdits

Les utilisations de Certificats émis par l'AC à d'autres fins que celles prévues au § 1.4.1 ci-dessus ne sont pas autorisées. En pratique, cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des Certificats qu'elle émet autre que celles prévues dans la présente PC.

Les Certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation.

Cette PC décrit la gestion du cycle de vie des Certificats SSL et bi-clés associées indépendamment de leur support de génération et d'utilisation, elle n'a pas vocation de remplacer une politique de sécurité des serveurs SSL et des machines Client SSL qui elle décrit la gestion des sessions SSL et la protection des bi-clés sur les serveurs.

Il convient au CT d'élaborer leur propre politique de sécurité afin de définir notamment les engagements et les limites de responsabilités qu'un accès à un nom de domaine lors d'une session SSL confère au données,

diffusées ou reçues, et aux fonctions ainsi accessible, ainsi que les moyens et conditions de protection des bi-clés.

## 1.5 Gestion de la PC

### 1.5.1 Entité gérant la PC

La présente PC est sous la responsabilité de l'AGPC.

### 1.5.2 Point de contact

Coordonnées de la personne ou de la direction responsable de l'élaboration de la PC :

DKB SOLUTIONS ;

Nom de la personne : Mr DJAHA

Contact : Bertin DJAHA Adresse : Riviera 3, Rue E128, Résidence Améthyste - Pavillon Cristal - 17 BP 519 Abidjan 17 -COTE D'IVOIRE

Email: bertin.djaha@dkbsolutions.com

Phone: +225-22-470050

Fax: +225-22-470475

### 1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

L'AGPC procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour les composantes de l'IGC de gérer des certificats.

### 1.5.4 Procédure d'approbation de la conformité de la DPC

L'AGPC possède ses propres méthodes pour approuver le présent document. L'AGPC approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.

## 1.6 Définitions et Acronymes

### 1.6.1 Définitions

**Accord d'utilisation de LCR:** Un accord spécifiant les termes et conditions sous lesquels une Liste de Certificats Révoqués ou les informations qu'elle contient peuvent être utilisées.

**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].

**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 mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

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

**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).

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

**Chemin de certification :** (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

**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.

**Confidentialité :** La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

**Contremarque de Temps** : Donnée signée qui lie une représentation d'une donnée à un temps particulier fournit par une UH, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là. Cette contremarque de temps est signée électroniquement par une Unité d'Horodatage (UH). Une Contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figure.

**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].

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

**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 :** fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes :

Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie ;

Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1] ;

Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

**Infrastructure de Gestion de Clés (IGC) :** également appelée IGC (Infrastructure de Gestion de Clés), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués. [2nd DIS ISO/IEC 11770-3 (08/1997)].

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

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

**Liste de Certificats Révoqués (LCR) :** 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.

**Nom de domaine :** nom enregistré par l'organisation auprès d'organismes tels que l'AFNIC ou l'INTERNIC. Il est composé du nom précédant l'extension (telle que .fr ou .com) et complété par l'extension elle-même. Le nom de domaine doit toujours être enregistré au nom de l'organisation qui en fait la demande. Pendant le processus d'enregistrement, le nom de domaine est « associé » à un contact technique qui est juridiquement autorisé à utiliser ce nom de domaine.

**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 (en anglais: Certificate Signing Request: CSR).

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

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

**Politique de Certification (PC) :** ensemble de règles 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].

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

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

**Registrar** : Une entité légale qui enregistre et gère officiellement des noms de domaine en conformité avec les règles de l'ICANN (Internet Corporation for Assigned Names and Numbers) . Un Registrar met en œuvre un service dit « WHOIS » de recherche d'information sur la gestion des Noms de domaine (y compris pour les Wildcard) et les adresse IP vérifiables sur internet.

**RSA :** algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

**Support :** Tout élément matériel logiciel (serveur, …) qui permet de générer et utiliser la bi-clé dont la clé public est associée au certificat SSL.

**Validation de certificat électronique** : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification.

**Wildcard** : Un nom de domaine complet contenant un astérisque (*) dans la position la plus à gauche dans le FQDN Client.

### 1.6.2 Acronymes

AC : Autorité de Certification ;

AE : Autorité d'Enregistrement ;

CC : Critères Communs ;

DN : Distinguished Name ;

DPC : Déclaration des pratiques de certification ;

EAL : Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;

HTTP : Hypertext Transport Protocol ;

IGC : Infrastructure de Gestion de Clés ;

IP : Internet Protocol ;

ISO : International Organization for Standardization ;

LCR : liste de certificats révoqués ;

LDAP : Lightweight Directory Access Protocol ;

OCSP : Online Certificate Status Protocol ;

OID : Object Identifier ;

PC : Politique de Certification ;

PIN : Personal Identification Number ;

PKCS : Public-Key Cryptography Standard ;

AGPC : Autorité de Gestion des Politiques de Certification ;

RFC : Request for comment ;

RSA : Rivest, Shamir, Adleman ;

SHA : Secure Hash Algorithm (norme fédérale américaine) ;

SP : Service de Publication ;

URL : Uniform Resource Locator.

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

## 2.1 Entités chargées de la mise à disposition des informations

Le SP est en charge de la publication des données identifiées au § 2.2 ci-dessous.

## 2.2 Informations devant être publiées

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

- La PC des AC
  - PC personne physique : https://dkbsolutions.com/storage/documents/pki/Fr/PC_DKB_SOLUTIONS_Certificats_Personnes_V1.0.pdf
  - PC cachet serveur : https://dkbsolutions.com/storage/documents/pki/Fr/PC_DKB_SOLUTIONS_Certificats_Cachet_Serveur_V1.0.pdf
  - PC ssl : https://dkbsolutions.com/storage/documents/pki/Fr/PC_DKB_SOLUTIONS_Certificats_SSL_V1.0.pdf
- Les versions antérieures des présentes PC, tant que des certificats émis selon ces versions sont en cours de validité,
- Les certificats des AC la chaîne de confiance auxquels les AC sont rattachés : https://dkbsolutions.com/storage/documents/pki/Fr/Certificats_Electroniques_ACR_et_AC_DKBS.rar
- Le formulaire de demande de certificat ;
- Le formulaire et/ou les modalités de révocation d'un certificat ;
- Les conditions générales d'utilisation (CGU)
  - Personne physique : https://dkbsolutions.com/storage/documents/pki/Fr/DKBS_CGU_Personne_Physique_V1.1.pdf
  - Cachet serveur : https://dkbsolutions.com/storage/documents/pki/Fr/DKBS_CGU_Cachet_Serveur_V1.1.pdf
  - SSL : https://dkbsolutions.com/storage/documents/pki/Fr/DKBS_CGU_SSL_OV_V1.1.pdf
- LCR : AC : "AC DKB SOLUTIONS PERSONNES 1"
  - https://dkbsolutions.com/storage/documents/pki/Fr/ACDKBSolutionsPersonnes1.crl
- ARL : ACR : "AC RACINE DKB Solutions" :
  - https://dkbsolutions.com/storage/documents/pki/Fr/ACDKBSolutionsMachines1.crl
- OCSP pour l'ACR
- OCSP pour l'AC

La DPC n'est pas publiée mais consultable auprès de L'AGPC sur demande justifiée et autorisée par l'AGPC.

L'AGPC s'assure que les conditions générales d'utilisation, en fonction du besoin des acteurs et des utilisateurs des services de l'IGC, sont rendues disponibles de la manière suivante :

- Porteur, Client et MC : les CGU sont contenues dans les demandes de certificats et demandes de créations de MC et sont donc signées par le MC, le Porteur et le Représentant Habilité du Client ou une personne autorisée par le Représentant Habilité du Client.

  Utilisateur de certificat : les conditions d'utilisation du service IGC sont décrites dans la présente PC aux paragraphes : 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, et 9.8.

## 2.3 Délais et fréquences de publication

La PC de l'AC et le certificat de l'AC sont disponibles en permanence et mises à jour selon les besoins suivant un taux de disponibilité définie dans la DPC.

Une nouvelle LCR est publiée toutes les 24 heures suivant un taux de disponibilité définie dans la DPC.

## 2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. L'AC s'assure que toute information conservée dans une base documentaire de son IGC et dont la diffusion publique ou la modification n'est pas prévue est protégée.

L'ensemble des informations publiques et publiées (Se reporter au § 2.2) est libre d'accès en lecture et téléchargement sur Internet.

# 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 propriétaire du nom de domaine (subject) sont identifiés par un Distinguished Name (DN).

Les attributs du DN sont encodés en « printableString » ou en « UTF8String » à l'exception des attributs emailAddress qui sont en « IA5String ».

#### 3.1.1.1 Certificat AC : « AC DKB SOLUTIONS MACHINES 1 »

L'identité de l'AC dans le certificat de l'AC est la suivante :

| Champ de base | Valeur |
|---|---|
| Issuer | C=CI<br>O = CertAfrique - DKBS<br>OU = CI-ABJ-2006-B-8567<br>CN = AC RACINE DKB Solutions 1 |
| Subject | C=CI<br>O = CertAfrique - DKBS<br>OU = CI-ABJ-2006-B-8567<br>CN = AC DKB Solutions MACHINES 1 |

#### 3.1.1.2 Certificat SSL OV :

L'identité du certificat est la suivante :

| Champ de base | Valeur |
|---|---|
| Issuer | C=CI<br>O = CertAfrique - DKBS<br>OU = CI-ABJ-2006-B-8567<br>CN = AC DKB Solutions MACHINES 1 |
| Subject | C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente d est officiellement enregistré (tribunal de commerce, ministère, …). Ce code est inscrit en majuscules ;<br>O = Nom officiel complet de l'organisation cliente tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …) ;<br>OU= identification de l'entité légale<br>Pour les Clients de droit ivoirien :<br>l'identification RCCM<br>Pour les entités de droit non ivoiriens, plusieurs possibilités existent : |

| | |
|---|---|
| | soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres<br><br>soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002<br><br>soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.<br><br>D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.<br><br>CN = FQDN, Wildcard ou IP (Cette valeur doit être identique à une seule des valeurs définie pour l'extension SAN ci-dessous).<br>L = ville l'entité légale du propriétaire du nom de domaine. |

### 3.1.2 Nécessité d'utilisation de noms explicites

Les noms contenus dans le certificat sont soit une IP, un Wildcard ou FQDN tel que vérifiable auprès d'un Registrar.

### 3.1.3 Anonymisation ou pseudonymisation

S'agissant de certificats de machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

### 3.1.4 Règles d'interprétation des différentes formes de noms

Les UC peuvent se servir de l'identité incluse dans les certificats (se reporter au § 3.1.1) afin d'authentifier des noms de domaine.

### 3.1.5 Unicité des noms

Les identités portées par l'AC dans les certificats (se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un propriétaire de nom de domaine ou de serveur ne peut être attribué à un autre propriétaire de nom de domaine ou serveur.

A noter que l'unicité d'un certificat est basé sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au certificat et ne permet donc pas d'assurer une continuité de l'identification dans les Certificats successifs d'un nom de domaine donné. Ces numéros de série doivent avoir au moins 64 bits d'entropie.

En cas de différent au sujet de l'utilisation d'un nom pour un certificat, l'AGPC a la responsabilité de résoudre le différend en question.

### 3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles des lois ivoiriennes relatif à

la Propriété intellectuelle appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

## 3.2 Validation initiale de l'identité

### 3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par le CT est réalisée par les procédures de génération de la clé privée (se reporter au § 6.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (se reporter au § 6.1.3 ci-dessous).

### 3.2.2 Validation de l'identité d'un organisme

#### 3.2.2.1 Certificat OV

L'authentification des organisations (propriétaire de nom de domaine, Client pour le CT) repose sur la vérification des informations fournies par le CT dans le cadre de sa demande de certificat (se reporter au § 4.1). Ces informations comprennent le nom et l'adresse de l'organisation ainsi que les documents ou les références de l'existence de celle-ci, ainsi que le nom de domaine qu'elle détient.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro l'immatriculation au Registre de Commerce et de Crédit Mobilier (RCCM), le numéro de contribuable, etc.

Dans tous les cas, la vérification de l'appartenance d'un CT à l'organisation de « type » Administration et Entreprise dont il se réclame est effectuée en utilisant un appel téléphonique auprès de l'entité légale à partir d'un numéro de téléphone récupéré auprès de l'entité légale ou dans des bases de données officielles de référence.

En vue de la délivrance du Certificat SSL, il est également nécessaire de vérifier que le nom de domaine présent dans la demande appartient à cette organisation (propriétaire de nom de domaine), et qu'elle est donc autorisée à l'utiliser. Les vérifications sont effectuées en consultant les bases de données officielles de noms de domaine de type AFNIC ou INTERNIC. L'AE vérifie que le CT que le nom de domaine inclus dans le FQDN du serveur appartient bien à l'entité qu'il représente.

De même, l'AE applique les vérifications requises par le [CAB Forum] sur les entités légales.

### 3.2.3 Validation de l'identité d'un individu

#### 3.2.3.1 Contact Technique

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du CT correspondant.

L'identification et l'authentification du CT s'effectue sur la base d'une pièce d'identité officielle (carte nationale d'identité et passeport).

L'identification et l'authentification du CT, et du(es) signataire(s) de la demande de certificat est effectuée par l'AE à partir des informations contenues dans le dossier de demande de certificat (se reporter au § 4.1).

Un CT peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant. Dans ce cas, tout nouveau CT fait également l'objet d'une procédure d'enregistrement.

De même, l'AE applique les vérifications requises par le [CAB Forum] sur les personnes.

#### 3.2.4 Informations non vérifiées du CT

Les informations non vérifiées ne sont pas introduites dans les certificats.

#### 3.2.5 Validation de la capacité du demandeur

La validation de la capacité d'un CT correspond à la validation de l'appartenance à une organisation (se reporter au § 3.2.2 ci-dessus) et son autorisation par le propriétaire du nom de domaine.

#### 3.2.6 Critère d'interopérabilité

Un CT qui obtient un certificat émis par l'AC à la garantie d'être authentifiable dans le domaine de confiance DKB SOLUTIONS.

Un certificat SSL émis par l'AC à la garantie d'être authentifiable dans les navigateurs car l'AC émettrice est signée par une ACR « AC RACINE DKB SOLUTIONS 1 » de DKB SOLUTIONS dont le certificat est largement diffusé dans les principaux outils que sont les systèmes d'exploitation et les navigateurs internet.

Un CT de certificat issu de l'une des AC conformément à la présente PC à la garantie d'être reconnu pour le niveau de sécurité ETSI EN 319 411-1 OVCP.

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

#### 3.3.1 Identification et validation pour un renouvellement courant

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2 ci-dessus).

#### 3.3.2 Identification et validation pour un renouvellement après révocation

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2).

### 3.4 Identification et validation d'une demande de révocation

Les demandes de révocation sont authentifiées par l'AE à l'aide d'informations seulement connues du CT et de l'AE. Lorsque le demandeur est une personne autre que le CT, l'authentification est réalisée suivant des procédures définies dans la DPC.

# 4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 4.1 Demande de certificat

#### 4.1.1 Origine d'une demande de certificat

Une demande de certificat est émise par un CT auprès de l'AE (service d'enregistrement).

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

Le dossier complet, daté et signé de demande de certificat doit être transmis à l'AE par le CT.

##### 4.1.2.1 Certificat SSL OV

Les informations suivantes doivent figurer dans la demande de certificat SSL :

La demande de certificat est signée par le CT (en fonction de l'origine de la demande), et datée de moins de 3 mois ;

Les informations souhaitées dans le DN et le SAN du certificat SSL ;

Un document officiel d'identité du CT (en fonction de l'origine de la demande), avec signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original" (uniquement pour les dossiers papiers), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;

Les Informations permettant à l'AE de contacter le CT, le propriétaire de nom de domaine (numéro de téléphone, courriel, etc.). Au minimum, une adresse de courrier électronique tel que portée dans le WHOIS doit être utilisée. Si ce n'est pas le cas, alors l'adresse de courrier électronique doit être confirmée à partir de l'adresse de courrier électronique contenue dans le WHOIS ou être de la forme « admin », « administrator », « webmaster », « hostmaster », ou « postmaster »@<le nom de domaine demandé par le CT> ;

Le nom de l'entité légale qui détient le CN demandé et qui doit apparaître dans le certificat ;

Les Conditions Générales d'Utilisation (CGU) signée par le CT;

La CSR pour la clé publique à certifier.

## 4.2 Traitement d'une demande de certificat

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

L'AE authentifie le demandeur.

L'AE s'assure que le demandeur a pris connaissance des CGU.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

#### 4.2.2 Acceptation ou rejet de la demande

En cas d'approbation de la demande, l'AE (service de demande de certificat) transmet la demande à l'AC (service de génération de certificat).

En cas de rejet de la demande, l'AE en informe le CT, en justifiant le rejet..

#### 4.2.3 Durée d'établissement du certificat

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

## 4.3 Délivrance du certificat

### 4.3.1 Actions de l'AC concernant la délivrance du certificat

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat SSL.

L'AC transmet le certificat au service de retrait de certificat de l'AE.

L'AE transmet le certificat au CT.

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

La remise du certificat au CT (service de remise au CT) s'effectue par courrier électronique au CT.

## 4.4 Acceptation du certificat

### 4.4.1 Démarche d'acceptation du certificat

Dès que le CT, a récupéré son certificat, l'AC considère le certificat comme accepté. L'acceptation est tacite.

Si le CT ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non consentement auprès de l'AE. Passé ce délai, le certificat est considéré comme accepté.

### 4.4.2 Publication du certificat

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

Les certificats SSL ne sont pas publiés par le SP.

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

Le demandeur, le contact technique (CT) sont informés de la délivrance d'un Certificat pour le ou les noms de domaine ou serveur dont ils sont responsables.

## 4.5 Usage de la bi-clé et du certificat

### 4.5.1 Utilisation de la clé privée et du certificat par le CT

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (se reporter au § 6.1.7). La clé privée ne peut être utilisée que pour une opération de type sécurité d'accès type session SSL/TLS.

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

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus.

## 4.6 Renouvellement d'un certificat

Cette section concerne le processus de renouvellement du certificat SSL, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

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

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat. Dans ce cas la procédure à appliquer pour renouveler un certificat SSL est identique à celles décrites pour la délivrance du premier certificat SSL (se reporter au § 3.3, § 4.2 ; § 4.3 et § 4.1 ci-dessus).

## 4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

## 4.9 Révocation et suspension des certificats

### 4.9.1 Causes possibles d'une révocation

#### 4.9.1.1 Certificat Composante IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

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 (par exemple, suite à un audit de qualification ou de conformité négatif) ;

Cessation d'activité de l'entité opérant la composante.

#### 4.9.1.2 Certificat SSL

Un certificat est révoqué quand l'association la clé publique et l'identité qu'il certifie n'est plus considérée comme étant valide. Les motifs qui invalident cette association sont :

Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du DN), ceci avant l'expiration normale du certificat ;

Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;

La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le DN certifié ;

La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

La révocation de l'AC ;

La fin de vie de l'AC ;

La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat en question doit être révoqué.

### 4.9.2 Certificat SSL Origine d'une demande de révocation

#### 4.9.2.1 Certificat composante IGC

L'AGPC ou une autorité judiciaire via une décision de justice est à l'origine de la demande de révocation des certificats d'AC.

L'AC est à l'origine de la demande de révocation des certificats de composantes d'IGC.

#### 4.9.2.2 Certificat SSL

Le CT peut faire une demande de révocation dans les cas suivants :

Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du DN), ceci avant l'expiration normale du certificat ;

Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;

La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'organisation Client (se reporter au § 1.3.6.1), pour les Entreprise et les Administration, peut demander la révocation d'un certificat dans les cas suivants :

Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du DN), ceci avant l'expiration normale du certificat ;

Le demandeur, CT n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;

La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le DN certifié ;

La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AC peut demander la révocation d'un certificat dans les cas suivants :

Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du DN), ceci avant l'expiration normale du certificat ;

Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;

La cessation d'activité de l'entité propriétaire du nom de domaine ou la fin d'activité du serveur qui met en œuvre site internet avec le DN certifié ;

La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

La révocation de l'AC ;

La fin de vie de l'AC ;

La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AE peut demander la révocation d'un certificat dans les cas suivants :

Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du DN), ceci avant l'expiration normale du certificat ;

Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;

La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

### 4.9.3 Certificat SSL Procédure de traitement d'une demande de révocation

#### 4.9.3.1 Certificat composante IGC

La DPC précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des CT concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les CT de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié par l'ARTCI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. L'ARTCI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

#### 4.9.3.2 Certificat SSL

Une demande de révocation contient les informations suivantes :

L'identité du demandeur du certificat utilisée dans le certificat (nom, prénom, etc.)

; le DN du serveur utilisée dans le certificat ;

Le nom du demandeur de la révocation ;

Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série du certificat, etc.).

La demande de révocation est conservée par l'AE dans ses journaux.

L'AE authentifie la demande de révocation qu'elle reçoit (se reporter au § 3.4).

L'AE transmet la demande de révocation à l'AC.

L'AC (service de révocation) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC (service de révocation) révoque le certificat en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective du certificat. De plus, si le CT n'est pas le demandeur, alors le CT est également informé de la révocation effective du certificat.

.

#### 4.9.4 Délai accordé au CT pour formuler la demande de révocation

Dès que le demandeur a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

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

##### 4.9.5.1 Certificat Composantes IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR/LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

##### 4.9.5.2 Certificat SSL

Une demande de révocation, authentifiée sur le portail web de l'AE par le CT est traitée dans un délai inférieur à 24 heures.

Toute demande de révocation, authentifiée et dûment établie par l'AE est traitée en urgence par l'opérateur d'AE dans un délai inférieur à 24 heures sauf les week-ends et jour fériés.

#### 4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats

Il appartient aux UC de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR mise en œuvre par l'AC.

#### 4.9.7 Fréquences d'établissement des LCR

La LCR est émise toute les 24 Heures.

#### 4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 30 minutes.

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

L'AC mettra en œuvre un serveur OCSP

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

Cf. chapitre 4.9.6 ci-dessus.

#### 4.9.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

#### 4.9.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats SSL, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC la révocation suite à une compromission de sa clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation de l'AC, l'ensemble des certificats SSL sont révoqués.

Les conditions générales d'utilisation du certificat mentionnent clairement qu'en cas de compromission de la clé privée du CT ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le CT s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

#### 4.9.12 Causes possibles d'une suspension

Sans objet.

#### 4.9.13 Origine d'une demande de suspension

Sans objet.

#### 4.9.14 Procédure de traitement d'une demande de suspension

Sans objet.

#### 4.9.15 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

Le service OCSP est mis à jour à partir des LCR émises par l'AC. Cependant le mécanisme principal de communication du statut des certificats est la LCR publiée par l'AC. Dans tous les cas, les utilisateurs de certificats peuvent utiliser un mécanisme de consultation libre de LCR. Ces LCR sont des LCR au format V2.

Les réponses OCSP de l'AC ont une date d'expiration de 10 jours maximum. Les réponses OCSP de l'ACR ont une date d'expiration de 10 jours maximum.

#### 4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir des informations de l'AC. Le service est disponible 24 heures sur 24 et 7 jours sur 7 suivant un taux de disponibilité préciser dans la DPC. Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue est fixé à un maximum donné dans la DPC.

### 4.11 Fin de la relation entre le CT et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le CT avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat est révoqué.

### 4.12 Séquestre de clé et recouvrement

Les bi-clés et les certificats des CT et d'AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.

# 5 MESURES DE SECURITE NON TECHNIQUES

## 5.1 Mesures de sécurité physiques

### 5.1.1 Situation géographique et construction des sites

Les sites d'exploitation de l'IGC respectent les règlements et standards en vigueur et son installation tient compte des résultats de l'analyse de risques de l'IGC.

La construction des sites respecte les règlements et normes en vigueur.

La localisation géographique des sites ne présente pas de risque concernant les tremblements de terre, les explosions ou les inondations.

Le site d'exploitation est protégé par des systèmes de détection d'intrusion, de caméra, de gardiennage permettant la protection contre les accès non autorisés aux équipements.

Les équipements doivent toujours être protégés contre tout accès non autorisé. Les exigences relatives aux équipements sont les suivantes :

S'assurer qu'aucun accès non autorisé au matériel ne soit autorisé.

S'assurer que tous les supports amovibles et documents papier contenant des informations sensibles en texte brut sont stockés de manière sûre.

S'assurer de l'existence d'une surveillance permanente via vidéo et gardiennage pour protéger les locaux contre les risques d'intrusions.

S'assurer que les ressources cryptographiques et les composantes de l'ACR et AC sont accessibles uniquement par des personnes autorisées.

Assurer qu'un journal des accès est entretenu et inspecté régulièrement.

Fournir plusieurs niveaux de renforcement pour la sécurité périmétrique des accès physique.

Assurer que seules les personnes physiques autorisées ont accès aux composantes de l'Infrastructure de Gestion de Clés.

Assurer la désactivation des modules cryptographiques avant leur stockage.

Assurer que les données d'activation utilisées pour accéder aux modules cryptographiques sont placées dans des coffres.

Assurer que les données d'activation sont soit mémorisées soit enregistrées et stockées de manière compatible avec la sécurité offerte par le module cryptographique.

Assurer que les données d'activation non nécessaire au fonctionnement quotidien de la ressource cryptographique « en ligne » ne sont pas stockées avec le module cryptographique associé.

Une personne ou un groupe de personnes doit être explicitement chargé d'effectuer ces contrôles.

Lorsque les locaux ne sont pas constamment surveillés, la dernière personne à les quitter paraphe une feuille d'inscription qui doit contenir son identité, la date et l'heure et qui affirme que tous les mécanismes nécessaires de protection physique sont en place et activés.

#### 5.1.2 Accès physique

L'accès physique aux fonctions sensibles de l'infrastructure est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.

La traçabilité des accès est assurée.

Des mesures de détection d'intrusion physique sont mises en œuvre, notamment via l'utilisation de caméras.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (DPC, documents d'applications).

#### 5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par l'IGC afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

#### 5.1.4 Vulnérabilité aux dégâts des eaux

Les systèmes de l'IGC sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

#### 5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'IGC permettent de respecter les exigences et les engagements pris par l'IGC dans la présente PC, en matière de disponibilité de ses fonctions.

#### 5.1.6 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

#### 5.1.7 Sauvegardes hors site

L'IGC 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.

### 5.2 Mesures de sécurité procédurales

#### 5.2.1 Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AC sont classés en 5 groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien de des systèmes qui supportent l'IGC en conditions opérationnelles de fonctionnement ;
- 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 de « sécurité », 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 porteurs de données d'activation de clé.

#### 5.2.2 Nombre de personnes requises par tâches

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.

#### 5.2.3 Identification et authentification pour chaque rôles

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de l'IGC avant de lui attribuer un rôle et les droits correspondants, notamment :

Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;

Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;

Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;

Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'AC. Chaque attribution d'un rôle à un membre du personnel de l'IGC lui est notifiée par écrit ou équivalent.

#### 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. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC.

### 5.3 Mesures de sécurité vis-à-vis du personnel

#### 5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'AC est soumise à une clause de confidentialité vis -à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

#### 5.3.2 Procédures de vérification des antécédents

L'AC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet 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.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

#### 5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère.

Le personnel a eu connaissance et 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, dans l'organisation, etc. en fonction de la nature de ces évolutions.

#### 5.3.5 Fréquence et séquence de rotation entre différentes attributions

Des précisions sont fournies dans la DPC.

#### 5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

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

Des précisions sont fournies dans la DPC.

#### 5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

### 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.

Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

#### 5.4.1 Type d'événements 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 / rejet d'une demande de certificat ;

Evènements liés aux clés d'AC et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...) ;

Génération des certificats;

Génération des bi-clés;

Transmission des certificats aux CT et selon les cas, acceptations / rejets par les CT

; Publication et mise à jour des informations liées à l'AC ;

Génération d'information de statut d'un certificat SSL.

Chaque enregistrement d'un évènement dans un journal contient les champs suivants :

Type de l'évènement ;

Nom de l'exécutant ou référence du système déclenchant l'évènement ;

Date et heure de l'évènement ;

Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

Destinataire de l'opération ;

Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;

Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;

Cause de l'évènement ;

Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

### 5.4.2 Fréquence de traitement des journaux d'événements

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement. Des précisions sont fournies dans la DPC.

### 5.4.3 Période de conservation des journaux d'événements

La journalisation doit être 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 doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être 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. Elle peut entraîner un besoin de protection en confidentialité.

### 5.4.4 Procédures de sauvegarde des journaux d'événements

L'IGC mettent en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques de l'AC.

### 5.4.5 Système de collecte des journaux d'événements

Des précisions sont fournies dans la DPC.

### 5.4.6 Evaluation des vulnérabilités

L'AC et l'AE doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés au moins à une fréquence mensuelle. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

## 5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

### 5.5.1 Type de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques (7 ans) ;
- La politique de certification (10 ans) ;
- La déclaration des pratiques de certification (10 ans) ;
- Les certificats tels qu'émis ou publiés (7 ans) ;
- Les justificatifs d'identité des CT et, le cas échéant, de leur entité de rattachement (pour les entreprises et les administrations) (7 ans) ;
- Les dossiers complets de demandes de certificats (7ans) ;
- Les journaux d'évènements des différentes entités de l'IGC (10 ans).

### 5.5.2 Période de conservation des archives

**Certificats et LCR émis par l'AC**

Les certificats SSL et d'AC sont archivés 7 ans après leur expiration.

**Journaux d'événements**

Les journaux techniques d'évènements traités au chapitre 5.4 sont archivés pendant 7 ans après leur génération.

**Dossier de demande de certificat**

Les dossiers d'enregistrement (papier ou électronique comme définit au § 4.1) ne sont conservés que 7 ans par l'AE.

**Réponse OCSP**

Les réponses OCSP sont conservées pendant 3 mois suite à leur expiration.

Toutes les autres données listées au § 5.5.1 sont conservées au moins 10 ans.

### 5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

Seront protégées en intégrité ;

seront accessibles aux seules personnes autorisées ;

pourront être consultées et exploitées.

### 5.5.4 Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 6.8.

### 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 (Se reporter au 5.5.3).

### 5.5.6 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

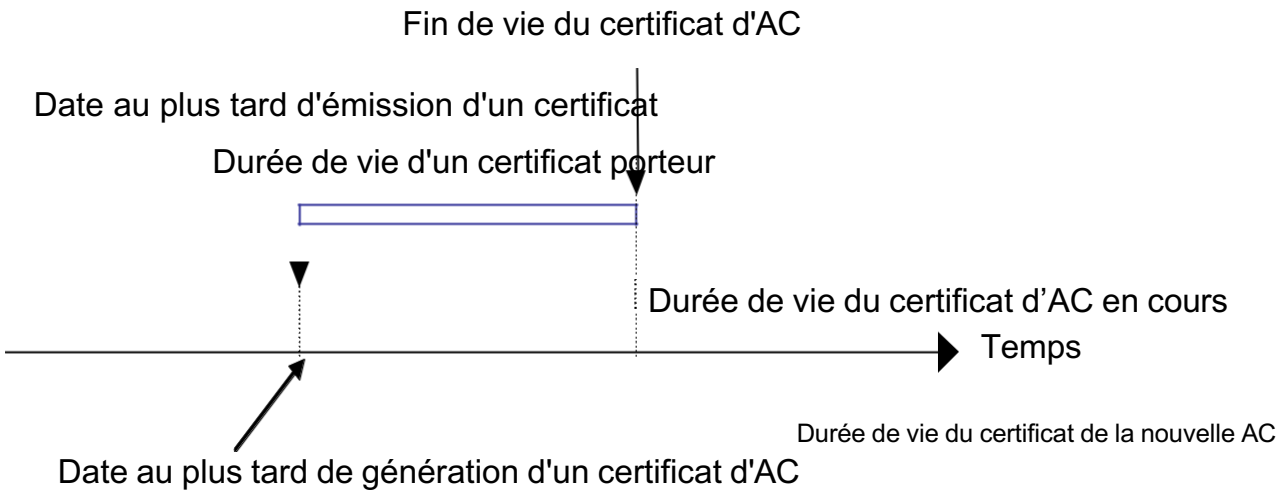
## 5.6 Changement de clé d'AC

### 5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière. La DPC précise les standards utilisés.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats SSL. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats SSL émis à l'aide de cette bi-clé.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

#### 5.6.2 Certificat SSL

La durée de validité d'un certificat est de 3 ans maximum.

### 5.7 Reprise suite à compromission et sinistre

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

L'AC a établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC.

L'AC a conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité de l'AC fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'AC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'AC détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses CT devient insuffisant pour son utilisation prévue restante, alors l'AC :

- Informe tous les CT et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats ;
- Révoque tous les certificats concernés.

Si nécessaire, l'ampleur des conséquences est évalué par l'AC afin de déterminer si les services de l'AC doivent être rétablis, quels certificats SSL doivent être révoqués, l'AC doit être déclarée compromise, certains services peuvent être maintenus (en priorité les services de révocation et de publication d'état des certificats SSL) et comment, selon le plan de reprise d'activité.

L'AC doit également prévenir directement et sans délai le point de contact identifié de l'ARTCI.

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

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des service de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

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

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- L'AGPC, après enquête sur l'évènement décide de révoquer le certificat de l'AC ;
- Tous les Clients dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- L'AGPC décide ou non de générer un nouveau certificat d'AC ;
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;

Les CT sont informés de la capacité retrouvée de l'AC de générer des certificats.

#### 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 § 5.7.1.
Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

### 5.8 Fin de vie d'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC 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 la 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 ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats SSL et des informations relatives aux certificats) ;

Assure 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.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des CT ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire ;

L'AC doit communiquer au point de contact identifié sur le site de l'ARTCI, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à l'ARTCI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les CT et les utilisateurs de certificats ;

L'AC doit tenir informées l'ARTCI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

#### 5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les

obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, 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, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

La notification des entités affectées ;

Le transfert de ses obligations à d'autres parties ;

La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés. Lors de l'arrêt du service, l'AC :

S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;

Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;

Révoque son certificat ;

Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;

Informe (par exemple par récépissé) tous les CT des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

# 6 MESURES DE SECURITE TECHNIQUES

## 6.1 Génération et installation de bi-clés

### 6.1.1 Génération des bi-clés

#### 6.1.1.1 Bi-clés d'AC

Suite à l'accord de l'AGPC pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle (Cf. 6.2.11).

Pour les autres AC, les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe 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. L'ensemble de la cérémonie des clés est enregistré sous vidéo.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

#### 6.1.1.2 Bi-clés SSL

La génération de la bi-clé est réalisée directement dans le Support de la bi-clé par le CT ou sous contrôle du CT. Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité.

L'AC n'est pas responsable du processus choisit par le CT pour la génération, la protection et l'utilisation de la bi-clé certifiée.

### 6.1.2 Transmission de la clé privée à son propriétaire

#### 6.1.2.1 Bi-clés SSL

Il n'y a pas de fourniture de clé privée au CT car c'est le CT ou qui gère la génération de la bi-clé à certifier.

La clé reste donc constamment sous le control et la responsabilité du CT.

### 6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise à l'AE par le CT, lors de la demande de certificat, au format PKCS#10 et la transmission est authentifiée par l'AE.

La clé publique est transmise à l'AC par le CT qui initie la demande de certificat auprès de l'AE, sous un format PKCS#10, et lors d'une connexion sécurisée (SSL) 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

Le certificat de l'AC est remis au CT lors de la remise du certificat au CT.

L'ensemble des certificats d'AC sont publiés par l'AC.

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le support qui est remis au CT lors de la remise du certificat au CT.

### 6.1.5 Taille des clés

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

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA-256 est utilisée pour l'AC. La taille de la bi-clé de l'AC est d'au moins 2048 bits.

La longueur des clés des certificats SSL est de 2048 bits pour l'algorithme RSA avec la fonction de hachage SHA-256.

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

##### 6.1.6.1 Bi-clé AC

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié renforcé.

##### 6.1.6.2 Bi-clés SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité.

#### 6.1.7 Objectifs d'usage de la clé

L'utilisation du champ "key usage" dans le certificat porteur et certificat AC est la suivante :

AC :

- Key CertSign ;
- Key CRL Sign ;

Certificat SSL:

- keyEncipherment.
- Digital signature.

L'utilisation du champ « Extented key usage » dans le certificat SSL est la suivante :

Certificat SSL :

- id-kp-serverAuth

### 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

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueurs ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

L'AC fournit le support matériel au CT, directement, et s'assure que :

La préparation des dispositifs de création de signature est contrôlée de façon sécurisée par le prestataire de service ;

Les supports matériels sont stockés et distribués de façon sécurisée dans l'IGC.

#### 6.2.2 Contrôle de la clé privée par plusieurs personnes

##### 6.2.2.1 Bi-clé AC

L'activation de la clé privée d'AC est contrôlée par au moins 2 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée

d'AC font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seul rôles de confiances qui peuvent émettre des certificats.

#### 6.2.2.2 Bi-clé Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité.

### 6.2.3 Séquestre de clé privée

Les clés privées d'AC et des serveurs ne font jamais l'objet de séquestre.

### 6.2.4 Copie de secours de de clé privée

#### 6.2.4.1 Bi-clé AC

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de 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. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée (AES ou 3DES).

#### 6.2.4.2 Bi-clé Certificat SSL

Le CT ne peut pas procéder à une copie de sauvegarde de sa clé privée.

### 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

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme AES ou 3DES. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

### 6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographique matérielles 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 Bi-clé AC

Les clés privées d'AC ne peuvent être activées qu'avec un minimum de 2 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

#### 6.2.8.2 Bi-clé Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité (se reporter au § 6.1.1).

### 6.2.9 Méthode de désactivation de la clé privée

#### 6.2.9.1 Bi-clé AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats SSL et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

#### 6.2.9.2 Bi-clé Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité.

.

### 6.2.10 Méthode de destruction des clés privées

#### 6.2.10.1 Bi-clé AC

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la retrouver.

#### 6.2.10.2 Bi-clé Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de destruction de bi-clé en toute sécurité (se reporter au § 6.1.1).

### 6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature

Se reporter au § 6.1.6.

## 6.3 Autres aspects de la gestion des bi-clés

### 6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (se reporter au § 5.5.2 ci-dessus).

### 6.3.2 Durée de vie des bi-clés et des certificats

#### 6.3.2.1 AC

Comme une AC ne peut émettre de certificats SSL d'une durée de vie supérieure à celle de son propre certificat, la bi -clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats SSL émis.

#### 6.3.2.2 Certificat SSL

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

## 6.4 Données d'activation

### 6.4.1 Génération et installation des données d'activation

#### 6.4.1.1 AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § 6.1.1.1). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

#### 6.4.1.2 Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité.

.

### 6.4.2 Protection des données d'activation

#### 6.4.2.1 Bi-clé AC

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

#### 6.4.2.2 Bi-clé Certificat SSL

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité.

### 6.4.3 Autres aspects liés aux données d'activation

Les données d'activation sont changées dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

## 6.5 Mesures de sécurité des systèmes informatiques

### 6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une IGC comprend les fonctions suivantes :

Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs) ;

Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;

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 rapide des droits d'accès ;

Protection du réseau contre toute intrusion d'une personne non autorisée ;

Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;

Fonctions d'audits (non-répudiation et nature des actions effectuées) ;

Eventuellement, gestion des reprises sur erreur.

Quand un composant d'IGC est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'IGC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

#### 6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'IGC utilisés pour supporter les services d'AC et qui sont hébergés par l'IGC ont été conçus en suivant les recommandations de sécurité des standards internationaux.

### 6.6 Mesures de sécurité des systèmes durant leur cycle de vie

#### 6.6.1 Mesures de sécurité liées au développement des systèmes

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

Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;

Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;

Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;

Les matériels et logiciels sont dédiés aux activités d'IGC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC ;

Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;

Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

#### 6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système d'IGC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AGPC et l'OT. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC. Lors de son premier chargement, on vérifie que le logiciel de l'IGC 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.

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

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

### 6.7 Mesures de sécurité réseau

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

Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, 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.

L'AC Racine n'est pas en ligne et n'est jamais connecter à réseau.

## 6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

Du début de validité d'un Certificat ;

De la révocation d'un Certificat ;

De l'affichage de mises à jour de LCR.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

# 7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

## 7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats SSL et AC sont définis par le RFC 5280.

### 7.1.1 Extensions de Certificats

#### 7.1.1.1 Certificat AC

Les informations principales contenues dans le certificat de l'AC sont les extensions suivantes :

Authority Key Identifier ;

Basic Constraint (critique)

; Key Usage (critique) ;

Extended Key Usage ;

CRL distribution point ;

Subject Key Identifier.

#### 7.1.1.2 Certificat SSL

Les informations principales contenues dans le certificat porteur sont les extensions suivantes :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Certificate Policies ;
- CRL Distribution Points ;
- Authority Information Access ;
- Key Usage (critique) ;
- Extended Key Usage ;
- Subject Alternative Name (contient au moins une entrée et qui est égale la valeur du CN du DN) ;
- Subject Key Identifier.

### 7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-2WithRSAEncryption: 1.2.840.113549.1.1.11.

### 7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1.2 pour l'identité des CT et de l'AC qui est portée dans les certificats émis par l'AC.

### 7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2 et l'OID 2.23.140.1.2.2 pour les certificats SSL.

### 7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

### 7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

### 7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

## 7.2 Profil de LCR

### 7.2.1 LCR et champs d'extensions des LCR

La DPC donne le détail.

## 7.3 Profil OCSP

La DPC donne le détail.

# 8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

## 8.1 Fréquence et / ou circonstances des audits

L'ensemble des composantes de l'IGC (y compris les AE des Revendeurs) fait l'objet d'audit périodique de conformité, réalisé par DKB SOLUTIONS ou une entité désignée par DKB SOLUTIONS, au moins une fois par an, pour permettre à l'AGPC d'autoriser l'AC d'émettre ou non (selon le résultat des audits) des certificats SSL au titre de la présente PC. Cet audit est réalisé dans le cadre de la qualification ARTCI de l'AC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par l'ARTCI.

A ce titre, des audits appelés « audit interne » quand ils sont réalisés par DKB SOLUTIONS et « audit externe » quand ils sont réalisés par un auditeur externe sont réalisés de manière régulière. De même, l'AE est informé que dans le cadre du schéma de qualification utilisé pour qualifier l'AC dans son ensemble, dont dépendent l'AE, l'auditeur externe, qui audit les composantes de l'IGC pour le service complet de gestion des certificats émis par l'AC, se réserve le droit de réaliser des audits dit « inopiné » des AE. La réalisation de ces audits (dit audit externe) n'est pas soumise à obligation de la part de DKB SOLUTIONS ni de l'auditeur d'avertissement spécifiques auprès de l'AE et peuvent se réaliser n'importe quand. Une AE qui est totalement autonome pour la gestion des certificats SSL, doit obligatoirement être auditée par un auditeur externe, vis-à-vis de l'ARTCI, pour les certificats qu'elle gère, et ce de manière régulière.

La démarche et les exigences liées aux audits de qualification sont définies par l'ARTCI et ne sont donc pas reprises ici.

## 8.2 Identités / qualifications des évaluateurs

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la PC. Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale. L'AGPC apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. L'AGPC effectue elle-même le choix des auditeurs.

## 8.3 Relation entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante de l'AGPC, soit une entité de l'AGPC suffisamment séparée de l'AC afin d'effectuer une évaluation juste et indépendante.

L'AGPC détermine si un auditeur remplit cette condition.

## 8.4 Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC opère ses services en conformité avec la présente PC et sa DPC.

## 8.5 Actions prises suite aux conclusions des évaluations

L'AGPC peut décider que l'AC ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, l'AGPC peut suspendre les opérations de la composante non conforme de l'IGC, ou peut donner l'ordre de cesser toute relation avec la composante en question, ou peut décider que des actions correctives sont à prendre.

Quand l'auditeur en charge de l'audit de conformité trouve une divergence avec les exigences de la présente PC, les mesures suivantes doivent être prises :

L'auditeur note la divergence ;

L'auditeur avise l'entité en question de la divergence. L'entité en avise rapidement l'AGPC ;

La partie responsable de la correction de la divergence détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC, et les effectue sans délai avec l'approbation de l'AGPC.

Suivant la nature et la gravité de la divergence, et la rapidité avec laquelle elle peut être corrigée, l'AGPC peut décider de suspendre temporairement le fonctionnement de l'AC, de révoquer le certificat émis par l'AC, ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, l'AC en informe l'AGPC et lui fournit un rapport de mise à hauteur, pour évaluation.

## 8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à l'AGPC comme prévu au § 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est pas rendu disponible à des tiers utilisateurs sur Internet.

# 9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

## 9.1 Tarifs

### 9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Les conditions tarifaires sont communiquées au Client par DKB SOLUTIONS ou le revendeur.

### 9.1.2 Tarifs pour accéder aux certificats

Les certificats de la chaîne de confiance sont accessibles par les utilisateurs de certificats gratuitement.

Les certificats SSL ne sont pas publiés.

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

Le service de publication de l'AC (qui contient la LCR pour les certificats SSL et d'AC) est accessible gratuitement sur Internet.

### 9.1.4 Tarifs pour d'autres services

Sans objet.

### 9.1.5 Politique de remboursement

La politique de remboursement applicable est définie dans les conditions générales d'utilisation à destination du CT.

## 9.2 Responsabilité financière

### 9.2.1 Couverture par les assurances

DKB SOLUTIONS décrit dans ses engagements cet aspect.

### 9.2.2 Autres ressources

DKB SOLUTIONS dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

### 9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amené à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et les contrats établis avec les revendeurs.

## 9.3 Confidentialité des données professionnelles

### 9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

La partie non-publique de la DPC de l'AC ;

Les clés privées de l'AC, des composantes et des CT ;

Les données d'activation associées aux clés privées d'AC et des CT ;

Tous les secrets de l'IGC ;

Les journaux d'évènements des composantes de l'IGC ;

Le dossier d'enregistrement du CT;

Les causes de révocations, sauf accord explicite du CT

; La politique de sécurité interne de l'AC ;

Les parties de la DPC considérées comme confidentielles.

Par ailleurs, l'AC garantit que seuls ses personnels dans des rôles de confiance autorisés, les personnels contrôleurs dans la réalisation des audits de conformité, ou d'autres personnes détenant le besoin d'en connaître, ont accès et peuvent utiliser ces informations confidentielles.

#### 9.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

#### 9.3.3 Responsabilité en termes de protection des informations confidentielles

L'AC a mis en place et respecte des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des CT à des tiers dans le cadre de procédures légales.

### 9.4 Protection des données personnelles

#### 9.4.1 Politique de protection des données personnelles

La collecte et l'usage de données personnelles par les composantes de l'IGC dans le cadre du traitement des demandes de certificats sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire ivoirien.

#### 9.4.2 Informations à caractère personnelles

L'AC considère que les informations suivantes sont des informations à caractère personnel :

Données d'identification contenues dans les dossiers d'enregistrement ;

Demande (renseignée) d'émission de certificat ;

Demande (renseignée) de révocation de certificat ;

Motif de révocation des certificats.

#### 9.4.3 Informations à caractère non personnel

Sans objet.

#### 9.4.4 Responsabilité en termes de protection des données personnelles

L'AC a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat SSL.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire ivoirien.

En application de la loi, les CT disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans la demande de certificat et les CGU associés. Pour l'exercer, les CT doivent s'adresser à DKB SOLUTIONS, par téléphone au +225-22-470050 ou par courrier électronique bertin.djaha@dkbsolutions.com.

Lorsqu'un revendeur est utilisé alors, il doit se conformer aux exigences de la loi et de la présente PC pour la gestion des données personnelles. DKB SOLUTIONS reporte ce type d'exigence dans le contrat avec le Revendeur.

#### 9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées lors de l'enregistrement ne peut être utilisée par l'IGC, pour une autre utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la part du CT le cas échéant et du Représentant Habilité ou une personne autorisée par le Représentant Habilité. Les consentements du CT pour l'utilisation desdites données pour celle définie dans

le cadre de la PC sont considérés comme obtenus lors de la soumission de la demande de certificat signée et du fait de l'acceptation par le CT du certificat émis par l'AC.

Le CT et Représentant habilité ou la personne désignée par le Représentant Habilité acceptent que les données personnelles les concernant recueillies lors de la demande de certificats fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AE, de permettre les vérifications nécessaires à la délivrance des certificats, à leur renouvellement et à leur révocation, de permettre la construction de l'identité portée dans les certificats et d'apporter les preuves nécessaires à la gestion des certificats.

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

L'AC agit conformément à la réglementation ivoirienne (loi n°2013-450 du 19 juin 2013) et dispose de procédures sécurisées pour permettre l'accès aux autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

#### 9.4.7 Autres circonstances de divulgation d'informations personnelles

L'AC obtient l'accord des signataires d'une demande de certificat (se reporter au § 9.4.5) de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

### 9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle.

L'AC détient tous les droits de propriété intellectuelle et elle est propriétaire de la PC et de la DPC associée, des certificats émis par l'AC.

Le CT détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats SSL émis par l'AC et dont il est propriétaire.

L'entité légale détient tous les droits de propriété intellectuelle sur les informations de l'entité légales contenues dans les certificats SSL et dont elle est propriétaires.

### 9.6 Interprétations contractuelles et garanties

Les composantes de l'IGC, les Clients et la communauté d'utilisateurs de certificats sont responsables pour tous dommages occasionnés en suite d'un manquement de leurs obligations respectives telles que définies aux termes de la PC, des CGU et des contrats.

#### 9.6.1 Obligations communes

Les obligations communes des différentes composantes de l'IGC sont :

- Assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- N'utiliser les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;
- Documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'IGC ;

Respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;

Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées ;

Respecter les conventions qui les lient aux autres entités composantes de l'IGC.

### 9.6.2 Obligations et garanties de l'AGPC

Les obligations de l'AGPC sont les suivantes :

L'élaboration de la PC et de la DPC ;

L'audit de l'AC ;

Le contrôle de la relation contractuelle avec le CT agissant en tant qu'AE ;

Documente les schémas de certification qu'elle entretient avec des AC tierces.

### 9.6.3 Obligations et garanties de l'ACR

DKB Solutions en qualité d'AC Racine (ACR) :

S'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats.

Est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'IGC fournit tous les services de certification en accord avec sa DPC.

Faire auditer son ACR.

Respecter les exigences minimales définies par l'AGPC, pendant, au minimum, la durée de validité de son certificat d'ACR émis par l'IGC.

Se conformer aux procédures et instructions particulières publiées par l'AGPC pour lui adresser ses demandes de certification, de révocation, ou toute autre demande.

Assurer l'authenticité, l'exactitude et la complétude des informations transmises à l'AGPC par elle-même et par les autorités auxquelles elle délègue.

Assurer l'information des porteurs, utilisateur de certificat en cas de révocation de l'AC ou d'une composante de l'IGC.

Publier les ARLs de l'IGC dans les délais impartis en fonction des besoins des utilisateurs de certificat.

Informer dans les plus brefs délais l'AGPC de tout événement modifiant ou susceptible de modifier les conditions d'application de la présente PC notamment pour une cause motivant une révocation.

### 9.6.4 Obligations et garanties de l'AC

L'AC s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats SSL.

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC sont :

Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;

N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;

Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée) ;

Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AGPC de contrôler et vérifier la conformité avec la PC ;

Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;

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 ;

Met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations ;

Prendre toutes les mesures raisonnables pour s'assurer que ses CT sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

L'AC est responsable de la conformité de sa PC, avec les exigences émises par l'ARTCI. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC par elle- même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des CT à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée.

### 9.6.5 Obligations de l'AE

Les obligations de l'AE sont les suivantes :

L'authentification du CT ;

L'authentification de la demande de certificat ;

L'authentification de la demande de révocation ;

Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AGPC de contrôler et vérifier la conformité avec la PC ;

Respecter la PC et la DPC de l'AC ;

En cas de délégation complète de l'AE, respecter les modalités du contrat établit avec DKB SOLUTIONS.

### 9.6.6 Obligations et garanties du CT

Les obligations du CT sont :

Protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation) ;

Transmettre la clé publique, correspondante à la clé privée, à l'AE ;

Se conformer à toutes les exigences de la PC et de la DPC associée ;

Garantir que les informations qu'il fournit à l'AE sont complètes et correctes ;

Prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité ;

Aviser immédiatement l'AE en cas de besoin de révocation de son certificat.

#### 9.6.7 Obligations et garanties du SP

Les obligations du SP sont :

De publier les LCR ;

De publier les certificats d'AC ;

De publier la PC et les CGU associées ;

De garantir les taux de disponibilités des informations publiées ;

De protéger les accès au SP.

#### 9.6.8 Obligations et garanties des autres participants

##### 9.6.8.1 Obligations et garanties de l'UC

Les obligations de l'UC sont de valider un certificat SSL à l'aide de la LCR fournit par DKB SOLUTIONS.

### 9.7 Limite de garantie

L'AC garantit au travers de ses services d'IGC :

L'identification et l'authentification de l'AC avec son certificat auto signé ;

L'identification et l'authentification des CT avec les certificats générés par l'AC ;

La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

L'émission de Certificats, conformément à la PC, ne fait pas de l'une des composantes de l'IGC, un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du CT et du Client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les CT, les Clients et les utilisateurs de Certificat sont des personnes juridiquement et financièrement indépendantes de l'AC et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification (Se reporter au § 1.3) ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre.

Le fait que le nom d'une organisation soit dans un certificat et utilisé à des fins de signature électronique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du CT.

## 9.8 Limite de responsabilité

DKB SOLUTIONS n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors de la demande d'émission, de renouvellement ou de révocation d'un Certificat.

DKB SOLUTIONS ne garantit pas l'exactitude des informations fournies par le CT et le Client à l'utilisateur de certificat, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au CT.

En outre, le CT demeure responsable à l'égard de DKB SOLUTIONS de toute utilisation non autorisée :

du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée ;

du Certificat et des dommages qui pourraient en résulter.

En outre, le CT demeure responsable à l'égard de DKB SOLUTIONS de toute utilisation non autorisée du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée.

DKB SOLUTIONS n'assume aucun engagement ni responsabilité quant aux conséquences dues à tout retards, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet. En outre, DKB SOLUTIONS n'est pas responsable de la qualité de la liaison internet du Client.

Dans le cas où la responsabilité de DKB SOLUTIONS serait retenue au titre des présentes Conditions Générales d'Utilisation, il est expressément convenu qu'DKB SOLUTIONS serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans les limites maximums fixées par DKB SOLUTIONS.

DKB SOLUTIONS exclut toute responsabilité en cas de non-respect par le Client de ses obligations définies dans les présentes et dans la PC.

DKB SOLUTIONS ne sera pas responsable des préjudices indirects ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d'économies anticipées, perte de clientèle, préjudice d'exploitation, atteinte à l'image de marque, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive des présentes ou inhérents à l'utilisation des Certificats émis par DKB SOLUTIONS.

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l'article 9.15.5 ci-après.

## 9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l'article 9.3 des présentes.

## 9.10 Durée et fin anticipée de validité de la PC

### 9.10.1 Durée de validité

La PC devient effective une fois approuvée par l'AGPC. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

#### 9.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC, l'AGPC décidera soit de faire procéder à un audit de la PC/DPC des AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

#### 9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités de l'AC pour les certificats émis conformément à la PC.

### 9.11 Amendements à la PC

#### 9.11.1 Procédures d'amendements

L'AGPC révise sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de l'AGPC. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées.

#### 9.11.2 Mécanisme et période d'information sur les amendements

L'AGPC donne un préavis d'1 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme de la PC et de la DPC.

#### 9.11.3 Circonstances selon lesquelles l'OID doit être changé

Si l'AGPC estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

### 9.12 Dispositions concernant la résolution de conflits

L'AGPC s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

Entre autre, l'AC définit sa politique de nommage et propose, et s'autorise dans certains cas, de régler les différends concernant l'identité à inscrire dans un certificat et dans le cas où les parties ne parviendraient pas à un accord amiable, le différend sera réglé par un tribunal français.

Lorsque le différend porte sur une identité, alors il est du ressort de l'AE de gérer et de résoudre le litige.

### 9.13 Juridictions compétentes

Les dispositions de la politique de certification sont régies par le droit Ivoirien.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents d'Abidjan, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

### 9.14 Conformité aux législations et réglementations

La PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués par l'ARTCI.

## 9.15 Disposition diverses

### 9.15.1 Accord global

Le cas échéant, la DPC précisera les exigences spécifiques.

### 9.15.2 Transfert d'activités

Sauf si spécifié dans d'autres contrats, seule l'AGPC a le droit d'affecter et de déléguer la PC à une partie de son choix.

### 9.15.3 Conséquence d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite Politique de Certification.

Les intitulés portés en tête de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

### 9.15.4 Application et renonciation

Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

### 9.15.5 Force majeure

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 CTs ou aux UC.

## 9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.


DKBS
DOCUMENT KNOWLEDGE BUSINESS SOLUTIONS
DEPUIS 1994